

روبین آبرناتی و تروی مک میلان

امنیت سیستم های اطلاعاتی



CISSP

مرجع کامل آزمون

ترجمه : دکتر سید سامان کریمی

بانا م خا لو گت

امنیت سیستم‌های اطلاعاتی

مترجم: دکتر سیدسامان کریمی

عنوان و نام پدیدآور	: امنیت سیستم‌های اطلاعاتی / [رابین ام ابرنثی، تروی مک‌میلان]؛ [ترجمه] سیدسامان کریمی.
مشخصات نشر	: تهران: موسسه آموزشی تالیفی ارشدان، ۱۳۹۹.
مشخصات ظاهری	: ۶۹۸ ص: مصور، نمودار، جدول.
شابک	: ۹۷۸-۶۲۲-۲۵۱-۷۶۷-۰
وضعیت فهرست نویسی	: فیپا
یادداشت	: عنوان اصلی: CISSP cert guide, Second edition, [2016]
موضوع	: داده‌پردازی -- کارمندان -- گواهی و گواهی‌نامه‌ها
موضوع	: Electronic data processing personnel -- Certification
موضوع	: کامپیوترها -- ایمنی اطلاعات -- آزمون‌ها -- راهنمای مطالعه
موضوع	: Computer security -- Examinations -- Study guides
شناسه افزوده	: مک‌میلان، تروی، ۱۹۵۳ - م.
شناسه افزوده	: McMillan, Troy
شناسه افزوده	: کریمی، سیدسامان، ۱۳۶۳-، مترجم
شناسه افزوده	: Karimi, Seyed saman
رده بندی کنگره	: TK۵۱۰۵/۵۹
رده بندی دیویی	: ۰۰۵/۸۰۷۶
شماره کتابشناسی ملی	: ۶۲۰۹۱۹۰



مؤسسه آموزشی تالیفی ارشدان

نام کتاب:	امنیت سیستم‌های اطلاعاتی
ترجمه:	دکتر سیدسامان کریمی
ناشر:	آموزشی تالیفی ارشدان
ویرایش:	اول
نوبت چاپ:	اول ۱۳۹۹
حروفچینی و صفحه آرایی:	www.irantypist.com
طراح و گرافیکست:	www.irantypist.com
شابک:	۹۷۸-۶۲۲-۲۵۱-۷۶۷-۰
شمارگان:	۱۰۰۰
مرکز خرید آنلاین:	www.arshadan.com www.arshadan.net
ارتباط با مترجم:	Drsamankarimi@Hotmail.com
مرکز پخش و توزیع:	۰۲۱۴۷۶۲۵۵
قیمت:	۹۷۰۰۰ تومان

به پاس تعبیر عظیم از کلمه ایثار

به پاس عاطفه سرشار و گرمای امیدبخش وجودشان که در این سردترین روزگاران بهترین

پشتیان است

به پاس قلب‌های بزرگشان که فریاد رس است و سرگردانی و ترس در پناهشان به شجاعت

می‌گراید

و به پاس محبت‌های بی دریغشان که هرگز فروکش نمی‌کند

این کتاب را به پدر و مادر عزیزم تقدیم می‌کنم

۳۷	 مقدمه مترجم
۳۹	 فصل ۱: امنیت و مدیریت ریسک (Security and Risk Management)
۴۲	 Security Terms شرایط امنیتی
۴۲	 CIA (Confidentiality, Integrity, Availability) سیا
۴۲	 Confidentiality محرمانه بودن
۴۳	 Integrity یکپارچگی
۴۳	 Availability دسترسی
۴۳	 Default Stance موضع پیش فرض
۴۴	 Defense in Depth دفاع در عمق
۴۴	 Job Rotation چرخش کار
۴۵	 Separation of Duties تفکیک وظایف
۴۵	 Security Governance Principles اصول حاکمیت امنیت
۴۶	 Security Function Alignment هماهنگ سازی (تطبیق) عملکرد امنیتی
۴۷	 Organizational Strategy and Goals استراتژی و اهداف سازمانی
۴۷	 Organizational Mission and Objectives اهداف و مأموریت سازمان
۴۸	 Business Case طرح کسب و کار
۴۸	 Security Budget, Metrics, and Effectiveness بودجه امنیت، معیارها و اثربخشی
۴۹	 Resources منابع
۵۰	 Organizational Processes فرآیندهای سازمانی
۵۰	 Acquisitions and Divestitures اکتساب و واگذاری
۵۲	 Governance Committees کمیته‌های حاکمیت
۵۲	 Security Roles and Responsibilities نقش‌های امنیتی و مسئولیت‌ها
۵۲	 Board of Directors هیئت مدیره
۵۳	 Management مدیریت
۵۴	 Audit Committee کمیته ممیزی
۵۴	 Data Owner مالک داده (صاحب داده)

۵۴.....	Data Custodian	نگهبان داده
۵۵.....	System Owner	صاحب سیستم
۵۵.....	System Administrator	مدیر سیستم (ادمین سیستم)
۵۵.....	Security Administrator	مدیر امنیت
۵۵.....	Security Analyst	تحلیلگر امنیتی
۵۵.....	Application Owner	مالک اپلیکیشن
۵۶.....	Supervisor	سرپرست
۵۶.....	User	کاربر
۵۷.....	Auditor	ممیز، مامور رسیدگی
۵۷.....	Control Frameworks	چارچوبهای کنترل
۵۸.....	ISO / IEC 27000 Series	
۶۰.....	Zachman	چارچوب Zachman
۶۱.....	The Open Group Architecture Framework (TOGAF)	چارچوب معماری گروه باز (TOGAF)
۶۱.....	Department of Defense Architecture Framework (DoDAF)	چارچوب معماری وزارت دفاع (DoDAF)
۶۱.....	British Ministry of Defence Architecture (MODAF)	چارچوب معماری وزارت دفاع بریتانیا (MODAF)
۶۱.....	Sherwood Applied Business Security Architecture (SABSA)	معماری امنیتی کسب و کار کاربردی شروود (SABSA)
۶۲.....	(CobiT)	اهداف کنترل اطلاعات و فن آوری مرتبط (CobiT)
۶۳.....	(NIST)	مؤسسه ملی استاندارد و فناوری (NIST)
۶۳.....	(OCTAVE)	تهدید بحرانی عملیاتی، ارزیابی آسیب پذیری و دارایی (OCTAVE)
۶۵.....	(ITIL) Information Technology Infrastructure Library	کتابخانه زیرساخت فناوری اطلاعات (ITIL)
۶۶.....	Six Sigma	شش سیگما
۶۸.....	(CMMI) Capability Maturity Model Integration	ادغام مدل بلوغ قابلیت (CMMI)
۶۸.....	(CRAMM)	تجزیه و تحلیل ریسک CCTA و روش مدیریت (CRAMM)
۶۸.....	Top-Down Versus Bottom-Up Approach	رویکرد بالا به پایین در مقابل پایین به بالا
۶۹.....	Security Program Life Cycle	چرخه عمر برنامه امنیتی
۷۰.....	Due Care	مراقبت مناسب
۷۰.....	Due diligence	مطالعه دقیق
۷۱.....	Compliance	انطباق

۷۲.....	Legislative and Regulatory Compliance	انطباق تنظیم و قانونگذاری
۷۳.....	Privacy Requirements Compliance	انطباق با الزامات حریم خصوصی
۷۳.....	Legal and Regulatory Issues	مسائل حقوقی و مقررات
۷۳.....	Computer Crime Concepts	مفاهیم جرایم رایانه‌ای
۷۴.....	Computer-assisted crime	جرایم به کمک رایانه
۷۴.....	Computer-Targeted Crime	جرایم رایانه‌ای هدفمند
۷۴.....	Incidental computer crime	جرایم تصادفی رایانه‌ای
۷۴.....	Computer prevalence crime	جرایم شایع رایانه‌ای
۷۵.....	Hackers Versus Crackers	هکرها در مقابل کراکرها
۷۵.....	Computer Crime Examples	نمونه‌های جرم رایانه‌ای
۷۶.....	Major Legal Systems	سیستم‌های حقوقی عمده
۷۷.....	Civil code law	قانون مدنی
۷۷.....	Common law	قانون عمومی
۷۷.....	Criminal law	قانون کیفری
۷۸.....	Civil/tort law	قانون مدنی / جرمه
۷۸.....	Administrative/regulatory law	قانون اداری / قانون تنظیمی
۷۸.....	Customary law	قانون عرفی
۷۹.....	Religious law	قانون مذهبی
۷۹.....	Mixed Law	قانون مختلط
۷۹.....	Licensing and Intellectual Property	مجوز لیسانس و مالکیت معنوی
۷۹.....	Patent	ثبت اختراع
۸۰.....	Trade secret	راز تجارت
۸۱.....	Trademark	علائم تجاری
۸۱.....	Copyright	حق چاپ (کپی رایت)
۸۲.....	Software Piracy and Licensing Issues	دزدی نرم افزار و مسائل صدور مجوز نرم افزار
۸۳.....	Internal Protection	حفاظت داخلی
۸۳.....	Digital Rights Management (DRM)	مدیریت حقوق دیجیتال
۸۴.....	Import/Export Controls	کنترل‌های واردات / صادرات
۸۴.....	Trans-Border Data Flow	جریان اطلاعات بین مرزی
۸۵.....	Privacy	حریم خصوصی

۸۵.....	اطلاعات شناسایی شخصی (PII) Personally Identifiable Information
۸۶.....	قوانین و مقررات Laws and Regulations
۸۷.....	قانون Sarbanes-Oxley (SOX)
۸۷.....	قانون مسئولیت پذیری بیمه درمانی قابل حمل
۸۷.....	قانون ۱۹۹۹ Gramm-Leach-Bliley (GLBA)
۸۸.....	قانون کلاهبرداری و سوء استفاده رایانه‌ای (CFAA) Computer Fraud and Abuse Act
۸۸.....	قانون حفظ حریم خصوصی فدرال Federal Privacy Act of ۱۹۷۴
۸۸.....	قانون نظارت بر اطلاعات فدرال (FISA) Federal Intelligence Surveillance Act of ۱۹۷۸
۸۹.....	قانون حفاظت از ارتباطات الکترونیکی (ECPA) of Electronic Communications Privacy Act
۸۹.....	قانون امنیت رایانه Computer Security Act of ۱۹۸۷
۸۹.....	دستورالعمل صدور احکام فدرال ایالات متحده سال ۱۹۹۱ United States Federal Sentencing
۸۹.....	Guidelines of
۸۹.....	قانون کمک‌های ارتباطی برای اجرای قانون ۱۹۹۴ (CALEA)
۹۰.....	قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی
۹۰.....	بازل دوم Basel II
۹۰.....	قانون مدیریت امنیت اطلاعات فدرال ۲۰۰۲ (FISMA)
۹۰.....	قانون جاسوسی اقتصادی سال ۱۹۹۶ Economic Espionage Act of ۱۹۹۶
۹۱.....	قانون PATRIOT آمریکا
۹۱.....	قانون تطبیق بهداشت و درمان و آموزش ۲۰۱۰
۹۱.....	مسائل مربوط به حریم خصوصی کارکنان و انتظارات حریم خصوصی
۹۲.....	اتحادیه اروپا European Union
۹۳.....	نقض داده‌ها Data Breaches
۹۳.....	اخلاق حرفه‌ای Professional Ethics
۹۳.....	اصول اخلاقی (ISC) ۲ Code of Ethics
۹۴.....	موسسه اخلاق رایانه Computer Ethics Institute
۹۴.....	انجمن معماری اینترنت Internet Architecture Board
۹۵.....	اخلاق سازمانی Organizational Ethics
۹۵.....	مستندات امنیتی Security Documentation
۹۶.....	سیاست‌ها Policies

سیاست امنیتی سازمان	Organizational Security Policy	۹۷
سیاست امنیتی سیستم خاص	System-Specific Security Policy	۹۸
سیاست امنیتی با موضوع خاص	Issue-Specific Security Policy	۹۸
دسته بندی‌های سیاست	Policy Categories	۹۸
استانداردها	Standards	۹۹
خط مبنا	Baselines	۹۹
دستورالعمل	Guidelines	۹۹
رویه‌ها	Procedures	۹۹
تداوم کسب و کار	Business Continuity	۱۰۰
تداوم کسب و کار و مفاهیم بهبود فاجعه	Business Continuity and Disaster Recovery Concepts	۱۰۰
اختلالات	Disruptions	۱۰۱
فاجعه	Disasters	۱۰۱
بهبود فاجعه و برنامه رفع فاجعه (DRP)	Disaster Recovery and the Disaster Recovery Plan (DRP)	۱۰۲
برنامه ریزی مداوم و طرح تداوم کسب و کار		۱۰۳
تجزیه و تحلیل تاثیر کسب و کار	Business Impact Analysis (BIA)	۱۰۳
برنامه اضطراری	Contingency Plan	۱۰۳
دسترسی	Availability	۱۰۴
قابلیت اطمینان	Reliability	۱۰۴
دامنه و طرح پروژه	Project Scope and Plan	۱۰۴
مولفه‌های پرسنلی	Personnel Components	۱۰۵
محدوده پروژه	Project Scope	۱۰۵
مراحل پیوستگی کسب و کار	Business Continuity Steps	۱۰۶
توسعه تجزیه و تحلیل تاثیرات کسب و کار	Business Impact Analysis Development	۱۰۷
شناسایی فرآیندها و منابع بحرانی	Identify Critical Processes and Resources	۱۰۷
شناسایی اثرات خرابی، و برآورد یا تخمین خرابی	Identify Outage Impacts, and Estimate	۱۰۸
Downtime		۱۰۸
شناسایی منابع مورد نیاز	Identify Resource Requirements	۱۰۹
شناسایی اولویت‌های بازیابی	Identify Recovery Priorities	۱۰۹

۱۱۰.....	Recoverability	قابلیت بازیابی
۱۱۰.....	Fault Tolerance	تحمل خطا
۱۱۰.....	Personnel Security Policies	سیاست‌های امنیتی پرسنل
۱۱۰.....	Employment Candidate Screening	غربالگری کاندید برای اشتغال
۱۱۲.....	Employment Agreement and Policies	توافق نامه و سیاست‌های کاری
۱۱۳.....	Employment Termination Policies	خط مشی‌ها یا سیاست‌های خاتمه کاری
۱۱۳.....	Vendor, Consultant, and Contractor Controls	فروشنده، مشاور و کنترل پیمانکار
۱۱۴.....	Compliance	انطباق
۱۱۴.....	Privacy	حریم خصوصی
۱۱۴.....	Risk Management Concepts	مفاهیم مدیریت ریسک
۱۱۷.....	Risk Management Policy	سیاست مدیریت ریسک
۱۱۷.....	Risk Management Team	تیم مدیریت ریسک
۱۱۷.....	Risk Analysis Team	تیم تحلیل ریسک
۱۱۸.....	Risk Assessment	ارزیابی ریسک
۱۲۰.....	(ملموس / نا ملموس)	هزینه‌ها و ارزش اطلاعات و دارایی
۱۲۰.....	Identify Threats and Vulnerabilities	شناسایی تهدیدها و آسیب پذیری‌ها
۱۲۱.....	Risk Assessment/Analysis	ارزیابی ریسک / تجزیه و تحلیل
۱۲۱.....	Quantitative Risk Analysis	تجزیه و تحلیل ریسک کمی
۱۲۲.....	Qualitative Risk Analysis	تجزیه و تحلیل ریسک کیفی
۱۲۳.....	Countermeasure (Safeguard) Selection	اقدام متقابل (حفاظت) منتخب
۱۲۴.....	Total Risk Versus Residual Risk	ریسک کامل در مقابل ریسک باقی مانده
۱۲۵.....	Handling Risk	اداره کردن ریسک
۱۲۵.....	Implementation	پیاده سازی
۱۲۶.....	Access Control Categories	طبقه بندی کنترل دسترسی
۱۲۶.....	Compensative	جبران کننده
۱۲۶.....	Corrective	تصحیح کننده
۱۲۷.....	Detective	کاراگاه
۱۲۷.....	Deterrent	مهار (بازدارنده)
۱۲۷.....	Directive	دستورالعمل
۱۲۷.....	Preventive	پیشگیرانه

۱۲۸.....	Recovery	بازیابی
۱۲۸.....	Access Control Types	انواع کنترل دسترسی
۱۳۲.....	Control Assessment, Monitoring, and Measurement	ارزیابی کنترل، نظارت و اندازه گیری
۱۳۲.....	Reporting and Continuous Improvement	گزارش و بهبود مستمر
۱۳۳.....	Risk Frameworks	چارچوب‌های ریسک
۱۳۳.....	Threat Modeling	مدل سازی تهدید
۱۳۴.....	Identifying Threats	شناسایی تهدیدات
۱۳۵.....		بازیگران داخلی
۱۳۵.....	External actors	بازیگران خارجی
۱۳۶.....	Potential Attacks	حمله‌های بالقوه
۱۳۷.....	Remediation Technologies and Processes	فرایندها و فن آوری‌های ترمیم
۱۳۷.....	Security Risks in Acquisitions	ریسک‌های امنیتی در اکتساب
۱۳۸.....	Hardware, Software, Services	سخت افزار، نرم افزار، خدمات
۱۳۸.....	Third Party	شخص ثالث
۱۳۹.....	Onsite Assessment	ارزیابی در محل
۱۳۹.....	Document Exchange/Review	بررسی / تبادل اسناد
۱۳۹.....	Process/Policy Review	بررسی سیاست / فرآیند
۱۳۹.....	Other Third-Party Governance Issues	سایر موارد مربوط به حاکمیت شخص ثالث
۱۴۰.....	Minimum Security Requirements	حداقل الزامات امنیتی
۱۴۰.....	Minimum Service-Level Requirements	حداقل الزامات سطح سرویس
۱۴۱.....	Security Education, Training, and Awareness	آموزش امنیت، پرورش و آگاهی
۱۴۱.....	Levels Required	سطح مورد نیاز
۱۴۲.....	Periodic Review	بررسی دوره‌ای
۱۴۳.....	فصل ۲: امنیت دارایی (Asset Security)	
۱۴۵.....	Asset Security Concepts	مفاهیم امنیت دارایی
۱۴۵.....	Data policy	سیاست داده‌ها
۱۴۷.....	Roles and Responsibilities	نقش‌ها و مسئولیت‌ها
۱۴۷.....	Data Owner	صاحب داده (مالک داده)
۱۴۷.....	Data Custodian	نگهبان داده
۱۴۸.....	Data Quality	کیفیت داده

۱۴۹.....	Data Documentation and Organization	سازماندهی و مستندسازی داده‌ها
۱۵۰.....	Classify Information and Assets	طبقه‌بندی اطلاعات و دارایی‌ها
۱۵۱.....	Sensitivity and Criticality	حساسیت و بحران
۱۵۲.....	Commercial Business Classifications	طبقه‌بندی کسب و کار تجاری
۱۵۲.....	Military and Government Classifications	طبقه‌بندی نظامی و دولتی
۱۵۳.....	Information Life Cycle	چرخه عمر اطلاعات
۱۵۵.....	Databases	پایگاه داده‌ها
۱۵۵.....	(DBMS Architecture and Models) DBMS	معماری و مدل‌های DBMS
۱۵۷.....	Database Interface Languages	زبانهای واسطه پایگاه داده
۱۵۸.....	Data Warehouses and Data Mining	انبار داده‌ها و داده کاوی
۱۵۹.....	Database Maintenance	نگهداری پایگاه داده
۱۵۹.....	Database Threats	تهدیدات پایگاه داده
۱۶۰.....	Database Views	مشاهدات پایگاه اطلاعاتی
۱۶۰.....	Database Locks	قفل‌های پایگاه داده
۱۶۰.....	Polyinstantiation	چند منظوره
۱۶۱.....	OLTP ACID	تست
۱۶۱.....	Data Audit	ممیزی داده‌ها
۱۶۲.....	Asset Ownership	مالکیت دارایی
۱۶۲.....	Data Owners	صاحبان داده (مالکان داده)
۱۶۳.....	System Owners	مالکان سیستم
۱۶۳.....	Business/Mission Owners	صاحبان مأموریت / کسب و کار
۱۶۴.....	Asset Management	مدیریت دارایی
۱۶۴.....	Redundancy and Fault Tolerance	افزونگی و تحمل خطا
۱۶۵.....	Backup and Recovery Systems	سیستم‌های پشتیبان‌گیری و بازیابی
۱۶۵.....	Identity and Access Management	هویت و مدیریت دسترسی
۱۷۰.....	SAN	
۱۷۱.....	NAS	
۱۷۱.....	HSM	
۱۷۲.....	Network and Resource Management	مدیریت شبکه و منابع
۱۷۳.....	Asset Privacy	حریم خصوصی دارایی

۱۷۷.....	Data Retention	حفظ داده‌ها
۱۷۸.....	Data Security and Controls	کنترل‌ها و امنیت داده
۱۸۷.....	Asset Handling Requirements	الزامات مدیریت دارایی
۱۸۷.....	Marking, Labeling, and Storing	علامت گذاری، برچسب زدن و ذخیره سازی
۱۸۷.....	Destruction	تخریب
۱۸۹.....	(Security Engineering)	فصل ۳: مهندسی امنیت (Security Engineering)
۱۹۲.....	Engineering Using Secure Design Principles	مهندسی با استفاده از اصول طراحی امن
۱۹۶.....	Security Model Concepts	مفاهیم مدل امنیتی
۱۹۶.....	Confidentiality, Integrity, Availability	محرمانه بودن، یکپارچگی و در دسترس بودن
۱۹۷.....	Security Modes	حالت‌های امنیتی
۱۹۷.....	Dedicated Security Mode	حالت امنیتی اختصاصی
۱۹۷.....	System High Security Mode	حالت امنیت بالای سیستم
۱۹۷.....	Compartmented Security Mode	حالت امنیتی تقسیم شده
۱۹۸.....	Multilevel Security Mode	حالت امنیتی چند سطحی
۱۹۸.....	Assurance	تضمین
۱۹۹.....	Defense in Depth	دفاع در عمق
۱۹۹.....	Security Model Types	انواع مدل امنیتی
۱۹۹.....		انواع مدل امنیتی
۱۹۹.....	State Machine Models	حالت‌های مدل ماشین
۲۰۰.....	Multilevel Lattice Models	مدل‌های شبکه چند سطحی
۲۰۰.....	Matrix-Based Models	مدل‌های مبتنی بر ماتریس
۲۰۱.....	Non-inference Models	مدل‌های غیر استنباطی
۲۰۱.....	Information Flow Models	مدل‌های جریان اطلاعات
۲۰۲.....	Security Models	مدل‌های امنیتی
۲۰۲.....	Bell-LaPadula	مدل Bell-LaPadula
۲۰۴.....	Biba	مدل Biba
۲۰۴.....	Clark-Wilson Integrity Model	مدل یکپارچگی کلارک-ویلسون
۲۰۵.....	Lipner	مدل Lipner
۲۰۶.....	Brewer-Nash (Chinese Wall) Model	مدل Brewer-Nash (دیوار چین)
۲۰۶.....	Graham-Denning Model	

۲۰۶.....	Harrison-Ruzzo-Ullman مدل
۲۰۷.....	System Architecture Steps مراحل معماری سیستم
۲۰۸.....	Computing Platforms (پلتفرم محاسباتی) بسترهای رایانشی
۲۰۸.....	Mainframe/Thin Clients
۲۰۸.....	Distributed Systems سیستم‌های توزیع شده
۲۰۹.....	Middleware میان افزار
۲۰۹.....	Embedded Systems سیستم‌های تعبیه شده
۲۰۹.....	Mobile Computing محاسبات (رایانش) سیار
۲۱۰.....	Virtual Computing محاسبات مجازی
۲۱۰.....	Security Services خدمات امنیتی
۲۱۲.....	System Components مولفه‌های سیستم
۲۱۲.....	CPU and Multiprocessing پردازنده و چند پردازشی
۲۱۳.....	Memory and Storage حافظه و ذخیره سازی
۲۱۶.....	Operating Systems سیستم‌های عامل
۲۱۷.....	Multitasking چند وظیفه‌ای
۲۱۹.....	Memory Management مدیریت حافظه
۲۱۹.....	System Security Evaluation Models مدل‌های ارزیابی امنیت سیستم
۲۱۹.....	TCSEC
۲۲۰.....	Rainbow Series سری‌های رنگین کمان
۲۲۰.....	Orange Book کتاب نارنجی
۲۲۳.....	Red Book کتاب قرمز
۲۲۳.....	ITSEC
۲۲۵.....	Common Criteria معیارهای مشترک
۲۲۶.....	Security Implementation Standards استانداردهای پیاده سازی امنیت
۲۲۷.....	ISO/IEC 27001
۲۲۸.....	ISO/IEC 27002
۲۲۹.....	(PCI-DSS) استاندارد امنیت داده‌های صنعت کارت پرداخت
۲۲۹.....	Controls and Countermeasures کنترل‌ها و اقدامات متقابل
۲۳۳.....	Certification and Accreditation صدور گواهینامه و اعتبارسنجی
۲۳۴.....	Security Architecture Maintenance تعمیر و نگهداری معماری امنیتی

Vulnerabilities of Security	آسیب پذیری‌های معماری امنیتی، طرح‌ها و عناصر راه حل
۲۳۵.....	Architectures, Designs, and Solution Elements
۲۳۵.....	Client-Based مبتنی بر مشتری
۲۳۷.....	Server-Based مبتنی بر سرور
۲۳۷.....	Data Flow Control کنترل جریان داده
۲۳۷.....	Database Security امنیت پایگاه داده
۲۴۲.....	Peer-to-Peer Computing رایانش هم‌تا
۲۴۲.....	Large-Scale Parallel Data Systems سیستم‌های داده موازی با مقیاس بزرگ
۲۴۳.....	Cryptographic Systems سیستم‌های رمزنگاری
۲۴۳.....	Industrial Control Systems سیستم‌های کنترل صنعتی
۲۴۴.....	Vulnerabilities in Web-Based Systems آسیب پذیری در سیستم‌های مبتنی بر وب
۲۴۵.....	Maintenance Hooks قلاب‌های نگهدارنده
۲۴۶.....	Time-of-Check/Time-of-Use Attacks حملات زمان بررسی / زمان استفاده
۲۴۶.....	Web-Based Attacks حملات مبتنی بر وب
۲۴۶.....	XML
۲۴۷.....	SAML
۲۴۷.....	OWASP
۲۴۷.....	Vulnerabilities in Mobile Systems آسیب پذیری در سیستم‌های سیار
۲۵۱.....	آسیب پذیری در دستگاه‌های تعبیه شده و سیستم‌های سایبر- فیزیکی
۲۵۲.....	Cryptography رمزنگاری
۲۵۳.....	Cryptography Concepts مفاهیم رمزنگاری
۲۵۵.....	Cryptographic Life Cycle چرخه عمر رمزنگاری
۲۵۶.....	تاریخچه رمزنگاری
۲۶۰.....	لوسیفر توسط IBM
۲۶۰.....	Cryptosystem Features ویژگی‌های سیستم رمزنگاری
۲۶۳.....	انواع رمزنگاری
۲۶۶.....	Block Ciphers رمزهای بلوک
۲۶۹.....	Substitution Ciphers رمزهای جایگزینی
۲۶۹.....	One-Time Pads پدهای یک‌زمانه
۲۷۰.....	Steganography پنهان سازی

۲۷۵.....	سه گانه DES, DES 3 و حالتها
۲۷۸.....	الگوریتم‌های نامتقارن Asymmetric Algorithms
۲۸۱.....	زیرساخت کلید عمومی Public Key Infrastructure
۲۸۳.....	OCSP
۲۸۳.....	گواهینامه‌ها Certificates
۲۸۴.....	لیست ابطال مجوزها Certificate Revocation List (CRL)
۲۸۵.....	گواهینامه متقابل Cross-Certification
۲۸۵.....	شیوه‌های عملیات مدیریت کلید Key Management Practices
۲۹۵.....	امضاهای دیجیتال Digital Signatures
۲۹۶.....	مدیریت حقوق دیجیتال Digital Rights Management (DRM)
۲۹۷.....	یکپارچگی پیام Message Integrity
۲۹۸.....	هش کردن Hashing
۳۰۲.....	کد تصدیق پیام Message Authentication Code
۳۰۳.....	Salting
۳۰۴.....	حملات تجزیه و تحلیل رمزنگاری Cryptanalytic Attacks
۳۰۹.....	تهدیدات جغرافیایی Geographical Threats
۳۰۹.....	تهدیدات داخلی در مقابل تهدیدات خارجی Internal Versus External Threats
۳۱۰.....	تهدیدهای طبیعی Natural Threats
۳۱۰.....	طوفان / طوفان گرمسیری Hurricanes/Tropical Storms
۳۱۰.....	گردبادها Tornadoes
۳۱۱.....	زلزله‌ها Earthquakes
۳۱۱.....	سیل Floods
۳۱۱.....	تهدیدات سیستم System Threats
۳۱۱.....	برق Electrical
۳۱۲.....	ارتباطات Communications
۳۱۳.....	خدمات رفاهی Utilities
۳۱۳.....	تهدیدات ناشی از انسان Human-Caused Threats
۳۱۷.....	طراحی سایت و تاسیسات Site and Facility Design
۳۱۸.....	مدل دفاعی لایه‌ای Layered Defense Model
۳۱۸.....	CPTED

۳۱۹.....	Physical Security Plan	طرح امنیت فیزیکی
۳۱۹.....	Deter Criminal Activity	فعالیت جنایی بازدارنده
۳۲۰.....	Delay Intruders	تأخیر مزاحمان
۳۲۰.....	Detect Intruders	تشخیص مزاحمان
۳۲۰.....	Assess Situation	ارزیابی وضعیت
۳۲۰.....	Respond to Intrusions and Disruptions	واکنش به اغتشاشات و اختلالات
۳۲۱.....	Facility Selection Issues	مسائل مربوط به انتخاب تاسیسات
۳۲۱.....	Visibility	میدان دید
۳۲۱.....	Surrounding Area and External Entities	محیط اطراف و اشخاص خارجی
۳۲۱.....	Accessibility	دسترسی
۳۲۲.....	Construction	ساخت و ساز
۳۲۳.....	Internal Compartments	محفظه داخلی
۳۲۳.....	Computer and Equipment Rooms	اتاق‌های تجهیزات و رایانه
۳۲۳.....	Building and Internal Security	ساختمان و امنیت داخلی
۳۲۴.....	Doors	درب‌ها
۳۲۴.....	Door Lock Types	انواع قفل درب
۳۲۵.....	Turnstiles and Mantraps	درب کنترل تردد و مانتراپ (تله آدمگیر)
۳۲۵.....	Locks	قفله‌ها
۳۲۷.....	Biometrics	بیومتریک
۳۲۷.....	Glass Entries	ورودی‌های شیشه‌ای
۳۲۸.....	Visitor Control	کنترل بازدید کنندگان
۳۲۸.....	Equipment Rooms	اتاق تجهیزات
۳۲۹.....	Work Areas	مناطق کار
۳۲۹.....	Secure Data Center	مرکز داده امن
۳۲۹.....	Restricted Work Area	محدوده منطقه کاری
۳۲۹.....	Media Storage Facilities	مرکز رسانه‌های ذخیره سازی
۳۳۰.....	Evidence Storage	ذخیره سازی مدارک
۳۳۰.....	Environmental Security	امنیت محیطی
۳۳۰.....	Fire Protection	حفاظت در مقابل آتش
۳۳۱.....	Fire Detection	شناسایی آتش

۳۳۱.....	مهار آتش Fire Suppression
۳۳۳.....	Power Supply
۳۳۳.....	انواع خاموشی
۳۳۳.....	Preventive Measures اقدامات پیشگیرانه
۳۳۴.....	HVAC
۳۳۴.....	نشت آب و جاری شدن سیل Water Leakage and Flooding
۳۳۵.....	Environmental Alarms هشدارهای محیطی
۳۳۵.....	Equipment Security امنیت تجهیزات
۳۳۹.....	فصل ۴: ارتباطات و امنیت شبکه (Communication and Network Security)
۳۴۱.....	اصول طراحی شبکه امن
۳۴۱.....	OSI مدل
۳۴۲.....	Application Layer لایه کاربردی
۳۴۳.....	Presentation Layer لایه نمایشی
۳۴۳.....	Session Layer لایه جلسه
۳۴۴.....	Transport Layer لایه انتقال
۳۴۴.....	Network Layer لایه شبکه
۳۴۴.....	Data Link Layer لایه پیوند داده
۳۴۵.....	Physical Layer لایه فیزیکی
۳۴۶.....	TCP / IP مدل
۳۴۷.....	Application Layer لایه کاربردی
۳۵۱.....	Internet Layer لایه اینترنت
۳۵۲.....	Link Layer لایه پیوند
۳۵۳.....	Encapsulation کپسوله سازی
۳۵۴.....	IP Networking
۳۵۴.....	TCP / UDP پورتهای مشترک
۳۵۶.....	IPv4
۳۵۸.....	IP کلاس
۳۵۹.....	Public Versus Private IP Addresses آدرسهای عمومی در مقابل آدرسهای خصوصی
۳۶۰.....	Network address translation (NAT) ترجمه آدرس شبکه
۳۶۱.....	IPv6 در مقابل IPv4

۳۶۱		آدرس دهی MAC
۳۶۲		انتقال شبکه Network Transmission
۳۶۲		آنالوگ در مقابل دیجیتال Analog Versus Digital
۳۶۳		ناهمگام در مقابل همگام Asynchronous Versus Synchronous
۳۶۴		باند گسترده در مقابل پهنای باند Broadband Versus Baseband
۳۶۵		Broadcast, Multicast, Unicast
۳۶۶		سیم در مقابل بی سیم Wired Versus Wireless
۳۶۷		انواع شبکه Network Types
۳۶۷		LAN
۳۶۷		اینترانت Intranet
۳۶۸		اکسترانت Extranet
۳۶۸		MAN
۳۶۹		WAN
۳۶۹		پروتکل ها و خدمات Protocols and Services
۳۶۹		ARP
۳۷۱		DHCP
۳۷۱		DNS
۳۷۲		FTP, FTPS, SFTP
۳۷۳		HTTP, HTTPS, SHTTP
۳۷۳		ICMP
۳۷۳		IMAP
۳۷۴		LDAP
۳۷۴		NAT
۳۷۴		NetBIOS
۳۷۴		NFS
۳۷۵		PAT
۳۷۵		POP
۳۷۵		CIFS / SMB
۳۷۵		SMTP
۳۷۵		SNMP

۳۷۶	Multi-Layer Protocols	پروتکل‌های چند لایه
۳۷۷	Converged Protocols	پروتکل‌های همگرا
۳۷۷	FCoE	
۳۷۸	MPLS	
۳۷۹	VoIP	
۳۷۹	 Internet Small Computer System Interface (iSCSI)	
۳۸۰	Wireless Networks	شبکه‌های بی سیم یا وایرلس
۳۸۱	802,11	تکنیک‌های 802,11
۳۸۳	 Satellites	ماهواره‌ها
۳۸۳	 WLAN	ساختار WLAN
۳۸۳	Access Point	نقطه دسترسی
۳۸۴	 SSID	
۳۸۴	Infrastructure Mode Versus Ad Hoc Mode	وضعیت زیرساخت در مقابل وضعیت Ad Hoc
۳۸۴	 WLAN	استانداردهای WLAN
۳۸۶	 Bluetooth	بلوتوث
۳۸۶	 Infrared	مادون قرمز
۳۸۷	 Near Field Communication (NFC)	ارتباط میدانی نزدیک (NFC)
۳۸۷	WLAN Security	
۳۸۷	Open System Authentication	احراز هویت سیستم باز
۳۸۷	 Shared Key Authentication	احراز هویت کلید مشترک
۳۸۸	WEP	
۳۸۸	 WPA	
۳۸۹	WPA2	
۳۸۹	 Personal Versus Enterprise	شخصی در مقابل سازمانی
۳۸۹	SSID	بخش SSID
۳۸۹	 MAC	فیلتر MAC
۳۹۰	 Communications Cryptography	رمزنگاری ارتباطات
۳۹۱	Email Security	امنیت ایمیل
۳۹۱	 PGP	
۳۹۳	 Quantum Cryptography	رمزنگاری کوانتومی

۳۹۳.....	امنیت اینترنت Internet Security
۳۹۴.....	دسترسی از راه دور Remote access
۳۹۴.....	SSL / TLS
۳۹۵.....	HTTP, HTTPS, S-HTTP
۳۹۵.....	تنظیم SET
۳۹۵.....	Cookies
۳۹۶.....	SSH
۳۹۶.....	IPsec
۳۹۷.....	مؤلفه‌های شبکه امن
۳۹۸.....	سخت افزار Hardware
۳۹۸.....	دستگاه‌های شبکه Network Devices
۳۹۸.....	Patch Panel
۳۹۸.....	مولتی پلکسر Multiplexer
۳۹۹.....	Telco Concentrator
۳۹۹.....	VPN Concentrator
۳۹۹.....	هاب Hub
۴۰۰.....	Repeater
۴۰۰.....	پل یا Bridge
۴۰۰.....	سوئیچ Switch
۴۰۱.....	سوئیچ لایه ۳ در مقابل لایه ۴
۴۰۱.....	VLAN ها
۴۰۲.....	مسیریاب (روتر) Router
۴۰۳.....	دروازه Gateway
۴۰۳.....	فایروال ها
۴۰۳.....	انواع فایروال
۴۰۶.....	معماری فایروال Firewall Architecture
۴۰۷.....	پروکسی سرورها Proxy Server
۴۰۸.....	PBX
۴۰۸.....	Honeypot ها
۴۰۹.....	سیستم تشخیص نفوذ IDS

۴۱۱.....	IPS
۴۱۲.....	نقطه دسترسی بی سیم Wireless Access Point
۴۱۲.....	دستگاه‌های سیار Mobile Devices
۴۱۲.....	مسیریابی شبکه Network Routing
۴۱۳.....	بردار مسافت، حالت پیوند، یا مسیریابی هیبریدی
۴۱۴.....	RIP
۴۱۵.....	OSPF
۴۱۵.....	Interior Gateway Routing Protocol (IGRP)
۴۱۵.....	Enhanced IGRP (EIGRP)
۴۱۵.....	VRRP
۴۱۶.....	IS-IS
۴۱۶.....	BGP
۴۱۶.....	رسانه انتقال Transmission Media
۴۱۶.....	کابل کشی Cabling
۴۱۷.....	کواکسیال Coaxial
۴۱۹.....	زوج بهم پیچ خورده Twisted Pair
۴۲۰.....	فیبر نوری Fiber optic
۴۲۲.....	توپولوژی‌های شبکه
۴۲۲.....	حلقه Ring
۴۲۳.....	Bus
۴۲۴.....	ستاره Star
۴۲۴.....	تار عنکبوتی یا Mesh
۴۲۵.....	Hybrid
۴۲۵.....	فن آوری‌های شبکه Network Technologies
۴۲۷.....	Token Ring 802.5
۴۲۸.....	FDDI
۴۲۹.....	روشهای بحث
۴۲۹.....	CSMA / CD در مقابل CSMA / CA
۴۳۰.....	دامنه‌های تصادم Collision Domains
۴۳۱.....	CSMA / CD

۴۳۲.....	CSMA / CA
۴۳۳.....	Token Passing عبور توکن
۴۳۴.....	Polling نظرسنجی
۴۳۴.....	WAN Technologies
۴۳۴.....	T خطوط
۴۳۵.....	E خطوط
۴۳۵.....	(SONET) OC خطوط
۴۳۶.....	CSU / DSU
۴۳۶.....	سوئیچ مدار در مقابل تعویض بسته
۴۳۶.....	Frame Relay رله فریم
۴۳۷.....	ATM
۴۳۷.....	X.25
۴۳۸.....	Switched Multimegabit Data Service تعویض سرویس داده مگا بیتی
۴۳۸.....	Point-to-Point Protocol (PPP) پروتکل نقطه به نقطه
۴۳۸.....	High-Speed Serial Interface (HSSI) واسط سریال پر سرعت
۴۳۹.....	PSTN (POTS, PBX)
۴۳۹.....	VoIP
۴۴۰.....	Network Access Control Devices دستگاههای دسترسی به شبکه
۴۴۱.....	Quarantine/Remediation قرنطینه / ترمیم
۴۴۲.....	فایروال ها / پروکسی ها
۴۴۲.....	Endpoint امنیت
۴۴۳.....	Content Distribution Networks شبکه‌های توزیع محتوا
۴۴۳.....	Secure Communication Channels کانال‌های ارتباطی امن
۴۴۴.....	Remote Meeting Technology فناوری جلسات از راه دور
۴۴۵.....	Instant Messaging پیام رسانی فوری
۴۴۵.....	Remote Connection Technologies فن آوری‌های اتصال از راه دور
۴۴۶.....	Dial-up
۴۴۷.....	ISDN
۴۴۷.....	DSL
۴۴۹.....	Cable کابل

۴۴۹.....	VPN
۴۵۳.....	TACACS + و RADIUS
۴۵۵.....	Remote Authentication Protocols پروتکل‌های احراز هویت از راه دور
۴۵۵.....	Telnet
۴۵۶.....	ورود به سیستم از راه دور، پوستره از راه دور، کپی از راه دور
۴۵۷.....	VPN:داینده صفحه نمایش (Scraper Screen VPN)
۴۵۷.....	Virtual Application/Desktop /اپلیکیشن مجازی دسکتاپ
۴۵۷.....	Telecommuting ارتباط از راه دور
۴۵۸.....	Virtualized Networks شبکه‌های مجازی
۴۵۸.....	Software-defined networking (SDN) شبکه تعریف شده نرم افزاری
۴۵۹.....	Virtual storage area network (VSAN) شبکه منطقه ذخیره سازی مجازی
۴۵۹.....	Guest Operating Systems سیستم عامل‌های مهمان
۴۶۰.....	Network Attacks حملات شبکه
۴۶۰.....	Cabling کابل کشی
۴۶۰.....	Noise نویز
۴۶۱.....	Attenuation تضعیف
۴۶۱.....	Crosstalk شکاف متقاطع
۴۶۱.....	Eavesdropping استراق سمع
۴۶۲.....	Network Component Attacks حملات مؤلفه شبکه
۴۶۲.....	Non-Blind Spoofing کلاهبرداری غیر جعلی
۴۶۲.....	Blind Spoofing کلاهبرداری جعلی
۴۶۳.....	Man-in-the-Middle Attack حمله انسان در وسط
۴۶۳.....	(MAC Flooding Attack) MAC حمله سیل
۴۶۴.....	ARP حمله
۴۶۴.....	ICMP حملات
۴۶۶.....	Traceroute Exploitation بهره برداری از ردیابی مسیر
۴۶۶.....	DNS حملات
۴۷۲.....	حملات دیگر

۴۷۵		(Identity and Access Management)	فصل ۵: هویت و مدیریت دسترسی
۴۷۷		Access Control Process	فرآیند کنترل دسترسی
۴۷۹		Physical and Logical Access to Assets	دسترسی فیزیکی و منطقی به دارایی
۴۸۱		Provisioning Life Cycle	ارائه چرخه عمر
۴۸۱		Information	اطلاعات
۴۸۱		Systems	سیستم‌ها
۴۸۲		Devices	دستگاه‌ها
۴۸۳		Facilities	تأسیسات
۴۸۳		Identification and Authentication Concepts	مفاهیم شناسایی و احراز هویت
۴۸۴			پنج عامل احراز هویت
۴۸۵		Knowledge Factors	عوامل دانش
۴۸۵		Identity and Account Management	هویت و مدیریت حساب
۴۸۶		Password Types and Management	انواع گذرواژه و مدیریت آن
۴۹۱		Ownership Factors	عوامل مالکیت
۴۹۱		Synchronous and Asynchronous Token	توکن همگام و ناهمگام
۴۹۱		Memory Cards	کارت‌های حافظه
۴۹۲		Smart Cards	کارت‌های هوشمند
۴۹۳		Characteristic Factors	عوامل مشخصه
۴۹۳		Physiological Characteristics	خصوصیات فیزیولوژیکی
۴۹۵		Behavioral Characteristics	خصوصیات رفتاری
۴۹۵		Biometric Considerations	ملاحظات بیومتریک
۴۹۸		Location Factors	عوامل موقعیت مکانی
۴۹۹		Time Factors	عوامل زمان
۴۹۹			شناسایی و اجرای احراز هویت
۵۰۲		Single Sign-on	اولین ورود یکپارچه
۵۰۳		Kerberos	
۵۰۶		Federated Identity Management	مدیریت هویت هم پیمان
۵۰۷		Security Domains	دامنه‌های امنیتی
۵۰۷		Session Management	مدیریت جلسه
۵۰۸		Registration and Proof of Identity	ثبت نام و اثبات هویت

۵۰۹.....	Credential Management Systems	سیستم‌های مدیریت اعتبارنامه
۵۱۰.....	Accountability	مسئولیت
۵۱۱.....	Auditing and Reporting	ممیزی و گزارشگیری
۵۱۳...	Identity as a Service (IDaaS) Implementation	هویت به عنوان یک سرویس پیاده سازی
۵۱۳....	Third-Party Identity Services Implementation	پیاده سازی خدمات هویت شخص ثالث
۵۱۴.....	Authorization Mechanisms	مکانیسم‌های مجوز
۵۱۴.....	Access Control Models	مدل‌های کنترل دسترسی
۵۱۸.....	Access Control Policies	سیاست‌های کنترل دسترسی
۵۱۹.....	Access Control Threats	تهدیدات کنترل دسترسی
۵۱۹.....	Dictionary Attack	حمله فرهنگ لغت
۵۲۰.....	Brute-Force	حمله بی رحمانه
	Prevent or Mitigate Access Control Threats	جلوگیری یا کاهش تهدیدات کنترل دسترسی
۵۲۵.....		

فصل ۶: ارزیابی و آزمون امنیت (Security Assessment and Testing) ۵۲۷

۵۲۹.....	Assessment and Testing Strategies	استراتژی‌های ارزیابی و آزمون
۵۲۹.....	Security Control Testing	آزمون کنترل امنیت
۵۲۹.....	Vulnerability Assessment	ارزیابی آسیب پذیری
۵۳۱.....	Penetration Testing	تست نفوذ
۵۳۳.....	log	بررسی‌های log
۵۳۹.....	Synthetic Transactions	تراکنش‌های مصنوعی
۵۴۰.....	Code Review and Testing	تست و بررسی کد
۵۴۱.....	Misuse Case Testing	تست حالت سوء استفاده
۵۴۱.....	Test Coverage Analysis	تجزیه و تحلیل پوشش تست
۵۴۲.....	Interface Testing	تست واسط
۵۴۲.....	Collect Security Process Data	داده‌های فرایند امنیت را جمع آوری کنید
۵۴۳.....	Account Management	مدیریت حساب
۵۴۴.....	Management Review	بررسی مدیریت
۵۴۵.....	Key Performance and Risk Indicators	شاخص‌های کلیدی عملکرد و ریسک
۵۴۶.....	Backup Verification Data	داده‌های تأیید نسخه پشتیبان
۵۴۶.....	Training and Awareness	آموزش و آگاهی

۵۴۶.....	Disaster Recovery and Business Continuity	بازیابی فاجعه و استمرار کسب و کار
۵۴۷.....	Analyze and Report Test Outputs	تجزیه و تحلیل و گزارش نتایج آزمون
۵۴۷.....	Internal and Third-Party Audits	ممیزی داخلی و شخص ثالث
۵۵۱.....	فصل ۷: عملیات امنیت (Security Operations)	
۵۵۴.....	Investigations	تحقیقات
۵۵۴.....	Forensic and Digital Investigations	تحقیقات دیجیتال و جرم شناسی رایانه‌ای
۵۵۶.....	Identify Evidence	شناسایی مدارک
۵۵۶.....	Preserve and Collect Evidence	حفظ و جمع آوری مدارک
۵۵۷.....	Examine and Analyze Evidence	بررسی و تجزیه و تحلیل مدارک
۵۵۷.....	Present Findings	یافته‌های حاضر
۵۵۸.....	Decide	تصمیم گیری
۵۵۹.....	Crime Scene	صحنه جرم
۵۶۰.....	MOM	
۵۶۰.....	Chain of Custody	زنجیره‌ای از توقیف
۵۶۱.....	Interviewing	مصاحبه
۵۶۱.....	Evidence	شواهد
۵۶۲.....	Types of Evidence	انواع شواهد
۵۶۴.....	Surveillance, Search, and Seizure	نظارت، جستجو و توقیف
۵۶۵.....	Media Analysis	تحلیل رسانه
۵۶۶.....	Software Analysis	تجزیه و تحلیل نرم افزار
۵۶۷.....	Network Analysis	تجزیه و تحلیل شبکه
۵۶۷.....	Hardware/Embedded Device Analysis	تجزیه و تحلیل دستگاه تعبیه شده / سخت افزار
۵۶۸.....	Investigation Types	انواع تحقیق
۵۶۸.....	Operations	عملیات
۵۶۸.....	Criminal	جنایی
۵۶۹.....	Civil	مدنی
۵۶۹.....	Regulatory	نظارتی
۵۶۹.....	eDiscovery	اکتشاف الکترونیکی
۵۷۰.....	Logging and Monitoring Activities	فعالیت‌های log و نظارت
۵۷۰.....	Audit and Review	ممیزی و بررسی

۵۷۱.....	Intrusion Detection and Prevention	تشخیص نفوذ و پیشگیری
۵۷۱.....	Security Information and Event Management (SIEM)	مدیریت رخداد و اطلاعات امنیتی
۵۷۲.....	Continuous Monitoring	نظارت مداوم
۵۷۲.....	Egress Monitoring	نظارت بر خروج
۵۷۳.....	Resource Provisioning	تأمین منابع
۵۷۳.....	Asset Inventory	فهرست موجودی دارایی
۵۷۵.....	Configuration Management	مدیریت پیکربندی
۵۷۶.....	Physical Assets	دارایی‌های فیزیکی
۵۷۷.....	Virtual Assets	دارایی‌های مجازی
۵۷۷.....	Cloud Assets	دارایی‌های ابری
۵۷۸.....	Applications	برنامه‌های کاربردی (اپلیکیشن‌ها)
۵۷۸.....	Security Operations Concepts	مفاهیم عملیات امنیتی
۵۷۸.....	Need to Know/Least Privilege	نیاز به دانستن / حداقل امتیاز
۵۷۹.....	Managing Accounts, Groups, and Roles	مدیریت حساب‌ها، گروه‌ها و نقش‌ها
۵۸۰.....	Separation of Duties	تفکیک وظایف
۵۸۰.....	Job Rotation	چرخش شغل
۵۸۱.....	Sensitive Information Procedures	رویه‌های حساس اطلاعات
۵۸۱.....	Record Retention	حفظ رکورد
۵۸۲.....	Monitor Special Privileges	نظارت بر امتیازات ویژه
۵۸۲.....	Information Life Cycle	چرخه عمر اطلاعات
۵۸۲.....	Service-Level Agreements	توافقاتنامه‌های سطح خدمات
۵۸۳.....	Resource Protection	حفاظت از منابع
۵۸۳.....	Protecting Tangible and Intangible Assets	محافظت از دارایی‌های ملموس و ناملموس
۵۸۳.....	Facilities	تاسیسات
۵۸۴.....	Hardware	سخت افزار
۵۸۵.....	Software	نرم افزار
۵۸۵.....	Information Assets	دارایی‌های اطلاعاتی
۵۸۵.....	Asset Management	مدیریت دارایی
۵۸۶.....	Redundancy and Fault Tolerance	افزونگی و تحمل خطا
۵۸۶.....	Backup and Recovery Systems	پشتیبان‌گیری و بازیابی سیستم‌ها

۵۸۷.....	Identity and Access Management	هویت و مدیریت دسترسی
۵۸۷.....	Media Management	مدیریت رسانه
۵۸۷.....	Redundant Array of Independent Disks (RAID)	آرایه‌های اضافی دیسک‌های مستقل
۵۹۲.....	SAN	
۵۹۲.....	NAS	
۵۹۳.....	HSM	
۵۹۴.....	Media History	تاریخچه رسانه
۵۹۴.....	Media Labeling and Storage	برچسب زدن رسانه‌ها و ذخیره سازی
۵۹۵.....	Sanitizing and Disposing of Media	پاکسازی و دفع رسانه
۵۹۵.....	Network and Resource Management	مدیریت شبکه و منابع
۵۹۶.....	Incident Management	مدیریت حادثه
۵۹۷.....	Event Versus Incident	رخداد در مقابل حادثه
۵۹۷.....	Incident Response Team and Incident Investigations	تیم واکنش به حادثه و تحقیقات حادثه
۵۹۸.....	Rules of Engagement, Authorization, and Scope	قواعد اشتغال، مجوز و حوزه
۵۹۸.....	Incident Response Procedures	روشهای واکنش حادثه
۵۹۹.....	Incident Response Management	مدیریت واکنش حادثه
۶۰۲.....	Preventive Measures	اقدامات پیشگیرانه
۶۰۲.....	Clipping Levels	سطح برش
۶۰۲.....	Deviations from Standards	انحراف از استاندارد
۶۰۲.....	Unusual or Unexplained Events	رخدادهای غیرمعمول یا غیر قابل توضیح
۶۰۳.....	Unscheduled Reboots	راه اندازی مجدد برنامه ریزی نشده
۶۰۳.....	Unauthorized Disclosure	افشای غیر مجاز
۶۰۳.....	Trusted Recovery	بازیابی مورد اعتماد
۶۰۳.....	Trusted Paths	مسیرهای قابل اعتماد
۶۰۴.....	Input/Output Controls	کنترل‌های ورودی / خروجی
۶۰۴.....	System Hardening	سخت شدن سیستم
۶۰۵.....	Vulnerability Management Systems	سیستم‌های مدیریت آسیب پذیری
۶۰۵.....	IDS / IPS	
۶۰۵.....	Firewalls	فایروال‌ها(دیوار آتش)

۶۰۶	لیست سفید / لیست سیاه Whitelisting/Blacklisting
۶۰۶	خدمات امنیت شخص ثالث Third-Party Security Services
۶۰۶	Sandboxing
۶۰۷	Honeypots / Honeynets
۶۰۷	ضد بدافزار / آنتی ویروس Anti-malware/Antivirus
۶۰۷	مدیریت پچ Patch Management
۶۰۸	تغییر فرآیندهای مدیریت Change Management Processes
۶۰۹	استراتژی‌های بازیابی Recovery Strategies
۶۰۹	سیستم‌های افزونه، تاسیسات و قدرت Redundant Systems, Facilities, and Power
۶۱۰	فن آوری‌های تحمل خطا Fault-Tolerance Technologies
۶۱۰	بیمه Insurance
۶۱۱	نسخه پشتیبان از داده‌ها Data Backup
۶۱۱	تشخیص و سرکوب آتش Fire Detection and Suppression
۶۱۱	در دسترس بودن زیاد High Availability
۶۱۲	کیفیت خدمات Quality of Service
۶۱۳	مقاومت سیستم System Resilience
۶۱۳	ایجاد استراتژی‌های بازیابی Create Recovery Strategies
۶۱۴	طبقه بندی اولویت‌های بازیابی دارایی Categorize Asset Recovery Priorities
۶۱۵	بازیابی فرآیند کسب و کار Business Process Recovery
۶۱۵	ترمیم تأسیسات Facility Recovery
۶۱۸	سایتهای افزونه Redundant sites
۶۱۹	تهیه و بازیابی فناوری Supply and Technology Recovery
۶۲۲	بهبود محیط کاربر User Environment Recovery
۶۲۳	بازیابی داده Data Recovery
۶۲۳	طرح‌های کلی و انواع نسخه پشتیبان از داده‌ها Data Backup Types and Schemes
۶۲۷	پشتیبان گیری الکترونیکی Electronic Backup
۶۲۸	آموزش پرسنل Training Personnel
۶۲۹	بهبود فاجعه Disaster Recovery
۶۳۳	طرح‌های تست بازیابی Testing Recovery Plans
۶۳۴	تست خواندن Read-Through Test

۶۳۴	 Checklist Test	تست چک لیست
۶۳۴	 Table-Top Exercise	اجرای جدول سطح بالا
۶۳۵	 Structured Walk-Through Test	تست بررسی ساخت یافته
۶۳۵	 Simulation Test	تست شبیه سازی
۶۳۵	 Parallel Test	تست موازی
۶۳۵	 Full-Interruption Test	تست وقفه کامل
۶۳۵	 Functional Drill	مانور عملکرد
۶۳۶	 Evacuation drill	مانور تخلیه
۶۳۶	 Business Continuity Planning and Exercises	اجرا و برنامه ریزی ادامه کسب و کار
۶۳۶	 Physical Security	امنیت فیزیکی
۶۳۷	 Perimeter Security	امنیت محیط
۶۳۷	 Gates and Fences	دروازه و نرده
۶۳۸	 Barriers (Bollards)	موانع (بولاردها)
۶۳۸	 Fences	نرده‌ها (حصارها)
۶۳۹	 Gates	دروازه
۶۳۹	 Walls	دیوارها
۶۳۹	 Perimeter Intrusion Detection	تشخیص نفوذ محیطی
۶۴۰	 Infrared Sensors	سنسورهای مادون قرمز
۶۴۰	 Electromechanical Systems	سیستم‌های الکترومکانیکی
۶۴۰	 Photoelectric Systems	سیستم‌های فوتوالکتریک
۶۴۰	 Acoustical Detection Systems	سیستم‌های تشخیص صوتی
۶۴۰	 Wave Motion Detector	ردیاب حرکت موج
۶۴۱	 Capacitance Detector	ظرفیت توان آشکارساز
۶۴۱	 CCTV	دوربین مدار بسته
۶۴۱	 Lighting	روشنایی
۶۴۲	 Types of Systems	انواع سیستم‌ها
۶۴۲	 Types of Lighting	انواع روشنایی
۶۴۳	 Patrol Force	نیروی گشت
۶۴۳	 Access Control	کنترل دسترسی
۶۴۳	 Building and Internal Security	ساختمان و امنیت داخلی

۶۴۴	Personnel Privacy and Safety	حریم شخصی و ایمنی پرسنل
۶۴۴	Duress	فشار
۶۴۵	Travel	مسافرت
۶۴۵	Monitoring	نظارت
۶۴۷	(Software Development Security)	فصل ۸: امنیت توسعه نرم افزار
۶۴۹	Software Development Concepts	مفاهیم توسعه نرم افزار
۶۴۹	Machine Languages	زبانهای ماشینی
۶۴۹	Assembly Languages and Assemblers	زبان اسمبلی و اسمبلرها
	High-Level Languages, Compilers, and Interpreters	زبانهای سطح بالا، کامپایلرها و مفسرها
۶۵۰		
۶۵۱	Object-Oriented Programming	برنامه نویسی شی گرا
۶۵۲	Polymorphism	چند ریختی
۶۵۲	Polyinstantiation	چند منظوره
۶۵۳	Encapsulation	کپسوله سازی
۶۵۳	Cohesion	انسجام
۶۵۳	Coupling	اتصال
۶۵۳	Data Structures	ساختارهای داده
۶۵۴	Distributed Object-Oriented Systems	توزیع سیستمهای شی گرا
۶۵۴	CORBA	
۶۵۴	DCOM و COM	
۶۵۵	OLE	
۶۵۵	Java	جاوا
۶۵۵	SOA	
۶۵۶	Mobile Code	کد سیار
	Security in the System and Software	امنیت در چرخه عمر توسعه نرم افزار و سیستم
۶۵۷	Development Life Cycle	
۶۵۷	System Development Life Cycle	چرخه عمر توسعه سیستم
۶۵۹	Software Development Life Cycle	چرخه عمر توسعه نرم افزار
	Software Development Methods and Maturity	روشهای توسعه نرم افزار و مدل های بلوغ
۶۶۴	Models	

۶۶۷	 مدل V شکل
۶۶۹	 Incremental افزایشی
۶۷۱	 (RAD) Rapid Application Development توسعه سریع برنامه‌های کاربردی
۶۷۵	 Integrated Product Team تیم محصول یکپارچه
۶۷۷	 Security Controls in Development کنترل‌های امنیتی در توسعه
۶۷۷	 Software Development Security Best Practices بهترین راهکارهای توسعه نرم افزار
۶۷۷	 Web Application Security Consortium(WASC) کنسرسیوم امنیت برنامه وب
۶۸۱	 Escalation of Privileges افزایش امتیازات
۶۸۱	 Backdoors درب پشتی
۶۸۱	 Rogue Programmers برنامه نویسان سرکش
۶۸۲	 Covert Channel کانال مخفی
۶۸۲	 Object Reuse استفاده مجدد از شی
۶۸۲	 Mobile Code کد سیار
۶۸۳	 Time of Check/Time of Use (TOC / TOU) زمان بررسی / زمان استفاده
۶۸۳	 Source Code Analysis Tools ابزارهای تجزیه و تحلیل کد منبع
۶۸۴	 Code Repository Security امنیت مخزن کد
۶۸۴	 Application Programming Interface Security واسط امنیت برنامه نویسی برنامه کاربردی
۶۸۵	 Software Threats تهدیدات نرم افزار
۶۸۵	 Malware بد افزار
۶۸۶	 Virus ویروس
۶۸۷	 Worm کرم
۶۸۷	 Trojan Horse اسب تروجان
۶۸۸	 Logic Bomb بمب منطقی
۶۸۸	 Spyware/Adware ابزار جاسوسی / ابزارهای تبلیغاتی
۶۸۸	 Botnet
۶۸۹	 Rootkit
۶۸۹	 Ransomware
۶۹۰	 Malware Protection محافظت از بدافزار
۶۹۰	 Antivirus Software نرم افزار آنتی ویروس
۶۹۰	 Anti-malware Software نرم افزار ضد بدافزار

۶۹۰	Scanning Types	انواع اسکن
۶۹۱	Security Policies	سیاست‌های امنیتی
۶۹۱		مکانیسم‌های محافظت از نرم افزار
۶۹۲	Assess Software Security Effectiveness	ارزیابی اثربخشی امنیت نرم افزار
۶۹۳	Auditing and Logging	ممیزی و ورود به سیستم
۶۹۳	Risk Analysis and Mitigation	تجزیه و تحلیل و کاهش ریسک
۶۹۴	Regression and Acceptance Testing	آزمون رگرسیون و پذیرش
۶۹۴	Security Impact of Acquired Software	تأثیر امنیتی نرم افزارهای اکتسابی

مقدمه مترجم

از زمانی که نوشتن و تبادل اطلاعات آغاز شد، همه انسان‌ها مخصوصاً سران حکومت‌ها و فرماندهان نظامی در پی راهکاری برای محافظت از محرمانه بودن مکاتبات و تشخیص دستکاری آن‌ها بودند. ژولیوس سزار ۵۰ سال قبل از میلاد یک سیستم رمزنگاری مکاتبات ابداع کرد تا از خوانده شدن پیام‌های سری خود توسط دشمن جلوگیری کند حتی اگر پیام به دست دشمن بیفتد. جنگ جهانی دوم باعث پیشرفت چشمگیری در زمینه امنیت اطلاعات گردید و این آغاز کارهای حرفه‌ای در حوزه امنیت اطلاعات شد. پایان قرن بیستم و سال‌های اولیه قرن بیست و یکم شاهد پیشرفتهای سریع در ارتباطات راه دور، سخت‌افزار، نرم‌افزار و رمزگذاری داده‌ها بود. در دسترس بودن تجهیزات محاسباتی کوچکتر، قوی‌تر و ارزان‌تر پردازش الکترونیکی داده‌ها باعث شد که شرکت‌های کوچک و کاربران خانگی دسترسی بیشتری به آن‌ها داشته باشند. این تجهیزات به سرعت از طریق شبکه‌های رایانه‌ای مثل اینترنت به هم متصل شدند.

همزمان با گسترش استفاده از رایانه‌های شخصی و مطرح شدن شبکه‌های رایانه‌ای و به دنبال آن اینترنت (بزرگترین شبکه جهانی)، حیات رایانه‌ها و کاربران آنان دستخوش تغییرات اساسی شده‌است. استفاده‌کنندگان رایانه به منظور استفاده از دستاوردها و مزایای فناوری اطلاعات و ارتباطات، ملزم به رعایت اصولی خاص و اهتمام جدی به تمامی مؤلفه‌های تأثیرگذار در تداوم ارائه خدمات در یک سیستم رایانه‌ای می‌باشند. امنیت اطلاعات و ایمن‌سازی شبکه‌های رایانه‌ای از جمله این مؤلفه‌ها بوده که نمی‌توان آن را مختص یک فرد یا سازمان در نظر گرفت. پرداختن به مقوله امنیت اطلاعات و ایمن‌سازی شبکه‌های رایانه‌ای در هر کشور، مستلزم توجه تمامی کاربران صرف‌نظر از موقعیت شغلی و سنی به جایگاه امنیت اطلاعات و ایمن‌سازی شبکه‌های رایانه‌ای بوده و می‌بایست به این مقوله در سطح کلان و از بعد منافع ملی نگاه کرد. وجود ضعف امنیتی در شبکه‌های رایانه‌ای و اطلاعاتی، عدم آموزش و توجیه صحیح تمامی کاربران صرف‌نظر از مسئولیت شغلی آنان نسبت به جایگاه و اهمیت امنیت اطلاعات، عدم وجود دستورالعمل‌های لازم برای پیشگیری از نقایص امنیتی، عدم وجود سیاست‌های مشخص و مدون به منظور برخورد مناسب و بموقع با اشکالات امنیتی، مسائلی را به دنبال خواهد داشت که ضرر آن متوجه تمامی کاربران رایانه در یک کشور شده و عملاً زیرساخت اطلاعاتی یک کشور را در معرض آسیب و تهدید جدی قرار می‌دهد.

آزمون و مدرک بین المللی CISSP مخفف Certified Information Systems Security Professional متعلق به کنسرسیوم امنیت اطلاعات International Information Security Certification Consortium, Inc² (ISC) می باشد. این شرکت در سال ۱۹۸۹ به عنوان یک کنسرسیوم غیر انتفاعی از پیشروان صنعت و با هدف عرضه مدارک بین المللی در زمینه امنیت اطلاعات در هر سطح و گرایشی آغاز به کار نمود. در سال ۱۹۹۲ کنسرسیوم مذکور اقدام به طرح مدرکی به نام CISSP نمود که به عنوان مدرکی بسیار کاربردی و مفید در شاخه امنیت اطلاعات، استراتژی های تأمین امنیت شبکه را ارائه می نماید. با توجه به نقش فن آوری اطلاعات در دنیای امروز و استفاده از انواع تکنولوژی های مرتبط، حفاظت از اطلاعات و امنیت سیستم های اطلاعاتی یک از اصلی ترین ارکان پایداری هر ارگان و سازمانی می باشد که با تدوین سیاست های امنیتی درست و دقیق می توان این هدف نیل نمود و به طبع آن تربیت متخصصین کار آمد در این زمینه جزء لاینفک نیازهای هر سازمان و مجموعه اطلاعاتی می باشد. مدرک CISSP به دلیل عدم وابستگی آن به محصولی خاص، به عنوان یک عنصر کلیدی در ارزشیابی داوطلبان کار در مؤسسات بزرگ و سیستم های سازمانی شناخته می شود. افراد دارای مدرک CISSP دارای توانایی لازم در طراحی و پیاده سازی سیاست های کلان امنیتی می باشند. این افراد دارای درک کامل و مستقلی از مسائل مربوط به مهندسی اجتماعی بوده و قادر به ایجاد امنیت اطلاعات در یک سازمان با ارائه خط مشی ویژه با سیاست های خاص امنیتی آن سازمان می باشند. با رشد سریع و استفاده گسترده از پردازش الکترونیکی داده ها و کسب و کار الکترونیک از طریق اینترنت، همراه با ظهور بسیاری از خرابکاری های بین المللی، نیاز به روش های بهتر حفاظت از رایانه ها و اطلاعات آن ها ملموس گردید. هدف مشترک این فعالیت ها و سازمان ها حصول اطمینان از امنیت و قابلیت اطمینان از سیستم های اطلاعاتی است.

کتاب حاضر ترجمه کاملی از کتاب CISSP Cert Guide نوشته Robin Abernathy و Troy McMillan که مطالعه آن را به تمامی متخصصین علاقه مند به مسائل امنیتی و طراحی سیستم های امنیت اطلاعات و ابزارهای توسعه یافته در این زمینه توصیه می کنم و از استادان و صاحب نظران ارجمند تقاضا می شود با همکاری، راهنمایی و پیشنهادهای اصلاحی خود، اینجانب را در جهت اصلاح کتاب حاضر یاری دهند.

سید سامان کریمی

خرداد ماه ۱۳۹۹

Drsamankarimi@Hotmail.com

فصل ۱

امنیت و مدیریت ریسک Security and Risk Management

این فصل موضوعات زیر را پوشش می دهد:

- ❖ شرایط امنیتی **Security terms**: مفاهیم مورد بحث شامل محرمانه بودن، یکپارچگی و دسترسی، نام اختصاری آن CIA، موضع به طور پیش فرض. دفاع در عمق، چرخش کار، و تفکیک وظایف.
- ❖ اصول حاکمیت نظارتی **Security governance principles**: مفاهیم مورد بحث عبارتند از هماهنگ سازی عملکرد امنیت، فرایندهای سازمانی، نقش ها و مسئولیت های امنیتی، چارچوب های کنترل، مراقبت کردن با دلیل و دقت مطالعه.
- ❖ انطباق **Compliance**: مفاهیم مورد بحث شامل تطابق قوانین و مقررات و الزامات حریم خصوصی است.
- ❖ مسائل قانونی و نظارتی **Legal and regulatory issues**: مفاهیم مورد بحث شامل مفاهیم جرم رایانه ای، سیستم های عمده قانونی، مجوز و مالکیت معنوی، کنترل واردات / صادرات، جریان داده های بین المللی، حفظ حریم خصوصی و نقض اطلاعات است.
- ❖ اخلاق حرفه ای **Professional ethics**: اخلاق مورد بحث شامل ISC اصول اخلاقی، موسسه اخلاق رایانه، انجمن معماری اینترنت و اخلاق سازمانی است.
- ❖ اسناد امنیتی **Security documentation**: انواع اسناد شامل سیاست ها، استانداردها، مبانی، دستورالعمل ها و رویه ها هستند.
- ❖ تداوم کسب و کار **Business continuity**: مفاهیم مورد بحث شامل تداوم کسب و کار و مفاهیم بهبود فاجعه، محدوده طرح و برنامه، تجزیه و تحلیل و تاثیر کسب و کار.
- ❖ سیاست های امنیتی پرسنل **Personnel security policies**: سیاست مورد بحث شامل (EMP) Employment Candidate Screening توافقنامه اشتغال و سیاست، سیاست های خاتمه کار، فروشنده، مشاور و قرارداد، انطباق، و حریم خصوصی.
- ❖ مفاهیم مدیریت ریسک **Risk management concepts**: مفاهیم مورد بحث عبارتند از آسیب پذیری، تهدید، عامل تهدید، ریسک، قرار گرفتن در معرض خطر، متقابل، سیاست مدیریت ریسک، تیم مدیریت ریسک، تیم تجزیه و تحلیل ریسک، ارزیابی ریسک، پیاده سازی، انواع کنترل دسترسی، ارزیابی و کنترل، نظارت، اندازه گیری، گزارش و بهبود مستمر و چارچوب ریسک.
- ❖ مدل سازی تهدید **Threat modeling**: مفاهیم مورد بحث عبارتند از شناسایی تهدیدات، حملات بالقوه، و ترمیم فن آوری ها و فرآیندها.

❖ ریسک‌های امنیتی در خرید **Security risks in acquisitions**: مفاهیم مورد بحث شامل سخت افزار، نرم افزار و خدمات، حاکمیت شخص ثالث، حداقل امنیت مورد نیاز، و حداقل سطح الزامات خدمات.

❖ آموزش امنیت، آموزش و آگاهی **Security education, training, and**

awareness: مفاهیم مورد بحث شامل سطح مورد نیاز و بررسی دوره‌ای است.

هزینه امنیت اطلاعات شامل اصول، چارچوب‌ها و روش‌هایی است که معیارهایی را برای حفاظت از دارایی‌های و سرمایه‌های اطلاعاتی، از جمله آگاهی از امنیت، ایجاد می‌کند. مدیریت ریسک به سازمانها اجازه می‌دهد تا شناسایی، اندازه‌گیری و کنترل ریسک‌های سازمانی را انجام دهند. مدل سازی تهدید به سازمان اجازه می‌دهد تا تهدیدات و حملات احتمالی را شناسایی کرده و مقابله با این تهدیدات و حملات را کاهش دهند. این جنبه‌ها اطمینان حاصل می‌کنند که کنترل‌های امنیتی که اجرا می‌شوند در تعادل با عملیات سازمان هستند. این جنبه‌ها اطمینان حاصل می‌کنند که کنترل‌های امنیتی که اجرا می‌شوند در تعادل با عملیات سازمان هستند. هر سازمان باید یک برنامه ریزی مناسب همراه با برنامه امنیتی سفارشی داشته که نیازهای سازمان را برآورده کند، در حالی که مطمئن شود سازمان طرح امنیتی خود را با دقت مورد توجه قرار می‌دهد.

متخصصان امنیت باید در برنامه امنیتی سازمان خود نقش اصلی ایفا کنند و به عنوان مشاوران ریسک عمل کنند. علاوه بر این، متخصصان امنیت باید مطمئن شوند که آنها مسائل و ریسک‌های امنیتی فعلی، مقررات دولتی و صنعت و کنترل‌های امنیتی را که می‌تواند اجرا شوند، درک می‌کنند. اخلاق حرفه‌ای برای پرسنل امنیتی نیز باید قابل درک باشد. امنیت یک فرآیند مداوم و مستمر است و کارشناسان امنیتی باید آن را در نظر بگیرند.

تداوم کسب و کار و بهبود فاجعه تضمین می‌کند که سازمان می‌تواند از هر حمله یا فاجعه‌ای که بر عملیات تاثیر می‌گذارد، بهبود یابد. با استفاده از نتایج ارزیابی ریسک و خطرات، متخصصان امنیت باید تضمین کنند که پیگیری‌های کسب و کار مناسب و طرح‌های (Plan) بهبود فاجعه شامل ایجاد، آزمایش و تجدید نظر در فواصل مناسب قرار می‌گیرد.

در این فصل خواهیم آموخت که چگونه از حاکمیت امنیت اطلاعات و اجزای مدیریت ریسک برای ارزیابی ریسک‌ها استفاده کنیم، کنترل‌هایی را برای ریسک شناسایی شده، نظارت بر اثربخشی کنترل، و انجام ارزیابی‌های ریسک در آینده، یاد بگیریم.

شرایط امنیتی Security Terms

هنگام اجرای امنیت و مدیریت ریسک، چندین اصول و شرایط امنیتی مهم وجود دارد که باید در نظر داشته باشید: محرمانه بودن، یکپارچگی و دسترسی (CIA)، موضع به طور پیش فرض. دفاع در عمق، چرخش کار، و تفکیک وظایف.

سیا CIA (Confidentiality, Integrity, Availability)

سه اصل امنیت عبارتند از محرمانه بودن، یکپارچگی و دسترسی که اغلب به عنوان سه گانه یا مثلث CIA شناخته می شود. هر راس از مثلث باید در هر جنبه ای از طراحی امنیتی مورد توجه قرار گیرد. مثلث CIA به راحتی می تواند در هر حوزه آزمون CISSP مورد بحث قرار گیرد. اکثر مسائل امنیتی منجر به نقض حداقل یک راس مثلث سیا می شود. درک این سه اصل امنیتی، متخصصان امنیت را کمک می کند تا مطمئن شوند که کنترل های امنیتی و مکانیسم های اجرا شده، حداقل در یکی از این اصول، پیاده سازی شده است. هر کنترل امنیتی که توسط یک سازمان به جای آن قرار می گیرد، حداقل یکی از اصول امنیتی CIA سه گانه را اجرا می کند. درک اینکه چگونه این اصول امنیتی را دور بزنیم، به اندازه فهمیدن چگونگی ارائه آنها، اهمیت دارد.

یک رویکرد امنیتی متعادل باید پیاده سازی شود تا اطمینان حاصل شود که هر سه جنبه در هنگام پیاده سازی کنترل امنیتی مورد توجه قرار می گیرد. هنگام اجرای هر گونه کنترل، باید مشخص کنید که آدرس کنترل چیست. به عنوان مثال، آدرس های RAID در دسترس بودن داده ها، یکپارچگی اطلاعات آدرسهای فایل های hash و دسترسی به محرمانه بودن اطلاعات. یک رویکرد متوازن تضمین می کند که هیچ جنبه ای از مثلث CIA را نادیده گرفته نمی شود.

محرمانه بودن Confidentiality

برای اطمینان از محرمانه بودن، باید از افشای اطلاعات به اشخاص غیر مجاز جلوگیری کنید. به عنوان بخشی از محرمانه بودن، قبل از قرار دادن هر گونه کنترل دسترسی، باید میزان حساسیت داده ها تعیین شود. داده ها با یک سطح بالاتر حساسیت، کنترل دسترسی بیشتری را نسبت به داده ها با حساسیت سطح پایین تر، در جای خود دارند. برای حفظ محرمانه بودن داده ها می توان از شناسایی، تصدیق و احراز هویت استفاده کرد.

نقطه مقابل محرمانه بودن، افشاگری می‌باشد. رمزگذاری احتمالا رایجترین نمونه از یک کنترل است که محرمانه بودن را فراهم می‌کند.

یکپارچگی Integrity

یکپارچگی، قسمت دوم مثلث CIA، تضمین می‌کند که داده‌ها از اصلاح غیر مجاز یا آلودگی اطلاعات، محافظت می‌کند. هدف یکپارچگی حفظ یکپارچگی داده‌ها که شامل اطلاعات ذخیره شده در فایل‌ها، پایگاه‌های داده، سیستم‌ها و شبکه‌ها است. نقطه مقابل یکپارچگی، فساد (Corruption) می‌باشد.

یک لیست کنترل دسترسی (Access control list (ACL نمونه‌ای از کنترل است که به ارائه یکپارچگی کمک می‌کند. هش کردن (Hashing) نیز کنترل دیگری است که به ارائه یکپارچگی فایل کمک می‌کند.

دسترسی Availability

دسترسی بدان معنی است که تضمین می‌شود که داده‌ها قابل دسترسی هستند، هر زمان که لازم باشد. فقط افرادی که نیاز به دسترسی به داده‌ها دارند باید دسترسی به این داده‌ها را داشته باشند. دو مورد اصلی که در دسترس بودن آنها تحت تاثیر قرار می‌گیرند (۱) هنگامی که حملات انجام می‌شوند که سیستم را غیرفعال یا فلج می‌کنند و (۲) وقتی از دست دادن خدمات در طول و پس از حملات رخ می‌دهد. هر سیستم باید با توجه به اهمیت آن در عملیات سازمانی ارزیابی شود. کنترل باید بر اساس سطح بحرانی هر سیستم اجرا شود.

در دسترس بودن نقطه مقابله انزوا (Destruction or Isolation) است. فن‌آوری‌های تحمل خطا Fault-Tolerant Technologies، مانند RAID یا سایت‌های افزونه Redundant، نمونه‌هایی از کنترل‌هایی هستند که به افزایش دسترسی می‌پردازند.

موضع پیش فرض Default Stance

یک رویکرد سازمان برای امنیت اطلاعات به طور مستقیم بر استراتژی کنترل دسترسی تاثیر می‌گذارد. برای یک وضعیت پیش فرض، سازمان دهی باید به گونه‌ای باشد که بین یک اجازه توسط پیش فرض یا یک موضع انکار به دلخواه یکی را انتخاب کنید. همانطور که در نام آن اشاره شده است، یک وضعیت اجازه به حالت پیش فرض اجازه دسترسی Allow-by-Default به هر

داده‌ای را می‌دهد مگر آنکه نیاز به محدود کردن دسترسی وجود داشته باشد. موضع انکار به واسطهٔ پیش فرض Deny-by-Default بسیار سخت تر است، زیرا انکار دسترسی که صراحتاً مجاز نیست. نهادهای دولتی و نظامی و بسیاری از سازمان‌های تجاری از موضع انکار به دلایلی استفاده می‌کنند.

امروزه تعداد کمی از سازمانها هر یک از این موقعیتهای را به طور کامل اجرا می‌کنند. در اکثر سازمان ها، ترکیبی از دو را مشاهده می‌کنید. اگر چه موضع اصلی باید سازمان را هدایت کند، سازمانها اغلب می‌گویند که این ترکیب لازم است تا تضمین شود که از داده‌ها در زمان دسترسی چندین کاربر محافظت می‌شود. به عنوان مثال، یک وب سایت عمومی ممکن است موضع اجازه به حالت پیش فرض را اعطا کند، در حالی که یک پایگاه داده SQL ممکن است یک موضع انکار به صورت پیش فرض داشته باشد.

دفاع در عمق Defense in Depth

استراتژی دفاع در عمق به استفاده از چند لایه امنیتی بین داده‌ها و منابع موجود در آن و مهاجمین احتمالی اشاره دارد. اولین لایه از یک استراتژی دفاع در عمق، مناسب برای استراتژی کنترل دسترسی است. کنترل دسترسی در همه زیرمجموعه‌های سیستم اطلاعاتی (IS) وجود دارد (بیشتر به عنوان یک زیرساخت IT شناخته می‌شود)، اما یک استراتژی دفاع در عمق فراتر از کنترل دسترسی است. آن‌ها همچنین امنیت توسعه نرم افزار، امنیت دارایی‌ها و تمام دامنه‌های دیگر CISSP را در نظر می‌گیرد.

شکل ۱-۱ یک نمونه از مفهوم دفاع در عمق را نشان می‌دهد.



شکل ۱-۱ مثال دفاع در عمق

چرخش کار Job Rotation

چرخش کار تضمین می‌کند که بیش از یک نفر یک موقعیت واحد را در یک سازمان انجام می‌دهد. این چرخش کار تضمین می‌کند که بیش از یک نفر قادر به انجام آن وظایف هستند، و

افزونگی را فراهم می‌کنند. همچنین یک ابزار قابل اعتماد برای کمک به یک سازمان برای تشخیص زمانی که فعالیت‌های ناخواسته رخ داده است، می‌باشد.

تفکیک وظایف Separation of Duties

تفکیک وظایف تضمین می‌کند که یک فرد قادر به ایجاد امنیت در سازمان نیست. هر فعالیتی که به عنوان ریسک منجر به آسیب شناخته می‌شود، باید به وظایف فردی تقسیم شود که بعداً می‌تواند به افراد یا ادارات مختلف اختصاص یابد. هنگامی که یک سازمان تقسیم کافی از وظایف را اجرا می‌کند، برای انجام تقلب در سازمان، باید توافق نامه بین دو یا چند نفر از کارکنان وجود داشته باشد. تقسیم دانش، تنوع جدایی از وظایف، تضمین می‌کند که هیچ یک از کارمندان تمام جزئیات را برای انجام یک کار را نمی‌دانند. به عنوان مثال می‌تواند دو نفر باشد که هریک بخشی از یک ترکیب ایمن را می‌دانند. یک تنوع دیگر کنترل دوگانه است که نیازمند آن است که دو کارمند باید برای تکمیل کار مشخصی، آماده باشند. به عنوان مثال دو مدیر برای چرخاندن کلیدها به طور همزمان در مکان‌های جداگانه برای راه اندازی یک موشک نیاز می‌باشد.

اصول حاکمیت امنیت Security Governance Principles

سازمان باید از اصول حاکمیت امنیتی استفاده کند تا تضمین شود که از تمام دارایی‌های سازمانی محافظت می‌شود. سازمانها معمولاً از بهترین شیوه‌ها استفاده می‌کنند که توسط سازمان‌های حاکمیت ثالث ایجاد می‌شود مانند:

- National Institute of Standards and Technology (NIST) موسسه ملی استاندارد

و فناوری

- Information Technology Infrastructure Library (ITIL) کتابخانه زیرساخت

فناوری

از آنجاییکه فناوری اطلاعات یک ضرورت عملی است، مدیریت باید نقش مهمی در ابتکار عمل حاکمیت امنیتی داشته باشد.

حاکمیت امنیت حقوق را تعیین می‌کند و از چارچوب قانونی برای تضمین تصمیم مناسب استفاده می‌کند. از اینرو باید تضمین شود که چارچوب استفاده شده با استراتژی کسب و کار هماهنگ است. زمامداری یا حاکمیت امنیت، جهت، استانداردها و اصول را ایجاد می‌کند و سرمایه گذاری‌ها را اولویت بندی می‌کند که در واقع مسئولیت مدیران و مدیران اجرایی سازمان است.

مؤسسه حاکمیت فناوری ITGI در جلسه توجیهی هیئت مدیره حاکمیت فناوری اطلاعات، نسخه ۲، صادر شده که

در وب سایت www.isaca.org/Knowledge-Center/Research/ResearchDeliverables/Pages/Board-Briefing-on-IT-Governance-2nd-Edition.aspx edge-center / Research / ResearchDeliverables /
ممیزی و کنترل سیستم های اطلاعاتی ISACA (Information Systems Audit and Control Association)، این تعریف را برای مدیریت فناوری اطلاعات فراهم می کند:

حاکمیت فناوری اطلاعات به عهده هیئت مدیره و مدیر اجرایی است و بخش تفکیک ناپذیر از مدیریت سازمانی است و شامل رهبری و ساختارها و فرآیندهای سازمانی و فرایندهایی است که نشان می دهد فناوری اطلاعات سازمان، استراتژی ها و اهداف سازمان را توسعه و گسترش می دهد. بر اساس این نشریه، مدیریت فناوری اطلاعات، نظارت راهبردی، تحویل ارزش، مدیریت ریسک، مدیریت منابع و اندازه گیری عملکرد را پوشش می دهد، که شامل چک لیست ها و ابزارهایی برای کمک به هیئت مدیره و مدیر اجرایی سازمان می باشد تا مدیریت IT را تضمین کند.

اصول حاکمیت امنیت عبارتند از:

تطبیق عملکرد امنیتی با استراتژی، اهداف، مأموریت و اهداف سازمان، فرآیندهای سازمانی، نقش و مسئولیت های امنیتی، چارچوب کنترل، مراقبت، و دقت کافی.

هماهنگ سازی (تطبیق) عملکرد امنیتی Security Function Alignment

عملکرد امنیتی باید با اهداف، مأموریت و نتایج سازمان مرتبط باشد که این شامل کنترل های دسترسی مورد نیاز برای ارائه CIA برای دارایی های سازمانی است. مدیریت امنیت موثر شامل ارزیابی تحمل ریسک سازمان، تعیین هزینه های کنترل دسترسی مناسب و ثبت مزایای کنترل های سازمان می باشد.

در حالتی که ۱۰۰٪ امنیت داده ها به عنوان یک هدف سازمانی مطلوب می باشد، چنین هدفی در جهان امروز دشوار است زیرا هر روز تهدیدات و آسیب پذیری های جدید کشف می شود. به همین دلیل مهم است که یک برنامه امنیتی سازمان باز و پیشگیرانه باشد.

برنامه امنیتی باز به این واقعیت اشاره دارد که تجزیه و تحلیل امنیتی و برنامه همیشه مورد بررسی قرار می گیرند.

برنامه امنیتی پیشگیرانه بدان معنی است که سازمان به صورت فعالانه می باشد نه فقط واکنشی، هنگامی که رخدادی اتفاق می افتد.

استراتژی و اهداف سازمانی Organizational Strategy and Goals

استراتژی و اهداف امنیتی سازمان باید مستند گردد. مدیریت امنیت، با استفاده از کنترل‌های فیزیکی، اداری و منطقی، از دارایی‌های سازمانی محافظت می‌کند. در حالی که مدیریت مسئول توسعه استراتژی امنیت سازمان است، مسئولان امنیتی در این سازمان مسئول انجام استراتژی هستند. بنابراین، متخصصان امنیت باید در ایجاد استراتژی و اهداف امنیتی سازمانی دخیل باشند. یک استراتژی یک طرح فعالیت یا یک سیاست طراحی شده برای دستیابی به هدف اصلی یا کلی است. اهداف Goals از طرح امنیتی مورد نظر می‌باشد. یک تیم مدیریت امنیت باید هنگام طراحی استراتژی و اهداف امنیتی سازمان، به کلیه حوزه‌های امنیتی از جمله محافظت از پرسنل، دارایی‌های فیزیکی و داده‌ها بپردازد. استراتژی و اهداف باید با گذشت زمان تغییر کند، زیرا علاوه بر اینکه سازمان رشد و تغییر می‌کند جهان نیز تغییر می‌کند. سالها پیش، سازمانها نیازی به نگرانی در مورد اطلاعات خود نداشتند که در اینترنت دزدیده می‌شد. اما امروز، اینترنت یکی از رایج ترین رسانه‌های مورد استفاده برای کسب غیر قانونی اطلاعات سازمانی محرمانه می‌باشد.

اهداف و مأموریت سازمان Organizational Mission and Objectives

اهداف مأموریت سازمان باید از طریق مدیریت سازمانی یا هیئت مدیره به تصویب برسد. تیم مدیریتی سازمان باید مطمئن شود، که هر استراتژی و اهداف امنیتی متناسب با مأموریت و اهداف سازمان است. اطلاعات و دارایی‌هایی که مأموریت سازمان را پشتیبانی می‌کنند باید به عنوان بخشی از استراتژی و اهداف امنیتی محافظت شوند.

باید تضمین شود، سیاست‌ها، رویه‌ها، استانداردها و دستورالعمل‌های مناسب و ریسک سازمانی در سطح قابل قبول باشد. متخصصان امنیت به مدیریت بر ریسک‌های سازمانی توصیه می‌کنند. ریسک سازمانی نیز تحت تاثیر مقررات دولتی قرار می‌گیرد که ممکن است سازمان را مجبور به اجرای معیارهای خاصی کند که برنامه ریزی نشده اند. در نهایت، ارزیابی ریسک سازمان و انتخاب اینکه آیا کنترل‌های امنیتی اجرا می‌شود، کار مدیریت ارشد Senior management است. مدیریت امنیت تضمین می‌کند در قالب حمایت از مأموریت سازمان و اهداف سازمان، ریسک‌ها شناسایی شده و کنترل کافی برای کاهش ریسک‌ها انجام می‌شود.

طرح کسب و کار Business Case

یک طرح کسب و کار یک سند رسمی است که دلایل پشت یک پروژه یا ابتکار سازمانی را به وجود می آورد و معمولاً توجیه مالی برای یک پروژه یا یک ابتکار را شامل می شود. تیم مدیریت امنیت باید یک طرح کسب و کار رسمی را برای ارزیابی امنیت کلی یک سازمان توسعه دهد. هنگامی که ارزیابی امنیتی سازمان کامل شد و طرح کسب و کار خود را ایجاد کرد، مدیریت تصمیم خواهد گرفت که چگونه این روند را اجرا کند. در آن زمان، طرح های کسب و کار دیگر برای پروژه های امنیتی فردی باید توسعه یابد. به عنوان مثال، اگر مدیریت می خواهد تیم مدیریت امنیت تضمین کند که شبکه داخلی سازمان در مقابل حملات محافظت می شود، تیم مدیریت امنیت می تواند یک طرح کسب و کار را تهیه کند که دستگاه های لازم برای اجرای این هدف را توضیح دهد. این طرح کسب و کار ممکن است شامل فایروال ها، سیستم های تشخیص نفوذ IDS ها، ACL ها و سایر دستگاه ها باشد و باید مشخص شود که چگونه دستگاه ها حفاظت را فراهم می کنند.

بودجه امنیت، معیارها و اثربخشی Security Budget, Metrics, and Effectiveness

افسر ارشد امنیت (CSO - Chief Security Officer) یا مدیر ارشد دیگر تعیین شده، بودجه امنیتی سازمان را تهیه می کند، معیارهای امنیتی را تعیین می کند، و گزارشات مربوط به کارایی برنامه امنیتی را ارائه می دهد. این افسر باید با متخصصان SME ها کار کند تا تضمین شود که تمامی هزینه های امنیتی صرف توسعه، تست، اجرا، تعمیر و نگهداری، پرسنل و تجهیزات می شود. فرآیند بودجه نیاز به بررسی تمام ریسک ها دارد و تضمین می کند که پروژه های امنیتی با بهترین نسبت هزینه / سود انجام شده است. پروژه هایی که طولانی تر از ۱۲-۱۸ ماه طول می کشد، بلندمدت و استراتژیک هستند و نیاز به منابع و بودجه بیشتری برای تکمیل دارند.

معیارهای امنیتی Security metrics، اطلاعات در مورد روند کوتاه مدت و بلند مدت را ارائه می دهند. با جمع آوری این معیارها و مقایسه آنها روز به روز، یک کارشناس امنیتی می تواند حجم کاری روزانه را تعیین کند. هنگامی که معیارها در یک دوره زمانی طولانی تر مقایسه می شوند، روند هایی که در آن رخ می دهد می توانند به شکل گیری پروژه های امنیتی و بودجه های آینده کمک کنند. روش ها باید مشخص کنند چه کسی who معیارها را جمع آوری کرده، کدام which معیارها جمع آوری شده، چه زمانی که when معیارها جمع آوری می شود، و چه what

زمانی که باعث اقدامات اصلاحی خواهد شد. متخصصان امنیت باید با چارچوب‌های حاکمیت امنیت اطلاعات، که بعدها در این فصل ذکر می‌شود، به ویژه ISO / IEC 27004 و NIST 800-55، برای کمک به ایجاد دستورالعمل‌ها و روش‌های معیار، بحث کنند. اگرچه تیم امنیتی باید به صورت روزانه معیارها را تحلیل کند، اما تجزیه و تحلیل دوره‌ای معیارها توسط شخص ثالث می‌تواند با تأیید نتایج تیم داخلی، از یکپارچگی و اثربخشی معیارهای امنیتی اطمینان حاصل کند. از داده‌های شخص ثالث برای بهبود برنامه امنیتی و فرآیند اندازه‌گیری‌های امنیتی استفاده می‌شود.

منابع Resources

اگر منابع مناسب به عملکرد امنیتی سازمان اختصاص نداشته باشند، حتی بهترین راه حل برنامه‌های امنیتی شکست خواهد خورد. این منابع شامل، محدود به پرسنل امنیتی، دستگاه‌ها و کنترل‌ها نیستند. همانطور که در "بودجه امنیت، معیارها و اثربخشی" بحث شده است، تخصیص منابع بر اساس بودجه امنیتی محدود است. تجزیه و تحلیل ریسک به سازمان کمک می‌کند تعیین کند که کدام منابع امنیتی ضروری نیستند. اما به خاطر داشته باشید که عملکرد امنیتی سازمان، به طور مداوم در حال تغییر است، بنابراین تخصیص منابع به عملکرد امنیتی باتوجه به نیاز تغییر می‌کند. ممکن است سال گذشته هزینه‌ای غیرقانونی داشته باشد، ممکن است در سال جاری یا چند سال پیش ضرورت وجود داشته باشد، ممکن است در نظر گرفته شده ولی منسوخ شده باشد و ممکن است سطح حفاظتهایی را که نیاز دارید فراهم کند. به همین علت، متخصصان امنیت باید به طور مرتب تحلیل فرایند تجزیه و تحلیل را برای تعیین اینکه چه بهبودی در عملکرد امنیتی یک سازمان انجام می‌شود، دوباره بررسی کنند.

متخصصان امنیت نیز باید درک کنند که چه منابع انسانی برای حمایت از هر گونه فعالیت امنیتی مورد نیاز است، که ممکن است شامل صاحبان داده‌ها، ادمین‌های سیستم، ادمین‌های شبکه، تکنسین IT، توسعه دهندگان نرم افزار، اجرای قانون، و مأمورین حسابداری باشد. اندازه سازمان در دسترس بودن منابع بر روی هر عملکرد امنیتی سازمانی تاثیر می‌گذارد. متخصصان امنیت باید برای ایجاد ارتباط با تمام منابع انسانی برای ایجاد یک برنامه امنیتی موفق همکاری کنند.

فرآیندهای سازمانی Organizational Processes

برای درک فرآیندهای سازمان، سازمان‌ها باید فعالیت مورد نیاز برای انجام یک هدف را تعیین کنند، فعالیت‌ها را به افراد اختصاص داده و فعالیت‌ها را در ساختار تصمیم‌گیری سازمانی مرتب کنند. نتیجه نهایی ادغام فرآیندها یک سازمان است که از قطعات متحد در هماهنگی برای اجرای وظایف برای دستیابی به اهداف استفاده می‌شود. اما همه سازمان‌ها بین دوره‌های رشد و کاهش حرکت می‌کنند. سازمان‌ها اغلب در طول این دوره‌ها، از طریق خرید، ادغام به تقسیم سود می‌پردازند. علاوه بر این، کمیته‌های حاکمیت برای کمک به بهبود سازمان و فرآیندهای آن تشکیل می‌شوند.

اکتساب و واگذاری Acquisitions and Divestitures

یک اکتساب زمانی اتفاق می‌افتد که یک سازمان، سازمان‌های دیگری را خریداری می‌کند و یک ادغام زمانی اتفاق می‌افتد که دو سازمان تصمیم می‌گیرند با یکدیگر متحد شوند تا یک سازمان شوند. در هر دو مورد، آنها می‌توانند دوستانه یا خصمانه در نظر گرفته شوند.

متخصصان امنیت باید توجه زیادی به توجه مدیران داشته باشند تا مطمئن شوند که امنیت سازمانی در نتیجه اکتساب یا ادغام به خطر نمی‌افتد. سازمان دیگری ممکن است انواع داده‌ها و فن‌آوری‌های جدیدی داشته باشد که ممکن است به حفاظت از آنچه در حال حاضر ارائه می‌شود نیاز بیشتری داشته باشد. به عنوان مثال، سازمان می‌تواند کارکنان را مجاز به استفاده از دستگاه‌های خود و استفاده از آنها در شبکه کند. در حالی که یک واکنش تند و سریع ممکن است فقط سیاست مشابهی را در سازمان کنونی اجرا کند، متخصصان امنیت باید ارزیابی کنند که چرا دستگاه‌های شخصی مجاز هستند و در فرهنگ سازمان وجود دارد.

یکی دیگر از موارد مورد نظر اکتساب یا ادغام برای متخصصان امنیت این است که کارکنان سازمان‌های دیگر ممکن است آموزش و آگاهی مناسب امنیتی را نداشته باشند. اگر آگاهی نداشته باشند، ممکن است ضروری باشد که آموزش‌های امنیتی در اسرع وقت به کارکنان شرکت اعطا شود.

هنگامی که اکتساب و یا ادغام رخ می‌دهد، معمولاً درصدی از پرسنل حفظ نمی‌شود. متخصصان امنیت باید هر گونه تهدیدی از سوی کارکنان سابق و هر گونه تهدید جدیدی که ممکن است به

علت اکتساب یا ادغام ایجاد شوند را درک کنند. متخصصان امنیت این تهدیدات را درک می‌کنند تا بتوانند طرح‌هایی برای کاهش تهدیدات ایجاد کنند.

به عنوان بخشی از ادغام یا اکتساب، تکنولوژی معمولاً یکپارچه می‌شود. در غیر این صورت این ادغام می‌تواند آسیب‌پذیری‌هایی را که سازمان با آن روبرو نخواهد شد، ارائه دهد. به عنوان مثال، اگر یک شرکت خریداری یک سیستم میراثی را حفظ کند، زیرا پرسنل به آن نیاز دارند، ممکن است سازمان برای محافظت از سیستم میراثی یا استقرار سیستم جدیدی که جایگزین آن خواهد شد، اقدامات لازم را انجام دهد.

سرانجام، با اکتساب یا ادغام، قوانین، مقررات و استانداردهای جدید ممکن است در سراسر سازمان جدید پیاده‌سازی شود. ارتباط با شرکای کسب و کار، فروشندگان و سایر اشخاص نیز باید بررسی شود. متخصصان امنیت باید تضمین کنند که مدیریت را در هر گونه مسائل امنیتی که ممکن است بوجود می‌آیند، به درستی راهنمایی کنند.

واگذاری که نقطه مقابل اکتساب است، زمانی رخ می‌دهد که بخشی از یک سازمان از سازمان اصلی به فروش می‌رسد یا جدا می‌شود. واگذاری بر کارکنان تأثیر می‌گذارد، زیرا معمولاً بخش‌هایی از کارکنان با واگذاری جدا می‌شوند.

همانطور که در مورد اکتساب سازمان، یا واگذاری‌ها، متخصصان امنیت باید ملاحظات خاصی را مورد توجه مدیریت قرار دهند تا مطمئن شوند که امنیت سازمانی در خطر می‌باشد، نشت اطلاعات ممکن است به عنوان یک نتیجه از خروج پرسنل رخ دهد. پرسنل که به دلیل نتیجه واگذاری از سازمان جدا شده‌اند، یک دغدغه خاص برای سازمان می‌باشند. این امر بستگی دارد که کارکنان خروجی تا چه حد دسترسی به دارایی‌ها و منابع سازمانی دارند. این دسترسی باید در زمان مناسب حذف شود و پروتکل‌ها و پورت‌هایی که دیگر مورد نیاز نیست باید حذف یا بسته شوند.

متخصصان امنیت نیز باید در نظر داشته باشند که در آن دارایی‌های امنیتی و کنترل‌های مختلف به پایان خواهد رسید. اگر دارایی‌های امنیتی بخشی از واگذاری باشند، باید تضمین شود که قبل از واگذاری، جایگزینی‌ها در صورت لزوم پیاده‌سازی می‌شوند. علاوه بر این، سیاست‌ها و رویه‌ها باید بررسی شوند تا تضمین شود که نیازهای سازمان جدید را بازتاب می‌کند.

کمیته های حاکمیت Governance Committees

یک کمیته حاکمیت هیئت مدیره سازمان را اداره و نگهداری می کند. چنین کمیته ای قدرت فوق العاده ای نسبت به یک سازمان دارد، زیرا در نهایت تصمیم می گیرد که رهبران چه کسانی باشند. متخصصان امنیت باید زمان را برای آموزش یک کمیته حاکمیت برای درک امنیت و مدیریت ریسک، از جمله آموزش آگاهی امنیتی که برای این گروه مناسب است، به راه بیندازند. به عنوان مثال، در حالی که پرسنل امنیتی ممکن است نیاز به درک اقدامات امنیتی مناسب که در وظایف روزمره خود دارند، اعضای کمیته حاکمیت تنها نیاز به درک ریسک های سازمان دارند، باید به دقت مورد توجه قرار گیرند. متخصصان امنیت نیز باید یک کمیته حاکمیت را تشویق کنند تا از میان اعضای هیئت مدیره افرادی که امنیت اطلاعات و ریسک ها را درک می کنند، حضور داشته باشند. در نهایت، یک متخصص امنیت بایستی یک خط ارتباطی با یک کمیته حاکمیت برای پاسخ دادن به هرگونه سؤال امنیتی، ریسک یا حفظ حریم خصوصی داشته باشد.

نقش های امنیتی و مسئولیت ها Security Roles and Responsibilities

اگرچه تمام سازمانها مسئولیت درون سازمان را دارند، امنیت رایانه به طور کلی مسئولیت همه افراد سازمان می باشد. این قسمت مسئولیت های نقش های مختلف در یک سازمان را در بر می گیرد.

هیئت مدیره Board of Directors

هیئت مدیره سازمان شامل افرادی است که توسط یک کمیته حاکمیت معرفی شده اند و توسط سهامداران انتخاب شده اند تا تضمین شود که این سازمان به درستی فعالیت می کند. وفاداری هیئت مدیره باید به سهامداران، نه مدیریت سطح بالا باشد. اعضای هیئت مدیره باید استقلال خود را از همه کارکنان سازمان حفظ کنند، به ویژه اگر قانون (Sarbanes-Oxley (SOX یا Gramm-Leach-Bliley (GLBA به این سازمان اعمال شود.

توجه داشته باشید

همه قوانین مربوط به امتحان CISSP بعداً در این فصل مورد بحث قرار می گیرند. به خاطر داشته باشید که برای اهداف آزمون، متخصصان امنیت فقط باید به درک نوع سازمان ها و داده هایی که این قوانین بر آنها تأثیر می گذارد، بپردازند.

در شرایط مشابه، مقامات ارشد از جمله هیئت مدیره و مدیر ارشد، باید وظایف خود را مشابه افراد عادی و محتاط کار، انجام دهند. این به عنوان قانون محتاطانه (Prudent-man Rule) شناخته شده است. مراقبت‌های متداول و دقت کافی، که بعداً در این فصل مورد بحث قرار خواهد گرفت، همچنین بر اعضای هیئت مدیره و مدیریت سطح بالا تأثیر می‌گذارد.

مدیریت Management

مدیریت سطح بالا دارای مسئولیت نهایی برای حفظ و محافظت از اطلاعات سازمانی است. مدیریت سطح بالا شامل CEO، CFO، CIO، CPO، CSO است. سطوح مدیریت دیگر، از جمله مدیران بخش‌های کسب و کار و مدیران عملیات کسب و کار، دارای مسئولیت‌های امنیتی نیز هستند.

مدیر عامل (Chief Executive Officer (CEO بالاترین مقام اداری در هر سازمان است و به طور مستقیم به سهامداران گزارش می‌دهد. مدیر عامل شرکت باید مطمئن شود که یک سازمان رشد و شکوفایی داشته است. مدیر مالی ارشد Chief Financial Officer (CFO) مسئول تمام جنبه‌های مالی یک سازمان است. اگرچه CFO ممکن است به طور مستقیم به مدیرعامل گزارش دهد، CFO همچنین باید اطلاعات مالی را به سهامداران و نهادهای دولتی ارائه دهد. افسر ارشد اطلاعات (Chief Information Officer (CIO مسئول تمام سیستم‌های اطلاعاتی و فن آوری مورد استفاده در سازمان است و به طور مستقیم به مدیر عامل و یا مدیر مالی گزارش می‌دهد. افسر ارشد اطلاعات معمولاً برای محافظت از دارایی‌های شرکت، از جمله هر برنامه امنیتی سازمانی تلاش می‌کند.

افسر ارشد امنیت خصوصی (Chief Privacy Officer (CPO) افسر مسئول اطلاعات خصوصی است و معمولاً به طور مستقیم به CIO گزارش می‌دهد. به عنوان یک موقعیت جدیدتر، این نقش هنوز اختیاری است اما به طور فزاینده‌ای در حال رایج شدن است، به ویژه در سازمان‌هایی که اطلاعات زیادی از جمله نهادهای پزشکی، شرکت‌های بیمه و موسسات مالی را اداره می‌کنند. متخصصان امنیت باید مطمئن شوند که در صورت لزوم همه ریسک‌ها به مدیریت اجرایی و هیئت مدیره اطلاع داده می‌شود. مدیریت اجرایی باید تعادل بین ریسک قابل قبول و عملیات کسب و کار را حفظ کند. در حالیکه مدیریت اجرایی از جزئیات هرگونه پیاده سازی امنیتی نگران نیست، هزینه‌ها یا مزایای هر پیاده سازی امنیتی و هر گونه ریسک باقی مانده Residual Risk پس از چنین پیاده سازی، برای اطمینان از خرید خود در پیاده سازی حیاتی خواهد بود.

مدیران واحد کسب و کار اطلاعات دپارتمان را برای اطمینان از اینکه کنترل های مناسب برای دپارتمان وجود دارد، ارائه می دهند. اغلب مدیران واحد کسب و کار که به عنوان مالک داده هستند تمام داده ها را برای دپارتمان طبقه بندی می کنند. برخی از مدیران واحد کاری دپارتمان وظایف امنیتی را برعهده دارند. به عنوان مثال، مدیر بخش عملیات کسب و کار بهترین گزینه برای نظارت بر توسعه سیاست امنیتی است.

کمیته ممیزی Audit Committee

یک کمیته ممیزی یک مکانیزم گزارشگری مالی سازمان را ارزیابی می کند تا تضمین شود که داده های مالی دقیق می باشد. این کمیته، ممیزی داخلی را انجام می دهد و در صورت لزوم ممیزهای مستقل را اداره می کند. اعضای این کمیته باید به صورت منظم آموزش های لازم را کسب کنند تا اطمینان حاصل شود که می توانند گزارش مالی را نظارت کنند و پاسخگویی را در فرایندهای مالی انجام دهند.

مالک داده (صاحب داده) Data Owner

مسئولیت اصلی مالک داده تعیین سطح طبقه بندی اطلاعاتی است که در اختیار دارد و وی مسئول محافظت از داده هایی را دارد، که در اختیار وی می باشد. این نقش، حقوق دسترسی به داده ها را تأیید یا رد می کند. با این حال، مالک داده معمولاً اجرای کنترلهای دسترسی به داده را مدیریت نمی کند.

نقش مالک داده ها معمولاً توسط فردی که داده ها را از طریق عضویت در یک واحد کسب و کار خاص درک می کند، تعیین می شود. هر واحد کسب و کار باید یک مالک داده داشته باشد. به عنوان مثال، یک کارمند اداره منابع انسانی داده های کارکنان منابع انسانی را بهتر از یک کارمند بخش حسابداری درک می کند.

نگهبان داده Data Custodian

نگهبان داده، طبقه بندی اطلاعات و کنترل را پس از اینکه توسط مالک داده تعیین می شود، پیاده سازی می کند. اگرچه مالک داده معمولاً فردی است که داده ها را درک می کند، اما نگهبان داده هیچ گونه اطلاعاتی از داده ها نداشته و کاری فراتر از طبقه بندی نمی کند. اگر چه یک مدیر

منابع انسانی بایستی مالک داده برای داده‌های منابع انسانی باشد ولی یک عضو بخش فناوری اطلاعات می‌تواند به عنوان نگهدارنده داده فعالیت کند.

صاحب سیستم System Owner

یک صاحب سیستم دارای یک یا چند سیستم است و باید تضمین کند که کنترل‌های مناسب در آن سیستم وجود دارد. اگر چه یک صاحب سیستم یک سیستم واحد است، صاحبان سیستمها می‌توانند مسئولیت اطلاعات در سیستم را بر عهده بگیرند. بنابراین، دارندگان سیستم باید بتوانند نیازهای مالکان داده‌های متعدد را مدیریت کرده و رویه‌های مناسب را برای اطمینان از ایمن بودن داده‌ها انجام دهند.

مدیر سیستم (ادمین سیستم) System Administrator

یک ادمین سیستم مدیریت روزانه یک یا چند سیستم را دارد و این وظایف امروزه شامل اضافه کردن و حذف کاربران سیستم و نصب نرم افزار سیستم می‌باشد.

مدیر امنیت Security Administrator

یک مدیر امنیت دستگاه‌های و نرم افزارهای امنیتی، از جمله فایروال، نرم افزار آنتی ویروس و غیره را نگهداری می‌کند. تمرکز اصلی مدیر امنیت، امنیت است، در حالی که تمرکز اصلی ادمین سیستم، دسترسی به سیستم است و تمرکز اصلی ادمین شبکه، دسترسی به شبکه است. مدیر امنیت تمام اطلاعات ممیزی امنیت را بررسی می‌کند.

تحلیلگر امنیتی Security Analyst

یک تحلیلگر امنیتی، نیازهای امنیتی سازمان را تجزیه و تحلیل می‌کند و مدارک اداری امنیت اطلاعات داخلی، از جمله سیاست‌ها، استانداردها و دستورالعمل‌ها را توسعه می‌دهد. این نقش بر طراحی امنیت، نه اجرای آن متمرکز است.

مالک اپلیکیشن Application Owner

یک مالک اپلیکیشن پرسنلی را تعیین می‌کند که می‌تواند به یک اپلیکیشن دسترسی داشته باشند. از آنجا که اکثر اپلیکیشن‌ها متعلق به یک واحد دپارتمان هستند، مدیران بخش کسب و

کار معمولا این نقش را بازی می کنند. با این وجود، مالک اپلیکیشن لزوما مدیریت روزانه اپلیکیشن را اجرا نمی کند. این مسئولیت را می تواند به یک عضو از کارکنان فناوری اطلاعات به دلیل مهارت های فنی مورد نیاز منتقل کند.

سرپرست Supervisor

یک سرپرست گروهی از کاربران و دارایی های متعلق به این گروه را مدیریت می کند. سرپرستان باید بلافاصله هرگونه تغییر نقش پرسنلی که بر امنیت تأثیر می گذارد را به مدیر امنیت اطلاع دهند.

کاربر User

یک کاربر فردی است که به داده ها دسترسی دارد تا وظایف شغلی خود را انجام دهد. کاربران باید هر روش و سیاست های امنیتی را برای داده هایی که به آنها دسترسی دارند، درک کنند. سرپرست مسئول اطمینان از اینکه کاربران دارای حقوق دسترسی مناسب می باشند، هستند.

توجه داشته باشید

گاهی اوقات بهترین و تخصصی ترین روش برای عیب یابی و رفع مشکل سیستم عامل ها، اپلیکیشن ها و سرویس ها، بررسی فایل های log است. فایل هایی که اپلیکیشن یا سرویس مورد استفاده در رابطه با مجموعه فعالیت ها و عملکرد خودش، ایجاد می نماید. اما واقعا فایل log چیست و چطور می توانیم آن را پیدا کنیم؟

فایل log نوعی فایل کم حجم است که به طور اتوماتیک ایجاد می شود و دربردارنده اطلاعات وسیعی از رویدادها و اتفاقاتی است که در درون نرم افزار یا سیستم عامل اتفاق افتاده است. تمام این موارد در فایل log ثبت و ضبط می شوند. در حقیقت آنها می توانند شامل طیف گسترده ای از موارد باشند و در اغلب اوقات فایل های log به منظور بررسی وقایعی که در طی عملکرد روزانه یک سیستم عامل یا اپلیکیشن روی داده اند، مورد استفاده قرار می گیرند.

به عنوان مثال فرض کنید شما از یک برنامه پشتیبان گیری برای گرفتن یک نسخه پشتیبان از فایل های پتان استفاده کرده اید. در این حالت به طور اتوماتیک یک فایل log ایجاد خواهد شد و به شما دقیقا نشان خواهد داد که در طی این رویه (پروسه) چه اتفاقاتی افتاده (یا نیفتاده) است. ویندوز این مجموعه از فایل های log را برای خدمات مختلف بایگانی کرده و نگهداری می کند.

در حقیقت هدف اصلی فایل‌های log پیگیری و نظارت دقیق بر اتفاقات پشت پرده است و از این طریق می‌توانید متوجه شوید در پس یک رویداد پیچیده نرم‌افزاری چه اتفاقاتی رخ داده است و به فهرست دقیقی از رویدادها، خرابی‌ها، اشتباهات و موارد مشابه دسترسی داشته باشید. اساساً هر حرکت و اقدامی که یک سرور، برنامه یا سیستم عامل انجام داده است و یا نتوانسته انجام دهد در این فایل‌ها ثبت می‌گردد.

با اینکه در بیشتر موارد این فایل‌ها با پسوند (log) در سیستم‌ها یا برنامه‌ها دیده می‌شوند ولی در برخی اپلیکیشن‌ها یا سیستم عامل‌ها از پسوند (txt) و مواردی از این دست برای ایجاد فایل‌های log استفاده می‌کنند. چگونه یک فایل log را باز کنیم؟

از آنجایی که اکثر فایل‌های log به صورت متون ساده نوشته می‌شوند، پس به راحتی می‌توانید با برنامه‌های ویرایشگر متن اقدام به باز نمودنشان نمایید. به طور پیش‌فرض در سیستم عامل ویندوز این امکان وجود دارد تا از نرم‌افزار ساده Notepad برای باز کردن یک فایل log استفاده کنید.

ممیز، مامور رسیدگی Auditor

ممیز فعالیت‌های کاربر را رصد می‌کند تا تضمین کند که کنترل‌های مناسب وجود دارد. ممیزها برای تأیید پیروی از سیاست‌های امنیتی، نیاز به دسترسی به کلیه ممیزی و logهای رخدادها دارند. باید توجه داشت از ممیزهای داخلی و خارجی هم می‌توان استفاده کرد.

چارچوبهای کنترل Control Frameworks

بسیاری از سازمانها چارچوب مدیریت و مدیریت فرآیندهای امنیتی را برای کمک به متخصصان امنیت طراحی کرده اند. این چارچوب‌ها و روش‌ها عبارتند از: استانداردهای توسعه برنامه‌های امنیتی، چارچوب توسعه معماری امنیتی و سازمانی، روش‌های توسعه کنترل امنیتی، روش‌های حاکمیتی شرکت، و روش‌های مدیریت فرایند. در این بخش چارچوب‌ها و روش‌های زیر مورد بحث قرار می‌گیرد:

- ISO/IEC 27000 Series
- Zachman Framework
- TOGAF
- DoDAF
- MODAF

- SABSA
- CobIT
- NIST
- COSO
- ITIL
- Six Sigma
- CMMI
- CRAMM
- رویکرد بالا به پایین در مقابل رویکرد پایین به بالا Top-down versus bottom-up approach
- چرخه عمر برنامه امنیتی Security program life cycle

ISO / IEC 27000 Series

سازمان بین المللی استاندارد سازی (ISO)، که غالبا به نادرستی به عنوان سازمان بین المللی استاندارد شناخته می شود، با کمیسیون بین المللی الکتروتکنیکال (IEC)، سازمان استاندارد بریتانیا ۷۷۹۹ (BS7799) را به یک استاندارد جدید جهانی که در حال حاضر به عنوان استاندارد ISO 27000 Series معرفی می کند. ISO 27000 یک استاندارد توسعه برنامه امنیتی در مورد نحوه توسعه و نگهداری سیستم مدیریت امنیت اطلاعات (ISMS) است. سری ۲۷۰۰۰ شامل لیستی از استانداردها است که هر کدام به یک جنبه خاص از ISMS می پردازد. این استانداردها منتشر شده یا در حال توسعه هستند. استانداردهای زیر به عنوان بخشی از سری ISO / IEC 27000 در این مبحث گنجانده شده است :

- 27000: مرور کلی ISMS و واژگان منتشر شده
- 27001: برای ISMS منتشر شده
- 27002: کد اجرا برای کنترل های امنیت اطلاعات
- 27003: دستورالعمل های اجرایی ISMS
- 27004: دستورالعمل های اندازه گیری ISMS
- 27005: دستورالعمل های مدیریت امنیت اطلاعات
- 27006: الزامات منتشر شده برای موسساتی که ممیزی و صدور گواهینامه ISMS را تأمین می کنند
- 27007: دستورالعمل های ممیزی ISMS
- 27008: ممیزی منتشر شده از دستورالعمل های ISMS

- 27010: مدیریت امنیت اطلاعات منتشر شده درون سازمانی و بیرون سازمانی برای دستورالعمل‌های ارتباطات
- 27011: دستورالعمل‌های مدیریت امنیت اطلاعات منتشر شده توسط سازمان‌های مخابراتی
- 27013: پیاده سازی یکپارچه از دستورالعمل ISO / IEC 27001 و ISO / IEC 20000-1
- 207014: دستورالعمل‌های حاکم بر امنیت اطلاعات منتشر شده
- 27015: انتشار خدمات مالی دستورالعمل‌های مدیریت امنیت اطلاعات
- 27016: دستورالعمل‌های اقتصاد سازمانی ISMS را منتشر کرد
- 27017: دستورالعمل‌های کنترل امنیت اطلاعات خدمات رایانش ابری در حال توسعه مبتنی بر ISO / IEC 27002
- 27018: کد منتشر شده برای حفاظت از اطلاعات قابل شناسایی شخصی PII در ابرهای عمومی به عنوان پردازنده‌های PII عمل می‌کنند
- 27019: سیستم کنترل فرایند تولید سیستم‌های انرژی منتشر شده ISMS بر اساس ISO / IEC 27002
- 27021: الزامات صلاحیت‌های منتشر شده برای متخصصین سیستم‌های مدیریت امنیت اطلاعات
- 27023: نقشه برداری منتشر شده نسخه‌های اصلاح شده ISO / IEC 27001 و ISO / IEC 27002
- 27031: دستورالعمل‌های تداوم کسب و کار برای آمادگی فناوری اطلاعات و ارتباطات
- 27032: دستورالعمل‌های امنیتی سایبری
- 27033-1: مرور کلی و مفاهیم امنیت شبکه
- 27033-2: دستورالعمل پیاده سازی و انتشار طراحی امنیت شبکه
- 27033-3: تهدیدات امنیت شبکه منتشر شده، تکنیک‌های طراحی، و دستورالعمل‌های مربوط به مسائل مربوط به کنترل
- 27033-4: انتشار امنیت ارتباطات بین شبکه‌ها با استفاده از دروازه‌های امنیتی
- 27033-5: انتشار امنیت ارتباطات در شبکه‌ها با استفاده از شبکه‌های خصوصی مجازی (VPN ها)
- 27033-6: در حال توسعه امنیت دسترسی IP شبکه بی سیم
- 27034-1: مرور کلی و مفاهیم امنیت نرم افزار
- 27034-2: دستورالعمل‌های چارچوب هنجاری سازمان امنیت اپلیکیشن در حال توسعه
- 27034-3: دستورالعمل‌های فرایند مدیریت امنیت اپلیکیشن در حال توسعه
- 27034-4: دستورالعمل‌های اعتبار سنجی امنیت اپلیکیشن در حال توسعه

- 27034-5: پروتکل های امنیتی اپلیکیشن در حال توسعه و کنترل دستورالعمل های ساختار داده
- 27034-6: دستورالعمل های امنیتی توسعه برای اپلیکیشن های خاص
- 27034-7: راهنمای در حال توسعه برای پیش بینی صحت امنیت اپلیکیشن
- 27035: دستورالعمل های مدیریت حوادث امنیت اطلاعات
- 27035-1: اصول مدیریت حادثه امنیت اطلاعات در حال توسعه
- 27035-2: دستورالعمل های آمادگی برای پاسخگویی به رخدادهای امنیت اطلاعات در حال توسعه
- 27035-3: دستورالعمل های مربوط به تیم واکنش به حادثه امنیت رایانه (CISRT) در حال توسعه
- 27036-1: امنیت اطلاعات منتشر شده برای نمای کلی و مفاهیم روابط عرضه کننده
- 27036-2: امنیت اطلاعات منتشر شده برای روابط عرضه کننده دستورالعمل های مورد نیاز مشترک
- 27036-3: انتشار اطلاعات و تکنولوژی ارتباطات ICT دستورالعمل های امنیتی زنجیره تامین
- 27036-4: دستورالعمل های در حال توسعه برای امنیت سرویس Cloud
- 27037: انتشار مدارک شناسایی دیجیتالی، دستورالعمل جمع آوری، مالکیت، و حفظ و نگهداری
- 27038: مشخصات امنیت ویرایش دیجیتالی
- 27039: دستورالعمل انتخاب، استقرار و عملیات منتشر شده IDS
- 27040: دستورالعمل های امنیتی منتشر شده ذخیره سازی
- 27041: راهنمایی در جهت اطمینان از مناسب بودن و کفایت روش تحقیق حادثه
- 27042: دستورالعمل تفسیر تجزیه و تحلیل شواهد دیجیتالی
- 27043: اصول و فرآیندهای تحقیق در مورد حوادث
- 27044: دستورالعمل های مربوط به امنیت اطلاعات در حال توسعه و مدیریت رخداد SIEM
- 27050: دستورالعمل های کشف الکترونیکی در حال توسعه eDiscovery
- 27799: امنیت اطلاعات منتشر شده در مورد دستورالعمل های سازمان های بهداشتی

چارچوب Zachman

چارچوب Zachman، یک چارچوب معماری سازمانی و یک سیستم طبقه بندی دو بعدی است که براساس شش سوال ارتباطی (چطور، کجا، کی، چرا، چه کسی و چگونه) (What, Where, When, Why, Who, How) که با دیدگاه های متفاوت (برنامه ریز، مالک، طراح، سازنده، پیمانکار و سیستم واقعی (Owner, Planner, Designer, Builder, Subcontractor) روبرو هستند، این

سیستم اجازه می‌دهد تا تجزیه و تحلیل یک سازمان را که مربوط به مسئولیت‌های گروه می‌باشد به گروه‌های مختلف در سازمان ارائه شود. اگر چه این چارچوب امنیت محور نیست، اما با استفاده از این چارچوب به ما کمک می‌شود تا اطلاعات را برای پرسنل در یک زبان و در قالبی که برای آنها مفید باشد، انتقال دهیم.

چارچوب معماری گروه باز (The Open Group Architecture Framework (TOGAF)

TOGAF، یکی دیگر از چارچوب معماری سازمانی که به سازمانها کمک می‌کند تا معماری اطلاعات سازمانی را طراحی، برنامه ریزی، پیاده سازی و مدیریت کنند و بر اساس چهار حوزه با یکدیگر مرتبط می‌باشند: فناوری، اپلیکیشن‌ها، داده‌ها و کسب و کار.

چارچوب معماری وزارت دفاع (Department of Defense Architecture Framework (DoDAF)

DoDAF یک چارچوب معماری است که مجموعه‌ای از محصولات را تحت هشت مورد نمایش می‌دهد: همه دیدگاه (مورد نیاز) (AV)، دیدگاه قابلیت (CV)، دیدگاه داده و اطلاعات (DIV)، دیدگاه عملیات (OV)، دیدگاه پروژه (PV) دیدگاه خدمات (SvcV)، دیدگاههای استاندارد (STDV) و دیدگاه سیستم (SV) استفاده می‌شود تا تضمین شود که فناوری‌های جدید DoD به طور مناسب با زیرساخت‌های فعلی ادغام می‌شوند.

all viewpoint (AV), capability viewpoint (CV), data and information viewpoint (DIV), operation viewpoint (OV), project viewpoint (PV), services viewpoint (SvcV), standards viewpoint (STDV), systems viewpoint (SV).

چارچوب معماری وزارت دفاع بریتانیا (British Ministry of Defence (MODAF Architecture Framework

یک چارچوب معماری است که اطلاعات را به هفت دیدگاه تقسیم می‌کند: دیدگاه استراتژیک (StV)، دیدگاه عملیاتی (OV)، دیدگاه سرویس گرا (SOV)، دیدگاه سیستم (SV)، دیدگاه اکتساب یا مالکیت (AcV)، دیدگاه فنی (TV)، و تمام دیدگاه (AV).

strategic viewpoint (StV), operational viewpoint (OV), service-oriented viewpoint (SOV), systems viewpoint (SV), acquisition viewpoint (AcV), technical viewpoint (TV), and all viewpoint (AV).

توجه داشته باشید

سازمانها بایستی چارچوب معماری سازمانی را به شیوه ای مناسب تر، بر اساس نیازهای ذینفعان، انتخاب کنند.

معماری امنیتی کسب و کار کاربردی شرود Sherwood Applied Business Security Architecture (SABSA)

SABSA یک چارچوب معماری امنیتی سازمانی می باشد که شبیه چارچوب Zachman است و با استفاده از شش سوال ارتباطی (چه، کجا، زمانی، چرا، چه کسی و چگونه) (What, Where, When, Why, Who, and How) با شش لایه (عملیاتی، جزء، فیزیکی، منطقی، مفهومی و متنی) contextual (operational, component, physical, logical, conceptual) متقاطع است، و باید توجه داشت که یک معماری مبتنی بر ریسک است، که در جدول ۱-۱ را مشاهده می شود.

Viewpoint	Layer	Assets (What)	Motivation (Why)	Process (How)	People (Who)	Location (Where)	Time (When)
Business	Contextual	Business	Risk model	Process model	Organizations and relationships	Geography	Time dependencies
Architect	Conceptual	Business attributes profile	Control objectives	Security strategies and architectural layering	Security entity model and trust framework	Security domain model	Security-related lifetimes and deadlines
Designer	Logical	Business information model	Security policies	Security services	Entity schema and privilege profiles	Security domain definitions and associations	Security processing cycle
Builder	Physical	Business data model	Security rules, practices, and procedures	Security mechanism	Users, applications, and interfaces	Platform and network infrastructure	Control structure execution
Tradesman	Component	Detailed data structures	Security standards	Security tools and products	Identities, functions, actions, and ACLs	Processes, nodes, addresses, and protocols	Security step timing and sequencing
Facilities Manager	Operational	Operational continuity assurance	Operation risk management	Security service management and support	Application and user management and support	Site, network, and platform security	Security operations schedule

جدول ۱-۱ ماتریس چارچوب SABSA

اهداف کنترل اطلاعات و فن آوری مرتبط (CobiT)

CobiT یک چارچوب توسعه کنترل امنیتی است که پنج اصل را ارائه می‌دهد:

ملاقات با نیازهای ذینفع

پوشش ساختاری به صورت END- TO-END

اعمال یک چارچوب یکپارچه

فعال کردن یک رویکرد جامع

حاکمیت جدا از مدیریت

این پنج اصل، اهداف کنترل را به هفت توانمندی تقسیم می‌کنند:

اصول، سیاست‌ها و چارچوب‌ها

فرآیندها

ساختار سازمانی

فرهنگ، اخلاق و رفتار

اطلاعات

خدمات، زیرساخت‌ها و برنامه‌های کاربردی

افراد، مهارت‌ها و شایستگی‌ها

مؤسسه ملی استاندارد و فناوری (NIST) انتشار ویژه

National Institute of Standards and Technology (NIST) Special Publication (SP)

NIST SP 800-53 یک چارچوب توسعه کنترل امنیت است که توسط سازمان NIST وزارت

بازرگانی ایالات متحده توسعه یافته است. SP 800-53 کنترل‌ها را به سه دسته تقسیم می‌کند:

فنی، عملیاتی، مدیریتی. هر کلاس دارای خانواده یا دسته‌های کنترل می‌باشد.

جدول ۱-۲ لیست خانواده NIST SP 800-53 می‌باشد.

Family	Class
Access Control (AC)	Technical
Awareness and Training (AT)	Operational
Audit and Accountability (AU)	Technical
Security Assessment and Authorization (CA)	Management
Configuration Management (CM)	Operational
Contingency Planning (CP)	Operational
Identification and Authentication (IA)	Technical
Incident Response (IR)	Operational
Maintenance (MA)	Operational
Media Protection (MP)	Operational
Physical and Environmental Protection (PE)	Operational
Planning (PL)	Management
Program Management (PM)	Management
Personnel Security (PS)	Operational
Risk Assessment (RA)	Management
System and Services Acquisition (SA)	Management
System and Communications Protection (SC)	Technical
System and Information Integrity (SI)	Operational

جدول ۱-۲: NIST SP 800-53 کنترل خانواده

NIST 800-55 یک چارچوب معیارهای امنیت اطلاعات است که راهنمایی در مورد توسعه روش‌های اندازه گیری عملکرد را با دیدگاه دولت ایالات متحده ارائه می‌دهد. کمیته سازمان‌های حمایت کننده (COSO) چارچوب کمیسیون تردد

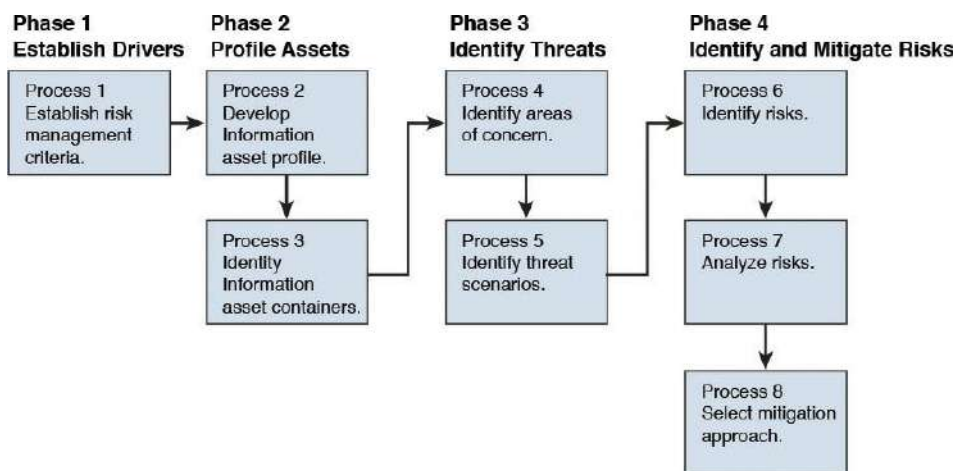
Committee of Sponsoring Organizations (COSO) of the Treadway Commission Framework

یک چارچوب حاکمیت شرکتی است که متشکل از پنج مولفه مرتبط است: محیط کنترل، ارزیابی ریسک، فعالیت‌های کنترل، اطلاعات و ارتباطات، و فعالیت‌های نظارت. CobiT از چارچوب COSO استخراج شده است. COSO F حاکمیت شرکتی می‌باشد و CobiT متعلق به مدیریت IT است.

تهدید بحرانی عملیاتی، ارزیابی آسیب پذیری و دارایی (OCTAVE)

Operationally Critical Threat, Asset and Vulnerability Evaluation

OCTAVE، که توسط موسسه مهندسی نرم افزار دانشگاه Carnegie Mellon توسعه یافته است و مجموعه‌ای از ابزارها، تکنیک‌ها و روش‌های ارزیابی و برنامه ریزی استراتژیک امنیت اطلاعات مبتنی بر ریسک را فراهم می‌کند. با استفاده از OCTAVE، یک سازمان تیم‌های کوچک را در بخش‌های کسب و کار و IT ادغام می‌کند تا با نیازهای امنیتی سازمان سازگار شوند. شکل ۱-۲ مراحل و فرآیندهای OCTAVE Allegro، آخرین نسخه OCTAVE را نشان می‌دهد.



شکل ۱-۲: مراحل و فرآیندهای OCTAVE Allegro

کتابخانه زیرساخت فناوری اطلاعات (ITIL) Information Technology Infrastructure Library

ITIL یک استاندارد توسعه مدیریت فرایند است که توسط اداره مدیریت و بودجه OMB Circular A-130 تهیه شده است. ITIL دارای پنج نشریه اصلی است: استراتژی سرویس ITIL، طراحی خدمات ITIL، انتقال خدمات ITIL، عملیات سرویس ITIL و ارتقاء خدمات مداوم ITIL. این پنج نشریه اصلی شامل ۲۶ پروسه است. گرچه ITIL دارای یک مولفه امنیتی می‌باشد، در درجه اول به مدیریت توافقات سطح خدمات (SLAs) بین یک بخش IT یا سازمان و مشتریان آن مربوط می‌شود و همینطور به عنوان بخشی از OMB Circular A-130 نیز می‌باشد، بررسی مستقل کنترل‌های امنیتی هر سه سال یکبار انجام می‌شود.

جدول ۳-۱ لیست پنج نشریه اصلی ITIL نسخه ۳ و ۲۶ فرآیند درون آنها را فهرست می کند.

ITIL Service Strategy	ITIL Service Design	ITIL Service Transition	ITIL Service Operation	ITIL Continual Service Improvement
Strategy Management	Design Coordination	Transition Planning and Support	Event Management	Continual Service Improvement
Service Portfolio Management	Service Catalogue	Change Management	Incident Management	
Financial Management for IT Services	Service Level Management	Service Asset and Configuration Management	Request Fulfillment	
Demand Management	Availability Management	Release and Deployment Management	Problem Management	
Business Relationship Management	Capacity Management	Service Validation and Testing	Access Management	
	IT Service Continuity Management	Change Evaluation		
	Information Security Management System	Knowledge Management		
	Supplier Management			

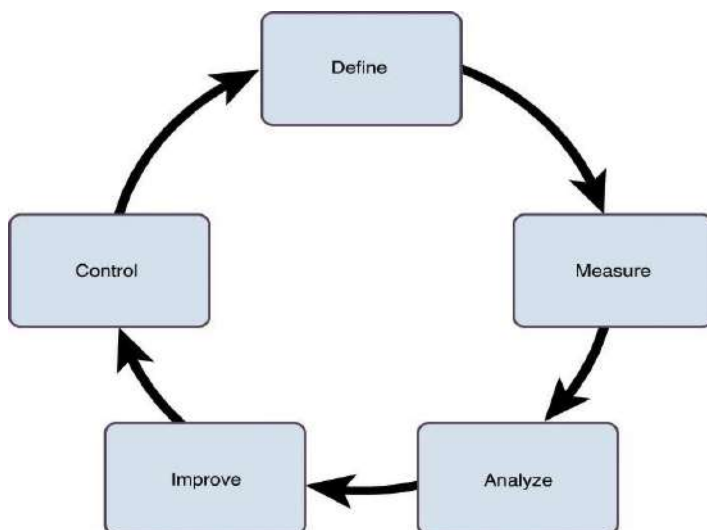
جدول ۳-۱: انتشارات اصلی و فرآیندهای ITIL v3

شش سیگما Six Sigma

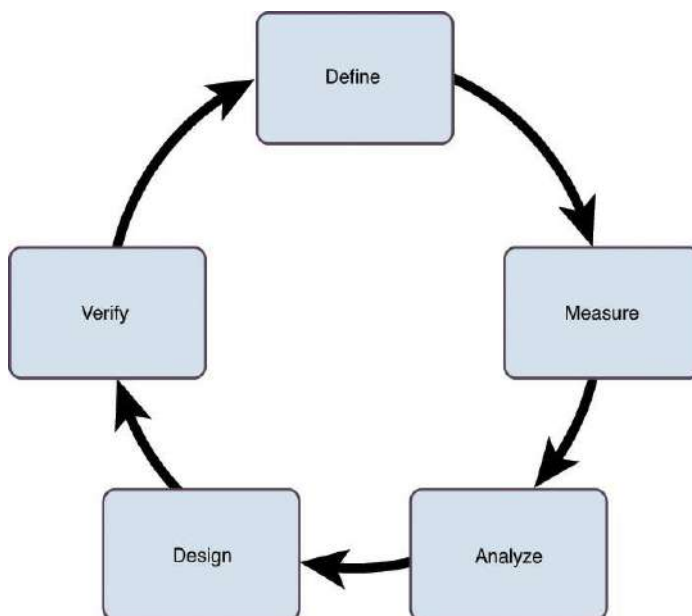
شش سیگما یک استاندارد بهبود فرایند است که شامل دو روش پروژه‌های است که از چرخه (طرح-اجرا در مقیاس کوچک -بررسی-اقدام) (Plan-Do-Check-Act) دمینگ الهام گرفته شده است:

روش DMAIC که شامل تعریف، اندازه گیری، تجزیه و تحلیل، بهبود و کنترل می باشد و روش DMADV شامل تعریف، اندازه گیری، تجزیه و تحلیل، طراحی و تأیید است. شش سیگما برای شناسایی و حذف نقص در فرآیند تولید طراحی شده است، اما می تواند در بسیاری از عملکردهای کسب و کار، از جمله امنیت، اعمال شود.

درمورد چرخه دمینگ بعداً بحث خواهد شد.
 شکل ۳-۱ و ۴-۱ هر دو روش‌های شش سیگما را نشان می‌دهد.



شکل ۳-۱: شش سیگما DMAIC



شکل ۴-۱: DMADV شش سیگما

ادغام مدل بلوغ قابلیت (CMMI) Capability Maturity Model Integration

یک رویکرد بهبود فرآیند است که در سه حوزه مورد توجه قرار می گیرد: توسعه محصول و خدمات (CMMI برای توسعه)، ایجاد خدمات و مدیریت (CMMI برای خدمات) و مالکیت محصول (CMMI برای مالکیت). CMMI دارای پنج مرحله بلوغ برای فرآیندها است: سطح ۱ ابتدایی، سطح ۲ مدیریت شده، سطح ۳ تعریف شده، سطح ۴ کمی مدیریت، و سطح ۵ بهینه سازی. تمام مراحل به یکی از پنج سطح بلوغ اختصاص می یابد.

تجزیه و تحلیل ریسک CCTA و روش مدیریت (CRAMM)

CCTA Risk Analysis and Management Method (CRAMM)

CRAMM یک تجزیه و تحلیل ریسک کیفی و ابزار مدیریتی است که توسط مرکز رایانه بریتانیا و آژانس ارتباطات دولت انگلیس CCTA طراحی شده است. بررسی CRAMM شامل سه مرحله است:

۱ شناسایی و ارزش دارایی ها.

۲ شناسایی تهدیدات و آسیب پذیری ها و محاسبه ریسکها.

۳ شناسایی و اولویت بندی کردن اقدامات متقابل.

تذکر: هیچ سازمانی کلیه چارچوبها یا روشهای فوق الذکر را اجرا نخواهد کرد. متخصصان امنیت باید به سازمان خود کمک کنند چارچوبی را انتخاب کنند که به بهترین وجه متناسب با نیاز سازمان باشد.

رویکرد بالا به پایین در مقابل پایین به بالا Top-Down Versus Bottom-Up Approach

در یک رویکرد بالا به پایین، مدیریت برنامه های امنیتی را آغاز، پشتیبانی و هدایت می کند. در یک رویکرد پایین به بالا، کارکنان قبل از دریافت مسیر و حمایت از مدیریت، یک برنامه امنیتی را توسعه می دهند. یک رویکرد بالا به پایین کارآمدتر از رویکرد پایین به بالا است، زیرا پشتیبانی مدیریت یکی از مهمترین اجزای برنامه امنیتی است.

چرخه عمر برنامه امنیتی Security Program Life Cycle

هر برنامه امنیتی یک چرخه عمر مداوم دارد و باید دائماً بررسی و بهبود یابد. چرخه عمر برنامه امنیتی مراحل زیر را شامل می‌شود.

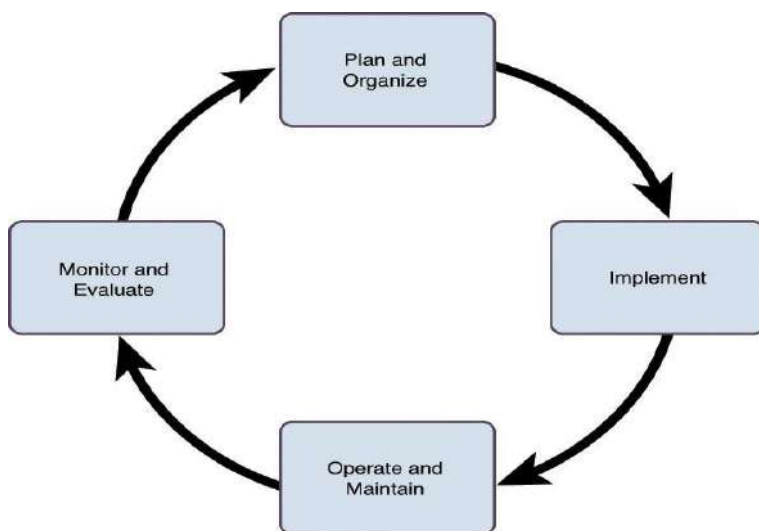
۱. طرح و سازماندهی Plan and Organize: شامل ارزیابی ریسک، ایجاد کمیته مدیریت و فرماندهی، ارزیابی حرکت دهندگان کسب و کار و کسب تایید مدیریت است.

۲. پیاده سازی Implement: شامل شناسایی و مدیریت دارایی ها، مدیریت ریسک، مدیریت هویت و کنترل دسترسی، آموزش امنیت و آگاهی، اجرای راه حل ها، اعطای نقش و ایجاد اهداف است.

۳. اداره و نگهداری Operate and Maintain: شامل اجرای ممیزی، انجام وظایف و مدیریت SLA است.

۴. نظارت و ارزیابی Monitor and Evaluate: شامل بررسی ممیزی و log ها، ارزیابی اهداف امنیتی و تهیه طرح‌های بهبود برای ادغام در طرح و مرحله سازماندهی (مرحله ۱).

شکل ۱-۵ یک نمودار چرخه عمر برنامه را نشان می‌دهد.



شکل ۱-۵: چرخه عمر برنامه امنیتی

مراقبت مناسب Due Care

مراقبت مناسب به این معنی است که یک سازمان برای جلوگیری از نقض امنیت تمام اقدامات معقول را انجام داده و همچنین در جهت کاهش خسارات ناشی از نقض های موفقیت آمیز گام برمی دارد که شامل اطمینان از اجرای صحیح سیاستها، رویه ها و استانداردها است. مراقبت دقیق همه چیز در مورد عملکرد است. سازمانها باید برای کلیه داراییهای سازمان، به ویژه مالکیت معنوی، حمایت و رویه های مناسب را اعمال کنند. در مراقبت مناسب، عدم رعایت حداقل استانداردها و عملکردها، غفلت تلقی می شود. اگر سازمانی اقداماتی را انجام نداد که شخص محتاط در چنین شرایطی انجام می دهد، سازمان غفلت کرده است.

مطالعه دقیق Due diligence

به این معنی است که یک سازمان تمام آسیب پذیری ها را مورد بررسی قرار داده است که شامل اجرای یک ممیزی مناسب و ارزیابی برای اطمینان در حفاظت سازمان است. تلاش در جمع آوری اطلاعات خلاصه می شود. سازمانها باید رویه های مناسب را برای تعیین هر گونه ریسکی برای دارایی های سازمانی ایجاد کنند. پس از اتمام کار، اطلاعات لازم برای اطمینان از اینکه سازمان به دقت مورد توجه قرار گرفته است، فراهم می شود. بدون مطالعه دقیق و بررسی کافی، دقت لازم نمی تواند رخ دهد.

مطالعه دقیق شامل بررسی پس زمینه کارمند، چک های اعتباری شریک کسب و کار، ارزیابی امنیت سیستم، ارزیابی ریسک، آزمایش نفوذ و برنامه ریزی و آزمایش بهبود فاجعه است NIST SP 800-53 که قبلا در این فصل مورد بحث قرار گرفته است، در قسمت "چارچوب های کنترل"، راهنمایی برای اجرای کنترل های امنیتی است که به مطالعه دقیق کمک می کند.

مراقبت مناسب و مطالعه دقیق در مدیریت حاکمیت و مدیریت ریسک نقش دارند. همانطور که می بینید، مراقبت مناسب و هم مطالعه دقیق به یک رابطه وابسته می باشند. هنگامی که مطالعه دقیق رخ می دهد، سازمانها زمینه های ریسک را تشخیص می دهند. مثال شامل یک سازمان است که پرسنل به طور منظم مسائل امنیتی اولیه را درک نمی کنند، مستندات چاپی مناسب نیستند و کارکنان دسترسی به فایل هایی را دارند که نباید داشته باشند. هنگامی که به دقت مورد توجه قرار می گیرد، سازمانها زمینه های ریسک را شناسایی می کنند و طرح هایی را برای محافظت در برابر ریسکها در نظر می گیرند. برای مطالعه دقیق شناسایی شده، نمونه هایی که

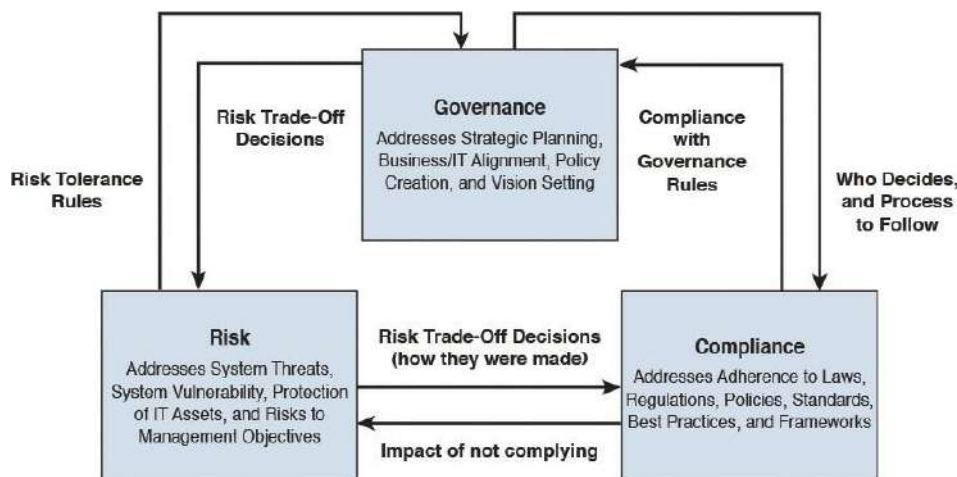
باید به آنها توجه شود، شامل آموزش آگاهی از امنیت پرسنل، قرار دادن روش هایی برای تخریب مناسب اسناد چاپی و اجرای کنترل دسترسی مناسب برای کلیه فایل ها است.

انطباق Compliance

انطباق شامل هماهنگی با استانداردها، دستورالعمل ها، مقررات و یا قانون است. یک سازمان باید با قوانین و مقررات دولتی مطابقت داشته باشد. با این حال، انطباق با سازمان های استاندارد و انجمن های صنفی اختیاری است.

تمام متخصصان امنیت باید استانداردها، دستورالعمل ها، مقررات و قوانین مربوط به امنیت و حفظ حریم خصوصی را درک کنند. معمولاً این موارد صنعت خاصی را شامل می شود، به این معنی که استانداردها، دستورالعمل ها، مقررات و قوانین بر اساس نوع کسب و کار سازمان درگیر هستند. مثال خوب در این مورد صنعت مراقبت های پزشکی است. با توجه به قانون حمل و نقل و مسئولیت پذیری بیمه بهداشت (HIPAA)، سازمان های مراقبت های پزشکی باید از مقررات مربوط به نحوه جمع آوری، استفاده، ذخیره و حفاظت از PII استفاده کنند. اغلب باید به دولت ها و سازمان های محلی، منطقه ای، ایالتی، فدرال و افراد توجه شود.

سازمان ها و متخصصان امنیت که آنها را به کار می گیرند باید تعیین کنند که چه قوانینی را باید رعایت کنند. یک سازمان باید سخت ترین قوانینی را که باید رعایت شود، اتخاذ کند. اگر قوانین با یکدیگر تعارض داشته باشند، سازمان ها باید زمان لازم را برای تعیین اینکه کدام قانون باید اولویت داشته باشد، بکار گیرند. این تصمیم می تواند براساس نوع داده، نوع صنعت، روش جمع آوری داده ها، استفاده از داده ها یا اقامت فردی از کسانی که PII را جمع آوری می کنند، باشد. هر گونه بحث در مورد رعایت نکردن یک روش حاکمیت، مدیریت ریسک، انطباق (GRC)، بدون چون و چرا ناقص است. حاکمیت شامل فعالیتهای اصلی سازمان، اقتدار درون سازمان، پاسخگویی سازمانی و اندازه گیری عملکرد می باشد. مدیریت ریسک شامل شناسایی، تحلیل، ارزیابی و نظارت بر ریسک می باشد. انطباق تضمین می کند که فعالیتهای سازمانی مطابق با قوانین ایجاد شده است. هر یک از سه هدف مجزا، ورودی و اهداف را به اهداف دیگر تبدیل می کند. رابطه GRC در شکل ۱-۶ نشان داده شده است.



شکل ۱-۶: روابط GRC (governance, risk management, compliance)

به عنوان بخشی از بحث در مورد انطباق، متخصصان امنیت باید در بلند مدت قوانین و مقررات و شرایط مربوط به حفظ حریم خصوصی را درک کنند.

انطباق تنظیم و قانونگذاری Legislative and Regulatory Compliance

هیچ سازمانی در حباب فعالیت نمی‌کند. همه سازمان‌ها تحت قوانین، مقررات و رعایت الزامات قرار می‌گیرند. متخصصان امنیت باید قوانین و مقررات کشور یا کشورهای را که در آن فعالیت می‌کنند و همچنین صنعتی که در آن فعالیت می‌کنند، درک کنند. در بسیاری از موارد، قوانین و مقررات به نحوی نوشته شده که به موجب آن اقدامات خاصی باید انجام شود. با این حال، مواردی وجود دارد که قوانین و مقررات را در اختیار سازمان قرار می‌دهد تا تعیین کنند که چگونه باید تطابق داشته باشند.

ایالات متحده و اتحادیه اروپا هر دو قوانین و مقرراتی را ایجاد کرده‌اند که بر روی سازمان‌هایی که در حوزه حاکمیت خود کار می‌کنند، تاثیر می‌گذارد. در حالی که متخصصان امنیت باید تلاش کنند تا قوانین و مقررات را درک کنند، ممکن است متخصصان امنیت سطح دانش و زمینه‌ای برای تفسیر این قوانین و مقررات برای محافظت از سازمان خود نداشته باشند. در این موارد، متخصصان امنیت باید با توجه به نمایندگی‌های قانونی در زمینه انطباق تنظیم و قانونگذاری فعالیت کنند.

انطباق با الزامات حریم خصوصی Privacy Requirements Compliance

رعایت موارد مربوط به حفظ حریم خصوصی اساسا مربوط به محرمانه بودن داده ها، به ویژه اطلاعات شناسایی شخصی PII (personal Identifiable Information) است.

PII به طور فزاینده‌ای تحت حمله در دنیای مدرن قرار دارد. تقریباً روزانه یک شرکت جدید، سازمان یا حتی نهاد دولتی اعلام می‌کند که PII در مورد مشتریان، کارکنان و یا حتی عوامل دولتی به خطر افتاده است. این سازش به شهرت سازمان آسیب می‌رساند و همچنین می‌تواند منجر به خسارت شود.

ایالات متحده و اتحادیه اروپا قوانین، مقررات و دستورالعمل‌های مربوط به جمع آوری، انتقال، نگهداری و انتقال PII را با هدف محافظت از افشای این اطلاعات به اشخاص غیر مجاز، تصویب کرده‌اند. متخصصان امنیت مسئول تأمین نیازهای مدیریتی و پیامدهای ناسازگار هستند. به روز ماندن در مورد آخرین تحولات مربوط به PII بسیار مهم است.

مسائل حقوقی و مقررات Legal and Regulatory Issues

مسائل حقوقی و مقررات که امروزه بر سازمان‌ها تأثیر می‌گذارد، با استفاده از رایانه‌ها و شبکه‌ها گسترش یافته است. در گذشته امنیت فیزیکی داده‌ها تنها دغدغه بود. با پیشرفت‌های تکنولوژیکی، راه‌های حملات رو به افزایش می‌باشد. در این بخش مفاهیم جرم رایانه‌ای، سیستم‌های حقوقی ارشد، مجوز و مالکیت معنوی، کنترل‌های واردات / صادرات، جریان داده‌های بین‌المللی و فرا مرزی، حریم خصوصی و نقض داده‌ها را مورد بحث قرار می‌دهد.

مفاهیم جرایم رایانه‌ای Computer Crime Concepts

معمولاً جرایم رایانه‌ای امروزه توسط بی‌دقتی قربانی امکان پذیر است. اگر جرم رایانه‌ای رخ دهد، اغلب اثبات قصد و عواقب جرایم دشوار است. تحقیق جرایم رایانه‌ای و پیگرد قانونی دشوار می‌باشد، زیرا شواهد بیشتر مستقیم است. علاوه بر اثرگذاری بر بررسی جرایم رایانه‌ای، واقعیت این است که دستیابی به شواهدی از فعالیت‌های انجام شده در رایانه بسیار دشوار است. به دلیل مسائل مربوط به جرم رایانه‌ای، مهم است که متخصصان امنیت، مفاهیم جرم رایانه‌ای زیر را درک کنند:

- جرایم به کمک رایانه Computer-assisted crime

- جرایم رایانه‌ای هدفمند Computer-targeted crime
- جرایم تصادفی رایانه‌ای Incidental computer crime
- جرایم شایع رایانه‌ای Computer prevalence crime
- هکرها در مقابل کراکرها Hackers versus crackers

جرایم به کمک رایانه Computer-assisted crime

جرم به کمک رایانه هنگامی اتفاق می‌افتد که از رایانه به عنوان ابزاری برای کمک به ارتکاب جرم استفاده شود. این نوع جرم می‌تواند بدون رایانه انجام شود اما از رایانه برای آسان تر کردن ارتکاب جرم استفاده می‌شود. به این روش فکر کنید: جنایتکاران می‌توانند داده‌های سازمانی محرمانه را در بسیاری از شیوه‌های مختلف سرقت کنند. این جرم بدون رایانه امکان پذیر است. اما وقتی مجرمان برای کمک در سرقت اطلاعات سازمانی محرمانه از رایانه استفاده می‌کنند، در این صورت جرم به کمک رایانه رخ داده است.

جرایم رایانه‌ای هدفمند Computer-Targeted Crime

زمانی که یک رایانه، قربانی است و هدف این حمله تنها آسیب رساندن به رایانه و صاحب آن است. این نوع جرم نمی‌تواند بدون استفاده از رایانه انجام شود. جرایم رایانه‌ای که در این دسته قرار دارند عبارتند از انکار سرویس Denial-of-Service (DoS) و حملات سرریز بافر Buffer Overflow Attacks.

جرایم تصادفی رایانه‌ای Incidental computer crime

زمانی جرایم تصادفی رایانه‌ای، اتفاق می‌افتد که یک رایانه درگیر در یک جرم رایانه‌ای شود بدون اینکه قربانی یا مهاجم باشد. یک رایانه که به عنوان یک زامبی در یک Botnet مورد استفاده قرار می‌گیرد، بخشی از جرم تصادفی رایانه‌ای است.

جرایم شایع رایانه‌ای Computer prevalence crime

یک جرم شایع رایانه‌ای در واقعیت به این دلیل است که رایانه‌ها در جهان امروز به طور گسترده‌ای مورد استفاده قرار می‌گیرند. این نوع جرم فقط به خاطر وجود رایانه‌ها می‌باشد. دزدی نرم افزار نمونه‌ای از این نوع جرم است.

هکرها در مقابل کراکرها Hackers Versus Crackers

هکرها و کراکرها دو اصطلاح هستند که اغلب در رسانه‌ها جایگزین هم استفاده می‌شوند، اما در واقع معنای مشابهی ندارند. هکرها افرادی هستند که تلاش می‌کنند به سیستم‌های امن نفوذ کنند تا از این طریق به دانش در مورد سیستم‌ها دست یابند و احتمالا از آن دانش استفاده می‌کنند تا شواهد ارتکاب جرم و جنایت را تشخیص دهند. از سوی دیگر، Crackers افرادی هستند که سعی می‌کنند تا امنیت سیستم را بشکنند از این طریق به دانش در مورد سیستم‌ها دست یابند و برای اهداف نامطلوب استفاده کنند.

در دنیای امنیت، اصطلاح کلاه سفید، کلاه خاکستری، کلاه سیاه به راحتی قابل درک می‌باشد و نسبت به اصطلاحات هکرها و کراکرها، کمتر سردرگمی ایجاد می‌کند. کلاه سفید هیچ هدف مخربی ندارد. کلاه سیاه دارای اهداف مخرب می‌باشد و کلاه خاکستری در جایی در وسط دو نوع دیگر قرار دارد.

کلاه خاکستری به سیستم نفوذ میکند و به ادمین حفره امنیتی Administrator of Security Hole اطلاع می‌دهد و پیشنهاد می‌کند که برای حل مسائل امنیتی هزینه کند.

نمونه‌های جرم رایانه‌ای Computer Crime Examples

اکنون که شما دسته‌های مختلف جرم رایانه‌ای و افرادی را که مرتکب جنایات شده‌اند را درک کردید، در اینجا مناسب است نمونه‌هایی از جنایات رایانه‌ای را که امروزه شایع هستند، ارائه شود.

نرم افزار آنتی ویروس جعلی یا سرکش Fake or Rogue Antivirus اغلب بر روی رایانه‌ها نصب می‌شود، زیرا تاکتیک‌های مورد استفاده برای ترساندن قربانیان است. جعبه‌های Pop-up به کاربر اطلاع می‌دهد که آلوده به ویروس شده است. با کلیک بر روی دکمه در جعبه Pop-up، قربانی می‌تواند نرم افزار آنتی ویروس را خریداری و نصب کند، اما به صورت آگاهانه رایانه را با نرم افزارهای مخرب آلوده می‌کند. مرورگرهای وب امروز مکانیزم‌هایی را ایجاد می‌کنند که کاربران را قادر می‌سازد پیام‌های Pop-up را مسدود کنند. با این حال، معایبی وجود دارد که گاهی اوقات مانع ظاهر شدن پنجره‌های مورد نظر می‌شود. با یک پیکربندی ساده و ایجاد یک استثنا برای سایت‌های معتبر Pop-up، بهتر از غیر فعال کردن و مسدود کردن به طور کامل Pop-up است.

Ransomware یا باج افزار دسته خاصی از نرم افزار است که سعی در اخاذی پول از قربانیان احتمالی دارد. یک دسته از باج افزارها داده های کاربر را رمزگذاری می کنند تا زمانی که پرداختی به مهاجم انجام شود. دسته دیگر به کاربر گزارش می دهد که رایانه وی برای فعالیت های غیرقانونی استفاده شده است و برای جلوگیری از پیگرد قانونی باید جریمه ای نیز پرداخت شود. اما در این حالت، "جریمه" به عنوان یک مقام دولتی یا سازمان اجرای قانون، به مهاجم جهت پرداخت ابلاغ می شود. در بسیاری موارد، بدافزارها حتی پس از حذف باج افزار همچنان در پس زمینه فعالیت خود را ادامه می دهند. این بدافزار اغلب برای ارتکاب کلاهبرداری مالی بیشتر بر روی قربانی استفاده می شود.

Scareware دسته ای از نرم افزارها می باشد که رایانه را قفل می کند و به کاربر اخطار می دهد که نقض قوانین فدرال یا بین المللی رخ داده است. به عنوان بخشی از این حمله، بنر یا مرورگر کاربر را به وب سایت پورنوگرافی کودکان هدایت می کند. مهاجم ادعا می کند کاربر و اقداماتش را ضبط می کند. قربانی باید جریمه ای را بدهد تا کنترل رایانه را بازگرداند. ارتباط بین Scareware و Ransomware بسیار نزدیک است و اغلب سخت است که بین این دو تفاوت قائل شد.

اینها تنها چند نمونه از حملات رایانه ای هستند و مهاجمان هر روز روش های جدیدی را ایجاد می کنند. این یک وظیفه متخصص امنیت است که از جدیدترین روند در این زمینه آگاهی داشته باشد. اگر روش جدیدی از حمله کشف شود، متخصصان امنیت در اسرع وقت باید اقدامات لازم را در ارتباط با کاربران در مورد حمله جدید انجام دهند. علاوه بر این، متخصصان امنیت باید تضمین کنند که آموزش و آگاهی امنیتی به روز بوده که هر روش جدید حمله را شامل می شود. آموزش کاربر End-user یکی از بهترین راه های کاهش این حملات می باشد.

سیستم های حقوقی عمده Major Legal Systems

متخصصان امنیت باید سیستم های مختلف حقوقی که در سراسر جهان استفاده می شود و از اجزای تشکیل دهنده سیستم ها استفاده می کنند، را به طور کامل درک کنند. این سیستم ها عبارتند از:

- قانون مدنی Civil code law
- قانون عمومی Common law
- قانون کیفری Criminal law
- قانون مدنی / جریمه Civil/Tort law

- قانون اداری / تنظیمی Administrative/regulatory law
- قانون عرفی Customary law
- قانون مذهبی Religious law
- قانون مختلط Mixed law

قانون مدنی Civil code law

قانون مدنی که در اروپا توسعه یافته است، بر اساس قوانینی نوشته شده که یک قانون مبتنی بر قاعده است و به هیچ وجه به مقوله اولویت تکیه نمی‌کند. شایعترین نظام حقوقی در جهان، قانون مدنی در دادگاه‌های سطح پایین نیازی به پیروی از تصمیمات دادگاه‌های عالی ندارد.

قانون عمومی Common law

قانون عمومی، توسعه یافته در انگلستان، براساس آداب و رسوم و سابقه است زیرا هیچ قوانینی کتبی موجود نیست. قانون عمومی بر اصول اخلاقی مردم تأثیر می‌گذارد و به شدت به اولویت بستگی دارد. در این سیستم، دادگاه پایین تر باید از هر سابقه‌ای که به علت تصمیمات دادگاه‌های عالی می‌باشد، پیروی کند.

این نوع قانون در حال حاضر در انگلستان، ایالات متحده، استرالیا و کانادا استفاده می‌شود. امروزه، قانون عمومی از یک سیستم مبتنی بر هیئت منصفه استفاده می‌کند که می‌تواند از بین برود، بنابراین یک قاضی تصمیم می‌گیرد اما دادستان باید فراتر از شک و تردید معقول باشد. قانون مشترک به سه سیستم تقسیم بندی می‌شود: حقوق جزا، قانون مدنی / جرمه و قانون اداری / تنظیمی.

قانون کیفری Criminal law

قانون کیفری هر گونه اقداماتی را که به دیگران آسیب می‌رساند را پوشش می‌دهد. این موضوع به رفتارهایی اطلاق می‌شود که قوانین حفاظت از مردم را نقض می‌کند. در قانون کیفری، احزاب متخلف ممکن است زندانی و یا جرمه شوند. قانون کیفری بر اساس قانون عمومی Common law و قانون موضوعی statutory law می‌باشد. قانون موضوعی توسط نهادهای قانونی فدرال، ایالتی یا محلی وضع می‌شود.

قانون مدنی / جرمه Civil/tort law

در قانون مدنی، طرف متعهد وظیفه قانونی قربانی را به عهده دارد. اشتباهاتی که علیه یک فرد یا سازمان متعهد است، بررسی می‌کند. طبق قانون مدنی قربانی مجاز به جبران خسارت، تنبیه و جبران خسارت قانونی است. جبران کننده خسارات Compensatory Damages آنهایی هستند که زیان قربانی را باید جبران کنند. خسارت‌های تنبیهی Punitive Damages آنهایی هستند که توسط هیئت منصفه مجرم شناخته می‌شوند تا مجازات شوند. خسارات موضوعی Statutory Damage آنهایی هستند که براساس تخلفات قانونی تعیین شده اند. در قانون مدنی، طرف مسئول باعث آسیب رساندن به قربانی می‌شود. قوانین مدنی شامل خسارات اقتصادی، مسئولیت، سهل انگاری، آسیب عمدی، صدمه به اموال، خسارت شخصی، مزاحمت و مجازات‌های انفرادی می‌باشد.

در ایالات متحده، قانون مدنی اجازه می‌دهد تا مقامات ارشدیک سازمان در قبال هر گونه اقدامات غیرنظامی توسط سازمان، مسئولیت پذیر باشند. بنابراین اگر یک سازمان غفلت کند، توسط مقامات ارشد می‌توان هر طرفی را که مرتکب اشتباه شده است تحت پیگرد قانونی قرار دهد.

قانون اداری / قانون تنظیمی Administrative/regulatory law

در قانون اداری، استانداردهای عملکرد یا رفتار توسط سازمان‌های دولتی برای سازمان‌ها و صنایع تعیین می‌شود. مناطقی که تحت پوشش قانون اداری قرار می‌گیرند شامل خدمات عمومی، ارتباطات، بانکداری، حفاظت از محیط زیست و مراقبت‌های پزشکی می‌باشد.

قانون عرفی Customary law

قانون عرفی بر اساس آداب و رسوم یک کشور یا منطقه است. قانون عرفی در اکثر سیستم‌ها به صورت جداگانه استفاده نمی‌شود، بلکه در بسیاری موارد در قوانین مختلط به کار برده شده است، به عنوان مثال از این قوانین در کشورهای آفریقایی، چین و ژاپن استفاده شده است. جرمه نقدی یا خدمات دولتی شایعترین نوع بازپرداخت در این نظام حقوقی است.

قانون مذهبی Religious law

قانون مذهبی مبتنی بر باورهای مذهبی است. اگر چه بیشتر قوانین مذهبی بر اساس یک مذهب خاص و قوانین در آن نوشته می‌شود، تفاوت‌های فرهنگی می‌توانند از کشور به کشور متفاوت باشند و بر قوانینی که اعمال می‌شوند، تاثیر بگذارد.

قانون مختلط Mixed Law

قانون مختلط ترکیبی از دو یا چند نوع قانون دیگر است. این قانون اغلب ترکیبی از قانون مدنی و قانون عمومی می‌باشد که استفاده می‌شود.

مجوز لیسانس و مالکیت معنوی Licensing and Intellectual Property

قانون مالکیت معنوی یک گروه از قوانین است که حقوق انحصاری را برای خلق ذهن به رسمیت می‌شناسد. مالکیت معنوی یک دارایی ملموس یا غیرملموس می‌باشد که صاحب آن حق انحصاری دارد.

مالکیت معنوی تحت پوشش این نوع قانون شامل موارد زیر است:

- ثبت اختراع Patent
 - راز تجارت Trade secret
 - علائم تجاری Trademark
 - کپی رایت Copyright
 - دزدی نرم افزار و مسائل مربوط به صدور مجوز (لیسانس) Software piracy and licensing issues
 - مدیریت حقوق دیجیتال (DRM) Digital rights management
- در این قسمت انواع مالکیت معنوی و ویژگی‌های حفاظت داخلی آن را توضیح می‌دهیم.

ثبت اختراع Patent

یک ثبت اختراع به یک فرد یا شرکت برای پوشش یک اختراع داده می‌شود. هنگامی که حق ثبت اختراع اعطا می‌شود، تنها صاحب حق ثبت اختراع می‌تواند برای مدت زمان، معمولاً ۲۰ سال از اختراع، استفاده یا به فروش برساند. اگر چه این یکی از قویترین حفاظت‌های مالکیت

معنوی در دسترس می باشد، اختراع پس از انقضای ثبت اختراع به مالکیت عمومی تبدیل می شود و به این ترتیب هر سازمانی اجازه تولید و فروش محصول را دارد.

قوانین ثبت اختراع در جهان امروز رایج است. معمولاً شرکت های فن آوری را مشاهده می کنید، مانند اپل، مایکروسافت، هیولت پاکارد و گوگل که فایل های مربوط به نقض حق ثبت اختراعات را ارائه می دهند (اغلب علیه یکدیگر). به همین دلیل، بسیاری از شرکت ها قبل از توسعه تکنولوژی های جدید، یک تیم حقوقی را برای تحقیقات حقوقی تشکیل می دهند. امروزه اولین ثبت اختراع صادر شده در بازار یک مزیت رقابتی قاطع می باشد.

در حال حاضر هر محصول تولید شده که تحت فرآیند ثبت اختراع قرار می گیرد، معمولاً با مهر و موم ثبت اختراع مشخص می شود که در شکل ۱-۷ نشان داده شده است.



شکل ۱-۷: مهر تایید ثبت اختراع

راز تجارت Trade secret

یک راز تجارت تضمین می دهد که اطلاعات فنی یا کسب و کار اختصاصی، محرمانه باقی خواهد ماند. یک راز تجاری باعث یک مزیت رقابتی در سازمان می شود. اسرار تجاری شامل دستور العمل ها، فرمول ها، لیست های عناصر و غیره می باشد که باید از افشای آنها جلوگیری شود. پس از اینکه راز تجاری توسط یک رقیب یا توسط عموم به دست می آید، دیگر راز تجاری محسوب نمی شود.

اکثر سازمان هایی که اسرار تجاری دارند، با استفاده از موافقت نامه های غیر افشا-Non Disclosure Agreements (NDA)، از این اسرار محافظت می کنند. این NDA ها باید توسط هر سازمانی که دسترسی به اطلاعات که بخشی از راز تجاری می باشد، امضا شود. اگر سازمان بتواند

اثبات کند که امضا کننده آن را نقض کرده است، هر فردی که NDA را امضا می کند عواقب قانونی ناشی از آن را باید بپذیرد.

علائم تجاری Trademark

یک علامت تجاری تضمین می کند که یک نماد، صدا یا عبارت استفاده می شود تا یک محصول یا یک سازمان را از سازمان دیگر متفاوت کند. این علامت تجاری اجازه می دهد تا محصول یا سازمان توسط عموم به رسمیت شناخته شود. اکثر علامت های تجاری با یکی از علامت های نشان داده شده در شکل ۸-۱ مشخص شده اند.



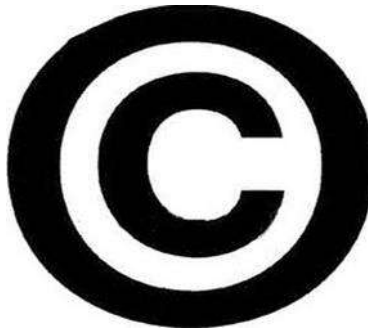
شکل ۸-۱: تخصیص علامت تجاری

اگر علامت تجاری ثبت نشده باشد، سازمان باید TM Capital را استفاده کند و اگر علامت تجاری ثبت شده باشد، سازمان باید از R احاطه شده استفاده کند.

حق چاپ (کپی رایت) Copyright

یک حق چاپ (کپی رایت) تضمین می کند که کارهایی که صورت گرفته، از نویسنده یا هنرمند که کار اصلی را ایجاد کرده اند در مقابل تولید مجدد یا حق نسخه برداری بدون رضایت مالک، محافظت می شود. کپی رایت طولانی تر از یک ثبت اختراع است. اگرچه دفتر کپی رایت ایالات متحده چندین دستورالعملی برای تعیین زمان کپی رایت دارد، قانون کلی زمان مولف برای آثار ایجاد شده پس از ۱ ژانویه ۱۹۷۸، بالای ۷۰ سال است.

در سال ۱۹۹۶، سازمان جهانی مالکیت معنوی (WIPO) World Intellectual Property Organization کپی رایت های دیجیتال را استاندارد کرد. مدیریت اطلاعات کپی رایت (CMI) Copyright Management Information مجوز و مالک اطلاعات است که به هر کار دیجیتالی اضافه می شود. در این استاندارد سازی، WIPO تصریح کرد که CMI موجود در کپی رایت را نمی توان تغییر داد. نماد نشان داده شده در شکل ۹-۱ نشان دهنده یک فعالیت می باشد که دارای حق کپی رایت است.



شکل ۹-۱: نماد کپی رایت

دزدی نرم افزار و مسائل صدور مجوز نرم افزار Software Piracy and Licensing Issues

برای درک مسائل مربوط به دزدی نرم افزار و مسائل صدور مجوز نرم افزار، متخصصان باید شرایط زیر را که برای تمایز میان انواع نرم افزار در دسترس استفاده می کنند را درک کنند:

- Freeware: نرم افزارهای موجود رایگان، شامل کلیه حقوق کپی، توزیع و تغییر نرم افزار.
- Shareware: نرم افزاری است که برای مدت زمان محدودی به اشتراک گذاشته می شود. بعد از یک مدت معینی (دوره آزمایشی)، کاربر نیاز به خرید نرم افزار برای دسترسی به تمام ویژگی های نرم افزار دارد. این نرم افزار نیز به عنوان Trialware نامیده می شود.
- Commercial software: نرم افزاری که توسط یک موسسه تجاری برای خرید در بازار عمده فروشی یا خرده فروشی مجاز می باشد.

دزدان نرم افزار تولید یا توزیع نرم افزار به صورت غیر مجاز دست به نسخه برداری می زنند. اگرچه دزدی نرم افزاری یک مسئله جهانی است، اما در آسیا، اروپا، آمریکای لاتین و آفریقا / خاورمیانه بسیار مرسوم است. بخشی از مشکل دزدی نرم افزاری ناشی از مسائل متقابل قانونی است که بوجود می آید. همکاری آژانس های اجرای قانون خارجی و دولتی اغلب مشکل یا غیرممکن است.

این ترکیب را با در اختیار داشتن سخت افزار مورد نیاز برای ایجاد نرم افزارهای سرقتی Pirated Software می‌توانید با سرعت انجام دهید، و مشکلاتی وجود دارد که در طول سال‌های آینده افزایش خواهد یافت.

متخصصان امنیت و سازمانهایی که با آنها کار می‌کنند باید تضمین کنند که سازمان اقدامات لازم را برای اطمینان جهت درک کارمندان از تأثیر نصب نرم افزارهای سرقتی انجام می‌دهند. علاوه بر این، سازمان‌های بزرگ ممکن است نیاز به استفاده از اپلیکیشن لیست موجودی در ساختار نرم افزار داشته باشد که به ادمین‌ها یک گزارش در مورد نرم افزار نصب شده ارائه دهد.

حفاظت داخلی Internal Protection

همانطور که قبلاً در این فصل ذکر شد، کارکنان بزرگترین تهدید برای هر سازمان می‌باشند. به همین دلیل، سازمان‌ها باید اقدامات لازم را برای محافظت از منابع محرمانه و دسترسی غیر مجاز داخلی انجام دهند. هر گونه اطلاعاتی که بخشی از یک ثبت اختراع، راز تجاری، علامت تجاری یا حق چاپ است، باید مشخص شود و طبقه بندی مناسب صورت گیرد. کنترل دسترسی باید برای این اطلاعات سفارشی شود و کنترل‌های ممیزی باید اجرا شود و هشدار پرسنل باید برای هر دسترسی رخ دهد. روشهای مراقبت مناسب و سیاست‌ها باید در نظر گرفته شود تا تضمین شود که هر گونه قوانینی که از این دارایی‌ها محافظت می‌کند می‌تواند مورد استفاده مجرم قرار گیرد.

مدیریت حقوق دیجیتال (DRM) Digital Rights Management

سازندگان سخت افزار، ناشران، صاحبان حق نسخه برداری و افراد از DRM برای کنترل از محتوای دیجیتالی استفاده می‌کنند. DRM اغلب شامل کنترل‌های دستگاه می‌باشد. نسل اول نرم افزار DRM کنترل کپی را دارد. نسل دوم DRM اجرا، مشاهده، کپی کردن، چاپ و تغییر آثار یا دستگاه‌ها را کنترل می‌کند.

قانون هزاره کپی رایت دیجیتال آمریکا (DMCA) 1998 Digital Millennium Copyright Act مجازات‌های کیفری برای کسانی که فن آوری‌های موجود را افشا می‌کنند، قرار داده است، هدف اصلی آنها حول فن آوری‌های حفاظت از محتوا می‌باشد. DRM شامل توافق نامه مجوز (لیسانس) محدود و رمزگذاری شده است. DRM از بازی‌های کامپیوتری و سایر نرم افزارها، اسناد، کتاب‌های الکترونیکی، فیلم‌ها، موسیقی و تلویزیون محافظت می‌کند. در بسیاری از پیاده سازی‌های

سازمانی، دغدغه اصلی شامل کنترل DRM برای اسناد با استفاده از محدودیت های دسترسی باز، ویرایش، چاپ و یا کپی که به صورت دائمی یا موقتی اعطا می شوند. راه حل ها می توانند مستقر شوند که داده های محافظت شده را در یک مدل متمرکز یا غیرمتمرکز ذخیره کنند. رمزگذاری در اجرای DRM برای محافظت از داده ها در هر دو حالت استراحت و انتقال استفاده می شود.

کنترل های واردات / صادرات Import/Export Controls

امروزه بسیاری از سازمان ها روابط تجاری با سازمان هایی که در کشورهای دیگر قرار دارند، ایجاد می کنند. سازمان ها باید از قوانین صادرات و واردات کشورهای مبدا و مقصد مطلع باشند. فن آوری های رمزگذاری برخی از محدود ترین فن آوری های مربوط به قوانین واردات و صادرات هستند. اگرچه ایالات متحده محدودیت صادرات فن آوری های رمزگذاری را به دلایل امنیت ملی محدود کرده است، کشورهای دیگر نیز مانند چین و روسیه واردات این فن آوری ها را محدود می کنند، زیرا کشور نمی خواهد شهروندان خود به آنها دسترسی داشته باشند. فن آوری و نرم افزار در دسترس عموم به جز فن آوری های رمزگذاری از اکثر قوانین صادرات معاف هستند. هر سازمانی که در فعالیتهای صادرات و واردات با اشخاص مستقر در کشورهای دیگر فعالیت می کند، باید اطمینان حاصل کند که مشاور حقوقی در این فرآیند دخالت دارد و تمام قوانین و مقررات پیگیری می شود. علاوه بر این، سازمان باید کنترل های لازم را انجام دهد تا تضمین شود که کارکنان به طور غریزی قوانین، مقررات و یا سیاست های شرکت های داخلی واردات و صادرات را نقض نمی کنند.

جریان اطلاعات بین مرزی Trans-Border Data Flow

در دنیای امروز، داده ها در سراسر مرزهای ملی حرکت می کنند. انتقال داده های بین المللی به سازمان ها و صنایع اجازه می دهد تا به صورت دیجیتالی اطلاعات را با شیوه ای بسیار سریعتر از گذشته به اشتراک بگذارند. همانطور که داده ها از سرور به سرور و در سراسر شبکه ها منتقل می شود، محل داده ها و محل میزبان داده باید در نظر گرفته شود. داده ها مشمول قوانین و نظام حقوقی هر حوزه قضایی در طول مسیر می باشند. این جریان حتی پیچیده تر می شود زیرا صلاحیت می تواند تحت تاثیر قرار گیرد زمانی که سازمان هایی در یک کشور که داده ها را دارند

در حالی که داده‌ها در مرکزی در کشور دیگر ذخیره می‌شود. متخصصان امنیت باید بر قوانین مربوط به حفظ حریم خصوصی و اطلاعات همه حوزه‌های قضایی که ممکن است بر سازمان تأثیر بگذارند، نظارت کنند. به همین علت، متخصصان امنیت بایستی یک نقشه جریان اطلاعات دقیق را برای تمام فرایندهای سازمانی ایجاد کنند.

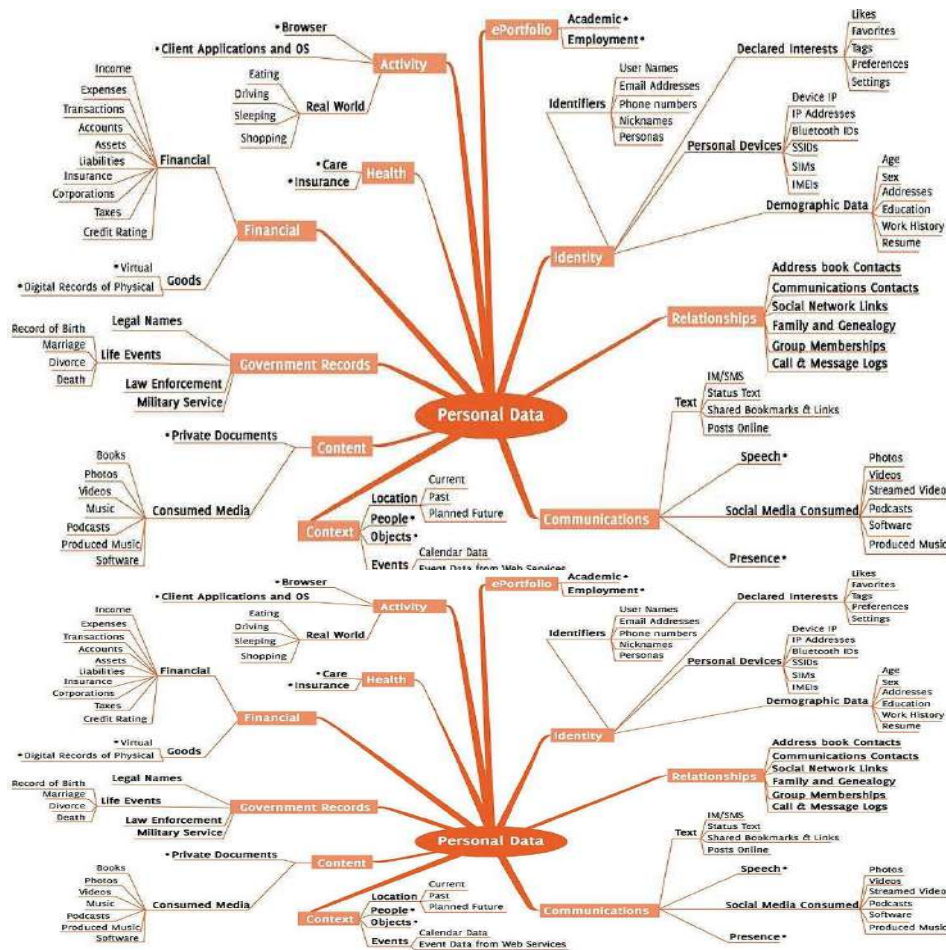
حریم خصوصی Privacy

امروزه با توجه به تکنولوژی و استفاده از آن، حریم خصوصی یک دغدغه عمده کاربران است. این دغدغه حریم خصوصی معمولاً سه حوزه را پوشش می‌دهد: کدام اطلاعات شخصی را می‌توان به اشتراک گذاشت، آیا پیام‌ها می‌توانند محرمانه محفوظ بمانند یا اینکه چگونه و چطور می‌توانند پیام‌ها را به صورت ناشناس ارسال کنند. حریم خصوصی بخشی تفکیک ناپذیر از هر اقدام امنیتی است، که یک سازمان را در بر می‌گیرد. به عنوان بخشی از اقدامات امنیتی که سازمانها باید برای حفاظت از حریم خصوصی انجام دهند، اطلاعات شناسایی شخصی PII باید درک، شناسایی و محافظت شوند. سازمان‌ها همچنین باید قوانین حفظ حریم خصوصی را که دولت‌ها تصویب کرده اند درک کنند. در نهایت، سازمان‌ها باید تضمین کنند که تمام قوانین و مقررات مربوط به حریم خصوصی تطابق دارند.

اطلاعات شناسایی شخصی (PII) Personally Identifiable Information

PII هر قطعه‌ای از اطلاعات است که می‌تواند به تنهایی یا با اطلاعات دیگر برای شناسایی یک فرد استفاده شود. هر PII که یک سازمان جمع‌آوری می‌کند باید از طریق قوی‌ترین تجهیزات محافظت شود. PII شامل نام کامل، شماره شناسایی (شامل شماره مجوز رانندگی و شماره امنیت اجتماعی)، تاریخ تولد، محل تولد، اطلاعات بیومتریک، شماره حساب‌های مالی (هر دو حساب بانکی و شماره کارت اعتباری) و هویت‌های دیجیتال (از جمله نام‌های رسانه‌های اجتماعی و برچسب‌ها)

به خاطر داشته باشید که کشورهای مختلف و سطوح مختلف دولت می‌توانند برای شناسایی PII دارای ویژگی‌های متفاوت باشند. متخصصان امنیت باید تضمین کنند که قوانین بین المللی، ملی، ایالتی و محلی و قوانین مربوط به PII را درک کرده اند. همانطور که سرقت این اطلاعات بسیار رایج شده است، می‌توانید انتظار داشته باشید که قوانین بیشتری بر کارمان تأثیر می‌گذارد. مجموعه لیستی از PII در شکل ۱-۱۰ نشان داده شده است.



شکل ۱-۱: فهرست PII

قوانین و مقررات Laws and Regulations

متخصصان امنیت معمولاً وکیل نیستند. به این ترتیب، انتظار نمی‌رود همه جزئیات قوانینی که بر سازمان آنها تاثیر می‌گذارد، درک کنند. با این حال، متخصصان امنیت باید از قوانین آگاه باشند و حداقل باید بدانند که این قوانین بر عملکرد سازمان تاثیر می‌گذارد. برای مثال، یک متخصص امنیت در یک مرکز مراقبت‌های پزشکی نیاز به درک همه دستورالعمل‌های امنیتی در حمل بیمه بهداشت و درمان و پاسخگویی به قانون HIPAA و همچنین محافظت از بیماران و

مراقبت مقرون به صرفه PPACA و قانون تطبیق بهداشت و درمان و آموزش و پرورش ۲۰۱۰ را دارد، که به عنوان Obamacare شناخته شده است. این قسمت بسیاری از قوانین را که بر روی یک متخصص امنیتی تأثیر می‌گذارد، بحث می‌کند. برای اهداف تست، نباید نگران تمام جزئیات قانون باشید. به سادگی باید نام (ها) قانون، هدف، و صنعت را که تحت تأثیر قرار می‌دهد را درک کنید. (در صورت لزوم).

قانون Sarbanes-Oxley (SOX)

قانون عمومی اصلاحات حسابداری و قانون حمایت از سرمایه گذاران در سال ۲۰۰۲، بیشتر به عنوان قانون Sarbanes-Oxley یا SOX شناخته شده است، هر سازمانی که در ایالات متحده آمریکا به طور عمومی معامله می‌کند را تحت تأثیر قرار می‌دهد. این روش حسابداری و گزارشگری مالی سازمان‌ها را کنترل می‌کند و مجازات و حتی زمان زندان برای کاربران اجرایی را تعیین می‌کند.

قانون مسئولیت پذیری بیمه درمانی قابل حمل

Health Insurance Portability and Accountability Act (HIPAA)

HIPAA، همچنین به عنوان قانون Kennedy-Kassebaum شناخته می‌شود، بر روی تمام مراکز درمانی، شرکت‌های بیمه درمانی و مکان‌های مراقبت پزشکی تأثیر می‌گذارد. این اداره توسط حقوق مدنی وزارت بهداشت و خدمات انسانی تأمین می‌شود. استانداردها و رویه‌هایی برای ذخیره سازی، استفاده و انتقال اطلاعات پزشکی و مراقبت‌های بهداشتی و درمانی فراهم می‌کند. HIPAA قوانین ایالتی را نادیده می‌گیرد مگر اینکه قوانین ایالتی سختگیرانه نباشد.

قانون Gramm-Leach-Bliley (GLBA) 1999

قانون Gramm-Leach-Bliley (GLBA) از سال ۱۹۹۹ بر تمام موسسات مالی از جمله بانک‌ها، شرکت‌های وام، شرکت‌های بیمه، شرکت‌های سرمایه گذاری و ارائه دهندگان کارت اعتباری تأثیر می‌گذارد. این قانون دستورالعملی برای اطمینان از تمام اطلاعات مالی و ممنوعیت به اشتراک گذاری اطلاعات مالی با اشخاص ثالث فراهم می‌کند. این عمل به طور مستقیم بر امنیت PII تأثیر می‌گذارد.

قانون کلاهبرداری و سوء استفاده رایانه‌ای (Computer Fraud and Abuse Act (CFAA)

CFAA قانون (1986) Craud and Fraud هر گونه نهادی که ممکن است هک کردن "رایانه‌های محافظت شده Protected Computer" را در در مورد قانون تعریف کند، تحت تاثیر قرار می‌دهد که در سال ۱۹۸۹، ۱۹۹۴، ۱۹۹۶ اصلاح شد. در سال ۲۰۰۱ توسط آمریکا با فراهم آوردن ابزار مناسب برای تسخیر و تخریب تروریسم (US PATRIOT) Act، در سال ۲۰۰۲، و در سال ۲۰۰۸ توسط قانون سرقت هویت و جبران مجازات، متحد و تقویت شد.

یک "رایانه محافظت شده Protected Computer" رایانه‌ای است که به طور انحصاری توسط یک موسسه مالی در تجارت یا ارتباطات داخلی و خارجی دولت ایالات متحده مورد استفاده قرار می‌گیرد، و همینطور رایانه‌ای را که در خارج از ایالات متحده قرار دارد و به نحوی بر تجارت بین ایالتی یا خارجی یا ارتباطات ایالات متحده تاثیر می‌گذارد، شامل می‌شود.

با توجه به ماهیت بین المللی بسیاری از ارتباطات اینترنتی و هر رایانه عادی تحت مجوز قانونی قرار گرفته است، مثل تلفن‌های همراه. این قانون شامل چندین تعریف هک شدن می‌باشد، از جمله دسترسی به رایانه بدون مجوز، دسترسی به رایانه برای بدست آوردن سوابق مالی به صورت عمد، اطلاعات دولت ایالات متحده، یا اطلاعات رایانه محافظت شده و انتقال ارتباطات تجاری کلاهبرداری با هدف قاچاق.

قانون حفظ حریم خصوصی فدرال Federal Privacy Act of 1974

قانون حفظ حریم خصوصی فدرال ۱۹۷۴ هر رایانه‌ای که حاوی پرونده هایی است که توسط سازمان فدرال استفاده می‌شود، تحت تاثیر قرار می‌دهد. این قانون، دستورالعمل هایی را برای جمع آوری، نگهداری، استفاده و انتشار PII در مورد افرادی که پرونده هایی در سیستم‌های سازمان‌های فدرال در زمینه جمع آوری، نگهداری، استفاده و توزیع PII نگهداری می‌شوند، فراهم می‌کند.

قانون نظارت بر اطلاعات فدرال Federal Intelligence Surveillance Act of 1978(FISA)

این قانون بر سازمان‌های اجرای قانون و اطلاعاتی تاثیر می‌گذارد. این اولین اقدام برای ارائه روش‌های نظارت فیزیکی و الکترونیکی و جمع آوری اطلاعات "اطلاعات خارجی" بین "قدرت‌های خارجی Foreign Powers" و "اطلاعات جاسوسی خارجی Foreign Intelligence"

Information" بود و فقط برای ترافیک در ایالات متحده استفاده می‌شد. این قانون توسط قانون PATRIOT ایالات متحده در سال ۲۰۰۱ و قانون اصلاحیه FISA سال ۲۰۰۸ اصلاح گردید.

قانون حفاظت از ارتباطات الکترونیکی Electronic Communications Privacy Act (ECPA) of 1986

سازمان‌های اطلاعاتی برای اجرای قانون و گسترش محدودیت‌های دولتی، استراق سمع مکالمات تلفنی که شامل دسترسی به ارتباطات الکترونیکی و انتقال داده‌های الکترونیکی که توسط رایانه ذخیره می‌شد، ممنوع کرد. این قانون توسط قانون ارتباطات 1994 (CALEA) و قانون PATRIOT ایالات متحده در سال ۲۰۰۱ و قانون اصلاحیه FISA 2008 اصلاح شد.

قانون امنیت رایانه Computer Security Act of 1987

توسط قانون مدیریت امنیت اطلاعات فدرال (FISMA) سال ۲۰۰۲ جایگزین شد. این قانون اولین قانونی بود که نیاز به یک طرح امنیتی رسمی رایانه‌ای داشت. برای محافظت و دفاع از هر یک از اطلاعات حساس در سیستم‌های دولت فدرال نوشته شد و امنیت آن اطلاعات را ارائه می‌داد و همچنین نیاز سازمان‌های دولتی برای آموزش کارمندان و شناسایی سیستم‌های حساس را در بر گرفت.

دستورالعمل صدور احکام فدرال ایالات متحده سال ۱۹۹۱ United States Federal Sentencing Guidelines of

بر افراد و سازمان‌هایی که متهم به جرائم جنایی و تخطی جدی کلاس A شده‌اند، طبق این دستورالعمل با آنها برخورد می‌شود. این دستورالعمل‌ها برای جلوگیری از اختلافات قضایی که در سراسر ایالات متحده وجود دارد ارائه شد.

قانون کمک‌های ارتباطی برای اجرای قانون 1994 (CALEA)

Communications Assistance for Law Enforcement Act

این قانون بر روی سازمان‌های اطلاعاتی و اجرای قانون تاثیر می‌گذارد. همچنین این قانون بر روی تغییر و طراحی تجهیزات، تاسیسات و خدمات وسایل مخابراتی و تولیدکنندگان تجهیزات مخابراتی جهت اطمینان از قابلیت‌ها، نظارت داخلی دارد و اجازه می‌دهد تا سازمان‌های فدرال بر

تمام تلفن، اینترنت، پهنای باند و ترافیک Voice over IP (VoIP) در زمان واقعی نظارت داشته باشند.

قانون حفاظت از اطلاعات شخصی و اسناد الکترونیکی

Personal Information Protection and Electronic Documents Act (PIPEDA)

بر نحوه فعالیت سازمان های بخش خصوصی برای جمع آوری، استفاده و افشای اطلاعات شخصی در حین تجارت کسب و کار در کانادا تاثیر می گذارد. این قانون برای رفع نگرانی اتحادیه اروپا درباره امنیت PII در کانادا نوشته شده است. این قانون سازمان ها را ملزم می کند که هنگام جمع آوری، استفاده یا افشای اطلاعات شخصی، رضایت خود را بدست آورند و از سیاست های اطلاعات شخصی شفاف، قابل فهم و در دسترس برخوردار باشند.

بازل دوم Basel II

بازل دوم بر موسسات مالی تاثیر می گذارد. الزامات حداقل سرمایه، بازرسی نظارتی و نظم بازار را مورد توجه قرار داده و هدف اصلی آن حفاظت از ریسک های بانک ها و سایر موسسات مالی است.

قانون مدیریت امنیت اطلاعات فدرال 2002 (FISMA)

Federal Information Security Management Act (FISMA) of 2002

بر هر سازمان فدرال تاثیر می گذارد و به سازمان های فدرال نیاز دارد تا یک برنامه امنیت اطلاعاتی را توسعه، مستند سازی و پیاده سازی کند.

قانون جاسوسی اقتصادی سال ۱۹۹۶ Economic Espionage Act of 1996

مسائل زیادی را با توجه به نحوه ساختن قانون بوجود آورد. اما با توجه به اهداف امتحان CISSP، این قانون بر شرکت هایی که اسرار تجاری دارند و هر کسی که قصد استفاده از تکنولوژی رمزگذاری برای فعالیت های بزهکارانه را دارد، شامل می شود. نیازی نیست راز تجاری به صورت ملموس توسط این قانون محافظت شود. با توجه به این قانون، سرقت از یک راز تجاری در حال حاضر جرم فدرال محسوب می شود، و کمیسیون محکومیت ایالات متحده باید در گزارش های

خود در خصوص اطلاعات مربوط به رمزنگاری یا تکنولوژی رمزگذاری و تقلب که به طور غیرقانونی مورد استفاده قرار می‌گیرد، اطلاعات خاصی را ارائه دهد.

قانون PATRIOT آمریکا

قانون PATRIOT ایالات متحده در سال ۲۰۰۱ بر سازمان‌های اطلاعات و اجرای قانون در ایالات متحده تاثیر گذاشت. هدف آن ارتقاء ابزارهای تحقیقاتی می‌باشد که می‌توان از اجرای قانون استفاده کند، از جمله ارتباطات ایمیل، پرونده‌های تلفن، ارتباطات اینترنتی، سوابق پزشکی و سوابق مالی. زمانی که این قانون تصویب شد، باعث اصلاح تعدادی از قوانین دیگر، از جمله FISA و ECPA 1986 شد.

اگرچه قانون PATRIOT ایالات متحده استفاده از ابزارهای تحقیقاتی را برای شهروندان خصوصی محدود نمی‌کند، اما شامل موارد استثنای بی‌نهایتی نیز می‌باشد: اگر شهروند خصوصی به عنوان یک کارمند دولتی عمل کند (حتی اگر به طور رسمی کار نکند)، اگر شهروند خصوصی جستجویی انجام دهد که برای ضمانت نیاز به اجرای قانون داشته باشد اگر دولت از جستجوی شهروندان خصوصی آگاهی داشته باشد یا اگر شهروند خصوصی به دنبال کمک به دولت باشد.

قانون تطبیق بهداشت و درمان و آموزش ۲۰۱۰

Health Care and Education Reconciliation Act of 2010

قانون تطبیق بهداشت و درمان و آموزش سال ۲۰۱۰ بر روی خدمات بهداشتی و آموزشی تأثیر گذاشت. این قانون برخی از اقدامات امنیتی را که باید برای حفاظت از اطلاعات مربوط به مراقبت‌های پزشکی افزایش داد، مورد استفاده قرار می‌دهد.

مسائل مربوط به حریم خصوصی کارکنان و انتظارات حریم خصوصی

Employee Privacy Issues and Expectation of Privacy

مسائل مربوط به حریم خصوصی کارکنان، باید توسط همه سازمان‌ها مورد توجه قرار گیرد تا اطمینان حاصل شود که سازمان امن است. با این حال، کارکنان سازمان باید از هر گونه نظارت اطلاع کافی داشته باشند. سازمانها همچنین باید تضمین کنند که نظارت بر کارکنان به طور صحیح اعمال شده است. بسیاری از سازمان‌ها یک سیاست بدون انتظار از حریم خصوصی را اجرا

می کنند که پس از دریافت آموزش مناسب، کارمند باید آن سیاستها را امضا کند. به خاطر داشته باشید که این سیاست باید به طور خاص رفتارهای غیر قابل قبول را توصیف کند. شرکتها نیز باید در نظر داشته باشند که برخی اقدامات توسط اصلاحیه چهارم، حفاظت می شوند. متخصصان امنیت و مدیریت ارشد باید با مشاوره حقوقی در هنگام طراحی و اجرای هر راه حل نظارت، مشورت کنند.

اتحادیه اروپا European Union

اتحادیه اروپا تعدادی قانون و مقرراتی را که بر امنیت و حریم خصوصی تأثیر می گذارد، پیاده سازی می کند. اصول اتحادیه اروپا در مورد حفظ حریم خصوصی، قوانین سختگیرانه برای محافظت از داده های خصوصی تنظیم شده است. دستورالعمل حفاظت از اطلاعات اتحادیه اروپا دستورالعملی را در مورد چگونگی پیروی از قوانین مندرج در اصول ارائه می دهد. سپس اتحادیه اروپا اصول خصوصی حراست امن Safe Harbor Privacy Principles را برای کمک به سازمانهای ایالات متحده مطابق با اصول حقوق خصوصی اتحادیه اروپا ایجاد کرد. برخی از دستورالعملها عبارتند از:

- داده ها باید طبق قانون جمع آوری شوند.
- اطلاعاتی که در مورد یک فرد جمع آوری شده را نمی توان با سازمان های دیگر به اشتراک گذاشت، مگر اینکه توسط فرد واجد شرایط به طور صریح اجازه داده شود.
- تنها در صورتی که سازمان به اشتراک گذاشته شده دارای امنیت مناسب باشد، می تواند اطلاعات را به سازمان های دیگر منتقل کند.
- داده ها باید تنها برای هدفی که جمع آوری شده مورد استفاده قرار گیرند.
- داده ها باید فقط برای مدت زمان معقولی استفاده شوند.

تذکر:

اصطلاح حراست امن (Safe Harbor) را با دسترسی به داده ها اشتباه نگیرید. با توجه به اتحادیه اروپا، یک حراست امن، یک نهاد است که مطابق با تمام الزامات اصول حقوق اتحادیه اروپا می باشد. جای امن یا پناهگاه داده ها (Data Haven) یک ناحیه ای است که نمی توان به طور قانونی از داده های شخصی با هدف اصلی جذب شرکت هایی که در جمع آوری داده ها مشغول فعالیت هستند محافظت کند.

دستورالعمل امنیت الکترونیکی اتحادیه اروپا اصول امضای الکترونیکی را تعریف می‌کند. در این دستورالعمل یک امضا باید به طور منحصر بفرد با امضا کننده و داده‌های مربوط به آن مرتبط باشد به طوری که هر گونه تغییر داده‌های بعدی قابل تشخیص باشد. امضا باید قادر به شناسایی امضا کننده باشد.

نقض داده‌ها Data Breaches

نقض داده‌ها هر حادثه‌ای است که در آن اطلاعاتی که خصوصی یا محرمانه تلقی می‌شوند برای احزاب غیرمجاز منتشر می‌شود. سازمان‌ها باید برنامه‌ای را در دست داشته باشند تا به طرز صحیح در مقابل این حوادث شناسایی و واکنش نشان دهند. صرفاً داشتن یک طرح واکنش به حادثه کافی نیست. همچنین یک سازمان باید پرسنلی آموزش دیده داشته باشد که با طرح واکنش به حوادث آشنا بوده و مهارت لازم برای پاسخگویی به هرگونه حادثه‌ای را که رخ داده داشته باشد.

اخلاق حرفه‌ای Professional Ethics

اخلاق برای هر حرفه، اعمال درست و غلط است که اصل اخلاقی آن شغل است. متخصصان امنیت، به ویژه کسانی که گواهینامه CISSP را دارند، بایستی اخلاقی را که توسط سیستم اطلاعاتی بین المللی منتشر شده مثل گواهینامه کنسرسیوم 2 (ISC)، موسسه اخلاق رایانه‌ای، هیئت معماری اینترنت (IAB) Internet Architecture Board و سازمانهایی که متخصصان آنجا فعالیت می‌کنند، را درک کنند.

اصول اخلاقی (ISC) 2 Code of Ethics

یک اصول اخلاقی برای صاحبان گواهینامه ارائه می‌شود. همه صاحبان گواهینامه باید کد اخلاقی را دنبال کرده و هر گونه نقض گزارش شده از کد، مورد بررسی قرار گرفته و دارنده گواهینامه مجرم شناخته شده و مجوز گواهینامه وی لغو خواهد شد. چهار قاعده اجباری برای اصول اخلاقی به شرح زیر می‌باشد:

- از جامعه، منافع عمومی، اعتماد و اطمینان عمومی لازم و زیرساخت‌ها محافظت کند.
- با احترام، صادقانه، صحیح، مسئولانه و قانونی عمل کند.
- ارائه خدمات مستمر و شایسته به مدیران.
- پیشرفت و حفاظت از حرفه.

صاحبان گواهینامه باید هر اقدامی را که توسط صاحبان گواهینامه دیگری انجام شده که احساس می کنند قوانین را نقض کرده گزارش دهند. در صورتی که یک دارنده گواهی گزارش دهد، یک کمیته بررسی اقدامات همکاران تشکیل و تصمیم می گیرند که شخصی که نقض کرده صاحب گواهینامه باشد یا خیر.

صدور گواهینامه یک امتیاز دست یافتنی است که باید حفظ شود. انتظار می رود که صاحبان گواهینامه برای تکمیل و اثبات شایستگی خود باید برخی از نیازهای آموزشی خود را در تمام جنبه های امنیتی تکمیل کنند و انتظار می رود که آنها برای فهم و پذیرش اقدامات امنیتی محتاطانه عمل کنند.

موسسه اخلاق رایانه Computer Ethics Institute

موسسه اخلاق رایانه ده فرمان اخلاقی رایانه را ایجاد کرد. در زیر فهرستی از این ده اخلاق را مطرح می کند:

- ۱- از رایانه برای آسیب رساندن استفاده نکنید.
- ۲- در کار رایانه دیگران دخالت نکنید.
- ۳- در فایل های رایانه های دیگران به جستجو نپردازید.
- ۴- از یک رایانه برای سرقت استفاده نکنید.
- ۵- از یک رایانه به دروغ استفاده نکنید.
- ۶- نصب و استفاده از نرم افزار مجاز در صورتی که هزینه آن را پرداخت شده باشد.
- ۷- از رایانه شخص دیگری استفاده نکنید، مگر اینکه مجوز داشته باشید یا غرامت مناسب برای استفاده از آن را پرداخت کرده باشید.
- ۸- استفاده از خروجی فکری فرد دیگری مناسب نیست.
- ۹- عواقب برنامه های که در حال نوشتن یا سیستمی را که طراحی می کنید را در نظر بگیرید.
- ۱۰- همیشه از رایانه به روش هایی استفاده کنید که باعث اطمینان و احترام سایر افراد و اموال آنها شود.

انجمن معماری اینترنت Internet Architecture Board

IAB بر طراحی، مهندسی و مدیریت اینترنت نظارت دارد. این انجمن به طور منظم به بررسی توصیه های استاندارد اینترنت می پردازد. اخلاق اینترنتی فقط بخش کوچکی از منطقه ای است

که پوشش می‌دهد. اظهارات اخلاقی که از سوی IAB صادر شده است، معمولاً جزئیات عملکردهایی را که آنها غیرمسئولانه تلقی می‌کنند، ارائه می‌دهد. این اقدامات شامل هدر رفتن منابع، از بین بردن یکپارچگی داده‌ها، به خطر انداختن حریم خصوصی و دسترسی به منابع است که کاربران مجاز به دسترسی آنها نیستند. درخواست نظرات 1087 (RFC)، به نام اخلاق و اینترنت، سند خاص IAB است که رفتار غیر اخلاقی اینترنت را مشخص می‌کند. برای اطلاعات بیشتر می‌توانید به لینک <http://tools.ietf.org/html/rfc1087> مراجعه کنید.

اخلاق سازمانی Organizational Ethics

سازمانها باید بیانیه اخلاقی داخلی و برنامه اخلاقی را توسعه دهند. با اتخاذ یک بیانیه و برنامه رسمی، انتظار می‌رود سازمان بر کارکنان خود تأکید کند که در کلیه معاملات کسب و کار به صورت کاملاً اخلاقی عمل کنند.

تعدادی قانون در ایالات متحده می‌تواند بر توسعه و پذیرش یک برنامه اخلاق سازمانی تأثیر بگذارد. اگر سازمان یک برنامه اخلاقی را اتخاذ کند، اغلب مسئولیت سازمان محدود می‌شود، حتی زمانی که کارکنان مجرم شناخته می‌شوند سازمان تضمین کند که پرسنل در اخلاق سازمان تعلیم دیده باشند.

مستندات امنیتی Security Documentation

در یک سازمان، حاکمیت امنیت اطلاعات شامل تعدادی اسناد می‌باشد که برای مدیریت جامع امنیتی استفاده می‌شود. داده‌ها و سایر دارایی‌ها باید به طور عمده بر اساس ارزش و حساسیت آنها محافظت شود. طرح‌های استراتژیک فعالیت‌های بلندمدت امنیتی (۳-۵ سال یا بیشتر) را هدایت می‌کنند. طرح‌های تاکتیکی به اهداف طرح استراتژیک دست می‌یابند و کوتاه‌ترند (۶-۱۸ ماه).

از آنجا که مدیریت مهمترین لینک در زنجیره امنیتی رایانه است، تصویب مدیریت باید به عنوان بخشی از نخستین گام در شکل‌گیری و اتخاذ سیاست امنیت اطلاعات باشد. مدیریت ارشد باید قبل از توسعه هر گونه سیاست امنیتی سازمانی اقدامات زیر را انجام دهد:

- تعریف دامنه برنامه امنیتی.
- شناسایی تمام دارایی‌هایی که نیاز به حمایت دارند.
- تعیین سطح حفاظت که هر دارایی نیاز دارد.

- تعیین مسئولیت های پرسنلی.
 - ایجاد عواقب ناشی از عدم مطابقت با سیاست امنیتی.
- با تایید کامل یک سیاست امنیتی سازمانی، مدیریت ارشد مالکیت امنیت سازمان را می پذیرد. سیاست های سطح بالا عبارتند از اظهاراتی که نشان می دهد قصد مدیریت ارشد حمایت از امنیت است.
- پس از بدست آوردن تایید مدیریت ارشد، اولین گام در ایجاد برنامه امنیت اطلاعات، اتخاذ یک بیانیه امنیت اطلاعات سازمانی است. سیاست امنیتی سازمان از این بیانیه امنیت اطلاعات سازمانی ناشی می شود. فرآیند برنامه ریزی امنیتی باید تعریف شود که چگونه امنیت مدیریت خواهد شد، چه کسی مسئولیت ایجاد و نظارت بر انطباق و همچنین چگونگی اقدامات امنیتی برای اثربخشی مورد آزمایش قرار می گیرد، چه کسی در ایجاد سیاست امنیتی دخیل است و در کجا سیاست امنیتی تعریف شده است.
- متخصصان امنیت باید بدانند که چگونه اسناد امنیت اطلاعات با یکدیگر کار می کنند تا یک طرح جامع امنیتی ایجاد شود. اسناد حاکمیت امنیت اطلاعات شامل موارد زیر است:

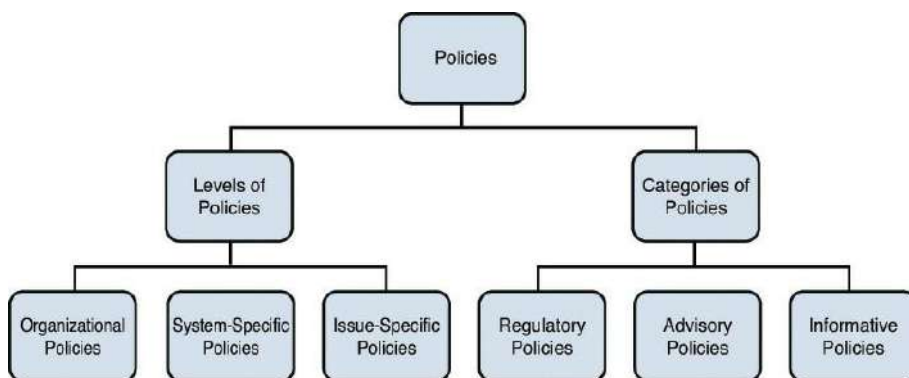
- سیاست ها Policies
- استانداردها Standards
- مبانی اولیه Baselines
- دستورالعمل Guidelines
- رویه ها Procedures

سیاست ها Policies

یک سیاست امنیتی، توسط مدیریت ارشد ارائه شده و نقش امنیت را به عهده دارد و به لحاظ استراتژیک، به معنی نتیجه امنیت است. سیاست ها به دو روش تعریف می شود: سطح در سازمان که در آن اجرا می شوند و مقوله ای که اعمال می شود. سیاست ها باید به طور کلی در طبیعت باشند، به این معنی که آنها مستقل از فناوری یا راه حل امنیتی خاص هستند. سیاست ها باید ماهیت کلی داشته باشند، به این معنی که آنها مستقل از یک فناوری خاص یا یک راه حل امنیتی هستند. سیاست ها اهداف را ترسیم می کنند، اما هیچ روش خاصی برای تحقق اهداف بیان شده ارائه نمی دهند. کلیه سیاست ها باید دارای یک منطقه استثناء باشند تا اطمینان حاصل شود که مدیریت قادر به مقابله با موقعیت هایی است که ممکن است مستثنا باشد.

سیاست‌ها گسترده هستند و پایه و اساس توسعه استانداردها، مبانی اساسی، دستورالعمل‌ها و رویه‌ها را فراهم می‌کنند، که همه اینها ساختار امنیتی را فراهم کرده و همچنین کنترل دسترسی مدیریتی، فنی و فیزیکی برنامه امنیتی را تکمیل می‌کنند.

سطوح سیاست که در امنیت اطلاعات به کار گرفته می‌شود، عبارتند از: سیاست‌های امنیتی سازمان، سیاست‌های امنیتی سیستم خاص، سیاست‌های امنیتی موضوع خاص. دسته بندی‌های سیاست‌های مورد استفاده در امنیت اطلاعات عبارتند از سیاست‌های امنیتی قانونی، سیاست‌های امنیتی مشاوره‌ای و سیاست‌های امنیتی اطلاعاتی. این سیاست‌ها در شکل ۱-۱۱ نشان داده شده است.



شکل ۱-۱۱: سطوح و دسته بندی‌های سیاست‌های امنیتی

سیاست امنیتی سازمان Organizational Security Policy

یک سیاست امنیتی سازمان، بالاترین سطح سیاست امنیتی است که توسط یک سازمان تصویب شده است. اهداف کسب و کار سیاست امنیتی سازمان را هدایت می‌کند. یک سیاست امنیتی سازمان حاوی دستورالعمل‌های عمومی است که باید اجزای زیر را داشته باشد:

- اهداف کلی سیاست امنیتی مشخص شود.
- مراحل کلی امنیت و اهمیت آن تعریف شود.
- چارچوب امنیتی برای رسیدن به اهداف کسب و کار تعیین شود.
- تایید سیاست دولت، از جمله حمایت از اهداف و اصول امنیتی.
- تعریف همه شرایط مربوطه.
- نقش و مسئولیت‌های امنیتی تعریف شود.

- تمام قوانین و مقررات مربوطه مطرح شود.
- مناطق مهم عملکردی شناسایی شود.
- الزامات انطباق و پیامدهای عدم انطباق تعریف شود.

یک سیاست امنیتی سازمان باید توسط همه سهامداران حمایت شود و باید برای همه پرسنل قابل مشاهده بوده و به طور منظم مورد بحث قرار گیرد. علاوه بر این، باید به طور منظم بررسی و بر اساس یافته‌های منظم تجدید نظر شود. هر نسخه از سیاست باید همراه با نسخه جدید ثبت و ضبط شود.

سیاست امنیتی سیستم خاص System-Specific Security Policy

یک سیاست امنیتی سیستم خاص، امنیت را برای یک رایانه، شبکه، تکنولوژی یا اپلیکیشن، مشخص می‌کند. این نوع سیاست، از یک سیاست امنیتی خاص متمرکز تر می‌باشد و چگونگی محافظت از سیستم یا تکنولوژی را مشخص می‌کند.

سیاست امنیتی با موضوع خاص Issue-Specific Security Policy

یک سیاست امنیتی با موضوع خاص در مورد مسائل مربوط به امنیت خاص می‌باشد. سیاست‌های مربوط به موضوع خاص شامل سیاست‌های حفظ حریم خصوصی ایمیل، سیاست‌های چک کردن ویروس، سیاست‌های خاتمه کارکنان، انتظارات از سیاست‌های حفظ حریم خصوصی و غیره می‌باشد. سیاست‌های مربوط به موضوع خاص از سیاست امنیتی سازمان پشتیبانی می‌کند.

دسته بندی‌های سیاست Policy Categories

سیاست‌های امنیتی نظارتی مقررات خاص صنعت، از جمله استانداردهای اجباری را مورد بررسی قرار می‌دهد. نمونه هایی از صناعی که باید سیاست‌های امنیتی نظارتی را در نظر بگیرند شامل امکانات درمانی، خدمات عمومی و مؤسسات مالی هستند.

سیاست‌های امنیتی مشاوره‌ای ارائه آموزش در مورد فعالیت‌های قابل قبول و غیر قابل قبول می‌باشد. در اکثر موارد، این سیاستها پیشنهاد می‌شود، البته نه به صورت اجباری. این نوع سیاست در صورت استفاده کاربران در فعالیت‌های غیر قابل قبول معمولاً نمونه هایی از عواقب احتمالی را نشان می‌دهد. سیاست‌های اطلاعاتی مناسب، اطلاعاتی را به عنوان ابزار آموزش در مورد موضوعات و قوانین معین ارائه می‌دهد.

استانداردها Standards

استانداردها نحوه اجرای سیاست‌ها در یک سازمان را توصیف می‌کنند. آنها اقدامات اجباری یا قوانینی هستند که ماهیت تاکتیکی دارند، به این معنی که مراحل لازم برای دستیابی به امنیت را ارائه می‌دهند. درست مانند سیاست‌ها، استانداردها باید مرتباً مورد بازبینی و تجدید نظر قرار گیرند.

خط مبنا Baselines

یک خط مبنا یک نقطه مرجع تعریف شده است تا به عنوان یک مرجع در آینده استفاده شود. گرچه گرفتن خط مبنا مهم است، استفاده از آن خط مبناها برای ارزیابی امنیت کشور نیز مهم می‌باشد. حتی جامع ترین خط مبناها اگر از آنها استفاده نشود بی فایده می‌باشد. دریافت یک خط مبنا در نقطه مناسب و زمان مناسب نیز مهم است. بازخورد باید زمانی باشد که یک سیستم به درستی پیکربندی و به طور کامل به روز شده است. هنگامی که بروز رسانی رخ می‌دهد، خط مبنا جدید باید دریافت شود و با خط مبناهای پیشین قبلی مقایسه شود. در آن زمان، انطباق خط مبناهای جدید بر اساس آخرین اطلاعات ممکن، ضروری می‌باشد.

دستورالعمل Guidelines

دستورالعمل‌ها اقدامات توصیه شده‌ای هستند که نسبت به استانداردها بسیار انعطاف پذیرتر بوده و در نتیجه برای شرایطی که ممکن است رخ دهد، کمک می‌کنند. دستورالعمل‌ها وقتی راهنمایی می‌کنند که استانداردها اعمال نشوند.

رویه‌ها Procedures

رویه‌ها شامل اقدامات دقیقی می‌باشد که پرسنل برای پیگیری نیاز به نزدیکترین رایانه‌ها و سایر دستگاه‌ها دارند. رویه‌ها اغلب شامل فهرست گام به گام در مورد چگونگی اجرای سیاست‌ها، استانداردها و دستورالعمل‌ها می‌باشند.

تداوم کسب و کار Business Continuity

تداوم کسب و کار یک قابلیت سازمان برای ادامه تحویل محصولات یا خدمات در سطوح از پیش تعیین شده قابل قبول پس از یک حادثه ناگوار است. به عنوان بخشی از مدیریت ریسک، متخصصان امنیت باید تضمین کنند که سازمان برنامه‌های مداوم کسب و کار مناسب را آماده کرده است. این بخش تداوم کسب و کار و بازیابی مفاهیم فاجعه، محدوده و طرح پروژه تداوم کسب و کار، و همینطور تاثیر تجزیه و تحلیل کسب و کار را پوشش می‌دهد.

تداوم کسب و کار و مفاهیم بهبود فاجعه Business Continuity and Disaster Recovery Concepts

متخصصان امنیت باید در توسعه هرگونه تداوم کسب و کار و بهبود فاجعه درگیر شوند. در نتیجه، متخصصان امنیت باید مفاهیم اساسی درگیر در تداوم کسب و کار و برنامه ریزی فاجعه را درک کنند، از جمله موارد زیر:

- اختلالات Disruptions
- فاجعه‌ها Disasters: تکنولوژیکی - عامل انسانی - طبیعی
- بهبود فاجعه و برنامه بهبود فاجعه Disaster Recovery and the Disaster Recovery Plan (DRP)
- برنامه ریزی مداوم و طرح تداوم کسب و کار Continuity Planning and the Business Continuity Plan (BCP)
- تجزیه و تحلیل اثر کسب و کار Business Impact Analysis (BIA)
- برنامه اضطراری Contingency Plan
- دسترسی Availability
- قابلیت اطمینان Reliability
- قابلیت بازیابی Recoverability
- تحمل خطا Fault Tolerance

اختلالات Disruptions

اختلال هر رخداد بدون برنامه ریزی که منجر به وقفه موقت هر دارایی سازمانی از جمله فرایندها، عملکردها و دستگاهها می شود، اختلالها به سه دسته اصلی تقسیم می شوند: غیر فاجعه، فاجعه، فاجعه ناگهانی Non-Disaster, Disaster and Catastrophe.

غیر فاجعه وقفه موقت است که به علت سوء عملکرد یا شکست رخ می دهد. غیر فاجعه ممکن است نیازی به اطلاع عمومی نداشته باشد و بسیار آسانتر از بهبود فاجعه یا فاجعه ناگهانی است. فاجعه یک رخداد ناگهانی است که تأثیر منفی در زندگی بلندمدت دارد. فاجعه ها نیازمند این است که این سازمان به طور علنی این رخداد را تایید کرده و اطلاعات عمومی را در مورد نحوه بهبودی و بازیابی سازمان ارائه دهد. فاجعه ها نیاز به تلاش بیشتر برای بازیابی از غیر فاجعه، اما تلاش کمتر از فاجعه ناگهانی است.

فاجعه ناگهانی Catastrophe یک فاجعه است که اثر بسیار گسترده تر و بسیار طولانی تری دارد. در اکثر موارد، در صورت از بین رفتن تاسیسات، یک فاجعه محسوب می شود و در نتیجه نیاز به بازسازی تاسیسات و استفاده از یک مرکز موقت خارج از سایت دارد.

فاجعه Disasters

یک فاجعه، یک وضعیت اضطراری است که فراتر از واکنش عادی منابع است. فاجعه معمولاً بر یک منطقه جغرافیایی گسترده تأثیر می گذارد و باعث خسارت شدید، آسیب دیدگی، از بین رفتن جان و مال می شود. هر گونه فاجعه تأثیر مالی منفی بر سازمان دارد. شدت خسارت مالی و اعتباری نیز تحت تأثیر میزان زمانی است که سازمان برای بهبود فاجعه لازم دارد. فاجعه ها به سه حوزه اصلی بر اساس مبدا تقسیم می شوند: بلایای تکنولوژیکی، بلایای ناشی از بشر و بلایای طبیعی. یک فاجعه زمانی اتفاق می افتد که تمام عناصر کسب و کار در مکان اصلی به عملکرد عادی برگردند. دغدغه اصلی در هر فاجعه ای، امنیت پرسنل است.

✓ بلایای تکنولوژیکی Technological Disasters

بلایای تکنولوژیکی زمانی رخ می دهد که یک دستگاه نتواند کار کند. این شکست می تواند منجر به نقص دستگاه، اجرای نادرست، نظارت نادرست یا خطای انسانی باشد. بلایای تکنولوژیکی

معمولا از روی عمد نیستند. اگر یک بلایای تکنولوژیکی به موقع از بین نرود، یک سازمان ممکن است دچار فروپاشی مالی شود.

اگر یک فاجعه به دلیل یک حمله عمدی به زیرساخت های سازمان رخ دهد، حتی اگر حمله علیه یک دستگاه یا تکنولوژی خاص باشد، این بلایا یک فاجعه ناشی از بشر محسوب می شود. در گذشته، تمام بلایای تکنولوژیکی به عنوان بلایای طبیعی به شمار می آمدند چرا که بلایای تکنولوژیکی معمولا به علت خطا یا غفلت انسانی بود. با این حال، در سال های اخیر، کارشناسان شروع به طبقه بندی بلایای تکنولوژیکی به طور جداگانه از بلایای طبیعی ناشی از بشریت کرده اند، هرچند که این دو به شدت بهم مرتبط هستند.

✓ بلایای ناشی از بشر Human-Caused Disasters

بلایای ناشی از بشر به صورت عمد یا خطا توسط انسان رخ می دهد. بلایای ناشی از بشر شامل حملات دشمن، بمب گذاری، خرابکاری، آتش سوزی، تروریسم، اعتصابات و یا سایر اقدامات شغلی، خرابی های زیربنایی، عدم دسترسی کارکنان به دلیل تخلیه اضطراری و توده های حمله عصبی است. در اغلب موارد، حوادث عمدی می باشد.

✓ بلایای طبیعی Natural Disasters

بلایای طبیعی به دلیل یک خطر طبیعی رخ می دهد. بلایای طبیعی شامل سیل، سونامی، زلزله، طوفان، گردباد و دیگر رخداد های طبیعی است. آتش سوزی که نتیجه انفجار نیست، همچنین یک بلایای طبیعی محسوب می شود.

بهبود فاجعه و برنامه رفع فاجعه Disaster Recovery and the Disaster Recovery Plan (DRP)

بهبود فاجعه تاثیرات یک فاجعه را به حداقل می رساند و شامل مراحل لازم برای بازگرداندن عملیات طبیعی می شود. بهبود فاجعه باید تمام منابع سازمانی، عملکرد و پرسنل را در نظر بگیرد. اثر بهبود فاجعه یک سازمان در طول و پس از اختلال در یک فاجعه ادامه خواهد یافت.

هر عملکرد سازمانی یا سیستم سازمانی، برنامه رفع فاجعه خود (DRP) را دارد. DRP برای هر عملکرد یا سیستم به عنوان نتیجه مستقیم آن و به عنوان بخشی از طرح مداوم کسب و کار BCP شناخته می شود. DRP زمانی پیاده سازی می شود که وضعیت اضطراری رخ داده که شامل

مراحل برای بازگرداندن عملکردها و سیستمها باشد. هدف DRP به حداقل رساندن یا جلوگیری از آسیب رساندن به اموال و جلوگیری از دست دادن زندگی است. جزئیات بیشتر در مورد بهبود فاجعه بعداً در این فصل ارائه می‌شود.

برنامه ریزی مداوم و طرح تداوم کسب و کار

Continuity Planning and the Business Continuity Plan (BCP)

برنامه ریزی مداوم با شناسایی تاثیر هر گونه فاجعه، و اطمینان از اینکه برنامه ریزی قابل اجرا برای هر عملکرد و سیستم اجرا می‌شود، مورد بررسی قرار می‌گیرد. تمرکز اصلی آن بر روی چگونگی انجام کارکرد سازمانی هنگام وقوع اختلال است. BCP تمام جنبه‌هایی را که تحت تأثیر یک فاجعه قرار دارند، شامل عملکردها، سیستم‌ها، پرسنل و تاسیسات در نظر می‌گیرد. و لیست خدمات و اولویت بندی‌های مورد نیاز، به ویژه ارتباطات و فناوری اطلاعات را فهرست می‌کند.

تجزیه و تحلیل تاثیر کسب و کار (Business Impact Analysis (BIA)

تجزیه و تحلیل تاثیر کسب و کار (BIA) یک تحلیل عملکردی است که به عنوان بخشی از تداوم کسب و کار و بهبود فاجعه رخ می‌دهد. انجام یک BIA کامل به واحدهای کسب و کار کمک خواهد کرد تا تاثیر یک فاجعه را درک کنند سند حاصل از یک BIA تولید شده، لیست کارهای مهم و ضروری کسب و کار، وابستگی به منابع و سطح بحرانی آنها را در کل سازمان نشان می‌دهد.

برنامه اضطراری Contingency Plan

برنامه اضطراری بخشی از BCP کلی سازمان است. اگرچه BCP جنبه‌های سازمانی را تحت تأثیر قرار می‌دهد و DRP نحوه بازیابی عملکردها و سیستمها را تعریف می‌کند، اما برنامه اضطراری دستورالعمل کارهایی را که باید انجام دهند تا کارکردها و سیستمها به عملکردهای کامل بازگردند، ارائه می‌دهد. به نظر می‌آید برنامه اضطراری به عنوان یک راهنما برای عملیات به حالت کاهشی است که معمولاً شامل اطلاعات تماس با کلید پرسنل، اطلاعات مربوط به قرارداد فروشنده و تجهیزات و نیازهای سیستم است.

شکست برنامه اضطراری معمولا یک شکست مدیریت است. یک برنامه اضطراری همراه با BCP و DRP حداقل باید یک بار در سال بررسی شود. همانطور که تمام چنین برنامه هایی، نسخه کنترل آن (version control) باید حفظ شود. برای اطمینان از دسترسی پرسنل در صورت تخریب تأسیسات اصلی سازمان، باید کپی هایی برای ذخیره سازی در داخل و خارج از محل تهیه شود.

دسترسی Availability

همانطور که از قبل می دانید، دسترسی یکی از اصول کل محرمانه بودن، یکپارچگی و دسترسی، مثلث CIA است که تقریبا در هر دامنه CISSP تعریف شده مورد بحث قرار می گیرد. در دسترس بودن جزء اصلی برنامه ریزی تداوم کسب و کار است. سازمان باید میزان قابل قبول بودن هر عملکرد یا سیستم را تعیین کند. اگر در دسترس بودن منابع زیر این سطح تعریف شده قرار بگیرد، باید تضمین شود که در دسترس بودن بازسازی شده، و باید اقدامات خاصی انجام شود. در رابطه با در دسترس بودن، بسیاری از خرابی های برنامه ریزی شده از عملکردها و سیستمها به دلیل خرابی سخت افزار است. در دسترس بودن تاکید بر تکنولوژی می باشد.

قابلیت اطمینان Reliability

قابلیت اطمینان توانایی یک عملکرد یا سیستم که به طور مداوم با توجه به مشخصات انجام می شود. این امر در تداوم کسب و کار حیاتی است تا تضمین شود که فرایندهای سازمان می توانند به فعالیت خود ادامه دهند. قابلیت اطمینان بر روی فرایندها تأکید می کند.

دامنه و طرح پروژه Project Scope and Plan

همانطور که از قبل می دانید، ایجاد BCP برای اطمینان از اینکه سازمان می تواند از یک فاجعه یا رخداد مخرب بهبود یابد بسیار حیاتی است. چندین گروه استانداردها و بهترین شیوه ها را برای تداوم کسب و کار ایجاد کرده اند. این استانداردها و بهترین روشها شامل بسیاری از مؤلفه ها و مراحل مشترک است. این بخش مؤلفه های پرسنلی، دامنه پروژه و مراحل تداوم کسب و کار را که باید تکمیل شود را پوشش می دهد.

مولفه‌های پرسنلی Personnel Components

مهمترین پرسنل در توسعه BCP مدیریت ارشد است. پشتیبانی ارشد مدیریتی از تداوم مشاغل و بهبود فاجعه، دیدگاه سازمانی کلی این فرآیند را هدایت می‌کند. بدون پشتیبانی مدیریت ارشد، این روند شکست خواهد خورد.

مدیریت ارشد اهداف کلی تداوم کسب و کار و بهبود فاجعه را تعیین می‌کند. یک مسئول هماهنگ کننده کسب و کار باید توسط مدیریت ارشد معرفی شود و کمیته BCP را رهبری کند. این کمیته BCP و DRP را توسعه، پیاده سازی و آزمایش می‌کند. کمیته BCP باید نماینده‌ای از هر واحد کسب و کار داشته باشد. حداقل یک عضو مدیریت ارشد باید بخشی از این کمیته باشد. بعلاوه، این سازمان باید به خاطر نقش حیاتی که این بخش‌ها در حین و بعد از فاجعه ایفا می‌کنند، نماینده بخش فناوری اطلاعات، بخش حقوقی، بخش امنیتی و بخش ارتباطات باشد. با راهنمایی مدیریت، کمیته BCP باید با واحدهای کسب و کار همکاری کند تا درنهایت پیوستگی کسب و کار و اولویت‌های بهبود فاجعه مشخص شود. مدیران ارشد واحد کسب و کار وظیفه شناسایی و اولویت بندی سیستم‌های زمان بحران را دارند. پس از مشخص شدن تمام جنبه‌های برنامه ها، کمیته BCP باید مأموریت داشته باشد که برنامه‌ها را بطور منظم بررسی کند تا از ماندگاری و عملکرد آنها مطمئن شود. مدیریت ارشد باید تمام تلاشهای تداوم کسب و کار را از نزدیک نظارت و کنترل کند و هرگونه موفقیت را علناً ستایش کند. پس از آنکه سازمان به برنامه ریزی بهبود فاجعه می‌رسد، تیم‌های دیگر نیز درگیر می‌شوند.

محدوده پروژه Project Scope

برای اطمینان از موفقیت آمیز بودن پیشرفتهای لازم، مدیریت ارشد باید محدوده BCP را تعریف کند. یک پروژه تداوم کسب و کار با دامنه نامحدود اغلب می‌تواند برای انجام صحیح کمیته BCP بسیار بزرگ شود. به همین دلیل، ممکن است مدیریت ارشد نیاز به تقسیم پروژه تداوم کسب و کار به بخش‌های کوچکتر و قابل کنترل تری داشته باشد.

با توجه به تقسیم BCP به بخش ها، یک سازمان ممکن است بخواهد بخش‌ها را براساس مکان یا مکان جغرافیایی تقسیم بندی کند. با این حال، یک BCP سازمانی باید توسعه یابد که سازگاری برنامه‌های فردی را تضمین کند.

مراحل پیوستگی کسب و کار Business Continuity Steps

بسیاری از سازمان ها استانداردها و دستورالعمل هایی را برای انجام تداوم کسب و کار و برنامه ریزی فاجعه ایجاد کرده اند. یکی از محبوب ترین استانداردها انتشار ویژه 800-34 (SP) نسخه R1 از موسسه ملی استاندارد و فناوری NIST است.

لیست زیر مراحل R1 SP 800-34 را بیان می کند:

۱. تدوین سیاست برنامه ریزی اضطراری. Develop contingency planning policy.

۲. انجام تحلیل تأثیر کسب و کار. Conduct business impact analysis (BIA).

۳. شناسایی کنترل های پیشگیرانه. Identify preventive controls.

۴. ایجاد استراتژی های بازیابی. Create recovery strategies.

۵. توسعه برنامه تداوم کسب و کار BCP. Develop business continuity plan (BCP).

۶. تست، آموزش و اجرا. Test, train, and exercise.

۷. حفظ طرح و برنامه. Maintain the plan.

شکل ۱-۱۲ یک فهرست دقیق تر از وظایف موجود در R1 SP 800-34 را نشان می دهد.

Develop contingency planning policy.	Conduct business impact analysis (BIA).	Identify preventive controls.	Create recovery strategies.	Develop business continuity plan (BCP).	Test, train, and exercise.	Maintain the plan.
Identify statutory or regulatory requirements. Develop IT contingency planning policy statement. Publish policy.	Identify critical processes and resources. Identify outage impacts, and estimate downtime. Identify resource requirements. Identify recovery priorities.	Identify controls. Implement controls. Maintain controls.	Develop backup and recovery strategies. Identify roles and responsibilities. Develop alternative site. Identify equipment and cost considerations. Integrate into architecture.	Document recovery strategy.	Test the plan. Train personnel. Plan exercises.	Review and update the plan. Coordinate updates with internal and external organizations. Control the distribution of the plan. Document the changes.

شکل ۱-۱۲: انتشار ویژه 800-34 NIST ویرایش ۱

توسعه تجزیه و تحلیل تاثیرات کسب و کار Business Impact Analysis Development

توسعه BCP بیشتر به توسعه BIA بستگی دارد. BIA به سازمان کمک می‌کند تا متوجه شود که یک رخداد مخرب بر سازمان تاثیر خواهد گذاشت. این یک تجزیه و تحلیل سطح مدیریتی است که تاثیر از دست دادن منابع سازمان را مشخص می‌کند.

چهار مرحله اصلی BIA عبارتند از:

۱ شناسایی فرآیندهای حیاتی و منابع.

۲ شناسایی اثرات تخریب، و تخمین خرابی.

۳ شناسایی نیازهای منابع.

۴ شناسایی اولویت‌های بازیابی.

BIA به شدت بر روی هر تجزیه و تحلیل آسیب پذیری و ارزیابی ریسک تکیه دارد. تجزیه و تحلیل آسیب پذیری و ارزیابی ریسک ممکن است توسط کمیته BCP یا به وسیله یک تیم ارزیابی ریسک جداگانه انجام شود. فرایند ارزیابی ریسک بعداً در این فصل مورد بحث قرار می‌گیرد.

شناسایی فرآیندها و منابع بحرانی Identify Critical Processes and Resources

هنگام شناسایی فرآیندها و منابع بحرانی یک سازمان، کمیته BCP باید ابتدا تمام واحدهای کسب و کار یا مناطق عملیاتی درون سازمان را شناسایی کند. پس از شناسایی همه واحدها، تیم BCP باید افرادی را انتخاب کند که مسئول جمع‌آوری داده‌های مورد نیاز باشند و نحوه دستیابی به داده‌ها را انتخاب کنند.

این افراد داده‌ها را با استفاده از تکنیک‌های مختلف، از جمله پرسشنامه‌ها، مصاحبه‌ها و نظرسنجی‌ها جمع‌آوری خواهند کرد. این افراد همچنین ممکن است تجزیه و تحلیل آسیب پذیری و ارزیابی ریسک را انجام دهند یا از نتایج این تست‌ها به عنوان ورودی برای BIA استفاده کنند.

در حین جمع‌آوری داده‌ها، فرایندها و کارکردهای کسب و کار سازمان و منابعی که این فرایندها و عملکردها به آنها بستگی دارند باید مستند شوند. این لیست باید شامل کلیه دارایی‌های کسب و کار، از جمله دارایی‌های فیزیکی و مالی متعلق به سازمان و هرگونه دارایی باشد که مزیت رقابتی یا اعتبار رقابتی را فراهم می‌کند.

شناسایی اثرات خرابی، و برآورد یا تخمین خرابی Identify Outage Impacts, and Estimate Downtime

پس از تعیین تمامی فرآیندهای کسب و کار، عملکردها و منابع، سازمان باید سطح بحرانی هر منبع را تعیین کند.

به عنوان بخشی از تعیین اینکه چگونه یک دارایی مهم است، شما باید شرایط زیر را درک کنید: حداکثر خرابی قابل تحمل (MTD) **Maximum tolerable downtime (MTD)**: حداکثر زمانی که یک سازمان می تواند تنها یک منبع یا عملکرد خرابی را تحمل کند. همچنین به عنوان حداکثر مدت زمان اختلال MPTD اشاره می شود.

زمان متوسط تعمیر (MTTR) Mean time to repair: میانگین زمان مورد نیاز برای تعمیر یک منبع یا عملکرد واحد در هنگام بروز یک فاجعه یا اختلال.

زمان متوسط بین شکست (MTBF) Mean time between failure: مقدار تخمین زمان کار دستگاه قبل از بروز خرابی. این تخمین توسط فروشنده دستگاه محاسبه می شود. قابلیت اطمینان سیستم با MTBF بالاتر و MTTR پایین تر افزایش می یابد.

هدف بازیابی (RTO) Recovery time objective: کوتاهترین مدت زمان پس از وقوع یک فاجعه یا یک رخداد مخرب که در آن باید یک منبع یا عملکرد برای بازیابی استفاده شود تا از عواقب غیرقابل قبول جلوگیری شود. RTO فرض می کند که یک دوره قابل قبول از خرابی وجود دارد. RTO باید از MTD کوچکتر باشد.

زمان بازیابی کار (WRT) Work recovery time: تفاوت بین RTO و MTD، که مدت زمان باقیمانده ای است که پس از RTO به مدت قبل از رسیدن به حداکثر تحمل خطا باقی مانده است.

هدف نقطه بازیابی (RPO) Recovery point objective: زمانی که منبع یا عملکرد خراب شده باید بازگردانده شود.

هر سازمان باید سطوح بحرانی مستند شده خود را توسعه دهد. یک مثال خوب از سطوح بحرانی منابع و عملکرد سازمان عبارتند از: بحرانی، فوری، مهم، عادی و غیر ضروری، Critical, Urgent, Important, Normal, Nonessential. منابع بحرانی منابعی است که برای عملیات سازمان حیاتی است و باید در دقیقه یا ساعت در حین وقوع حادثه یا حوادث ناگوار بازسازی شوند. منابع فوری باید در عرض ۲۴ ساعت بازسازی شوند اما مثل منابع بحرانی، اهمیت ندارند. منابع مهم باید در

۷۲ ساعت بازسازی شوند اما به اندازه منابع بحرانی و فوری، اهمیت ندارند. منابع عادی باید در ۷ روز بازسازی شوند، اما به اندازه منابع بحرانی، فوری و مهم، اهمیت ندارند. منابع غیر ضروری باید ظرف ۳۰ روز بازسازی شوند.

هر فرآیند، عملکرد، منبع Process, Function, Resource باید سطح بحرانی خود را تعریف کند تا به عنوان ورودی به DRP عمل کند. اگر سطوح اولویت بحرانی تعریف نشده باشد، DRP ممکن است در مدت زمانی که سازمان نیاز به بهبودی دارد، عملی نشود.

شناسایی منابع مورد نیاز Identify Resource Requirements

پس از تعیین سطح بحرانی بودن هر عملکرد و منبع، باید کلیه منابع مورد نیاز را برای هر عملکرد و منبع تعیین کنید. به عنوان مثال، سیستم حسابداری سازمان ممکن است به یک سرور که اپلیکیشن حسابداری را ذخیره می‌کند، و سرور دیگری که پایگاه داده را در اختیار دارد، متکی باشد و سیستم‌های مختلف مشتری که وظایف حسابداری را از طریق شبکه انجام می‌دهند، و دستگاه‌های شبکه و زیرساخت‌هایی که سیستم را پشتیبانی می‌کنند، متکی باشد. منابع مورد نیاز همچنین باید هرگونه الزامات منابع انسانی را در نظر بگیرند. هنگامی که منابع انسانی در دسترس نباشد، سازمان می‌تواند به همان اندازه تأثیر منفی داشته باشد که منابع فنی در دسترس نباشد.

به خاطر داشته باشید که اولویت برای هر CISSP باید امنیت زندگی انسان باشد. تمام منابع سازمانی دیگر را فقط بعد از امنیت پرسنل در نظر گرفته و از آن محافظت شود.

سازمان باید منابع مورد نیاز را برای هر منبع که نیاز به بازگرداندن آن در زمان وقوع رخداد دارد، مستند سازد. که شامل نام دستگاه، سیستم عامل یا نسخه پلتفرم، الزامات سخت افزار و دستگاه ارتباطات داخلی است.

شناسایی اولویت‌های بازیابی Identify Recovery Priorities

پس از شناسایی کلیه منابع مورد نیاز، سازمان باید اولویت‌های بازیابی را مشخص کند. اولویت‌های بازیابی را با در نظر گرفتن حساسیت فرآیند، اثرات قطع برق، تحمل خطا و منابع سیستم تعیین کند. پس از جمع‌آوری این اطلاعات، نتیجه سلسله مراتب اولویت بازیابی سیستم اطلاعات است. سه سطح اصلی اولویت‌های بازیابی که باید مورد استفاده قرار گیرد: بالا، متوسط و کم، High, Medium, Low.

BIA اولویت های بازیابی را تعیین می کند اما راه حل های بازیابی را ارائه نمی دهد. آنها موارد ذکر شده DRP را ارائه می دهند.

قابلیت بازیابی Recoverability

بازیابی توانایی یک سیستم یا عملکرد در صورت وقوع یک فاجعه یا رخداد مخرب است. به عنوان بخشی از قابلیت بازیابی، خرابی باید به حداقل برسد. قابلیت بازیابی تاکید بر پرسنل و منابع مورد استفاده برای بازیابی می باشد.

تحمل خطا Fault Tolerance

تحمل خطا زمانی فراهم می شود که یک مولفه پشتیبان شروع به کار کند، وقتی که مولفه اصلی نتواند کار کند. یکی از جنبه های مهم تحمل خطا، فقدان سرویس وقفه است. میزان تحمل خطا در بیشتر سطوح سازمانی براساس میزان سازماندهی که مایل به هزینه کردن است، می تواند حاصل شود. با این حال، مؤلفه تهیه نسخه پشتیبان اغلب همان سطح سرویس را به عنوان مؤلفه اصلی ارائه نمی دهد. به عنوان مثال، یک سازمان ممکن است اتصال T1 پر سرعت را بر روی اینترنت پیاده سازی کند. با این حال، اتصال پشتیبان به اینترنت که در صورت خرابی خط T1 استفاده می شود ممکن است بسیار کندتر اما با هزینه بسیار پایین تر از اتصال اولیه T1 باشد.

سیاست های امنیتی پرسنل Personnel Security Policies

پرسنل چه به طور عمدی یا ناخواسته مسئول عمده اکثریت مسائل امنیتی در یک سازمان هستند. به همین دلیل ضروری است که سازمان یک سیاست امنیتی مناسب برای پرسنل را اجرا کند. سازمانها باید سیاست های امنیتی خود را در نظر بگیرند که عبارتند از غربالگری، استخدام و سیاست های خاتمه دادن. متخصصان امنیت باید با پرسنل منابع انسانی همکاری کنند تا تضمین شود که سیاست های امنیتی مناسب برای پرسنل امنیتی وجود دارد.

غربالگری کاندید برای اشتغال Employment Candidate Screening

غربالگری کارکنان قبل از پیشنهاد اشتغال باید رخ دهد و ممکن است شامل سابقه کیفری، تاریخ کار، تحقیقات پیشین، تاریخ اعتبار، سوابق رانندگی، آزمایش سوء مصرف مواد، بررسی مرجع،

آموزش و تأیید مجوز، تأیید شماره تلفن‌های اجتماعی، و برای ورود به چک کردن یک لیست دیدبان برای مظنون به تروریست‌ها بررسی شود. هر سازمان باید نیازهای غربالگری را بر اساس نیازهای سازمان و چشم انداز اشتغال پرسنل تعیین کند. توصیف‌های شغلی باید نقش‌ها و مسئولیت‌های نقش شغلی و هر گونه تجربه یا آموزش مورد نیاز را داشته باشد. اگر مهارت‌ها باید حفظ یا ارتقا یابند، شرح شغل باید الزامات آموزش سالانه را ذکر کند، خصوصاً اگر به آموزش تخصصی امنیتی نیاز باشد. مشارکت سالانه در آموزش آگاهی امنیتی و سایر الزامات مربوط به انطباق باید به عنوان بخشی از توافق نامه اشتغال لحاظ شود.

چک کردن سابقه‌های جنایی تحت قانون گزارش اعتبار منصفانه (Fair Credit Reporting Act (FCRA مجاز است. کارفرمایان می‌توانند برای بسیاری از کارمندان بالقوه برای هفت سال گذشته سوابق کیفری را درخواست کنند. اگر متقاضی سالانه بیش از ۷۵۰۰۰ دلار درآمد کسب کند، هیچ محدودیتی برای تاریخ جنایی وجود ندارد. کارفرمایان باید سوابق کیفری استانی و شهرستانها، سوابق متخلف خشونت آمیز جنسی و سوابق زندان را جستجو کنند. بسیاری از شرکت‌ها چنین خدماتی را با هزینه دریافت می‌کنند.

سابقه کار باید تأیید شود. برای تأیید تاریخ کار، موقعیت‌ها، عملکرد و همینطور بابت دلیل ترک کار باید با کارفرمایان سابق تماس گرفته شود. با این حال، متخصصان امنیت باید در نظر داشته باشند که برخی از شرکت‌ها فقط مدت اشتغال را تأیید می‌کنند.

تحقیقات پیشین باید هر رزومه و ادعایی را که در مورد درخواست متقاضی مطرح شده است، تحقیق و بررسی کند. تأیید ادعای متقاضی برای حفاظت از سازمان با اطمینان از اینکه متقاضی دارای مهارت‌ها و تجربه‌ای است که ادعا می‌کند دارای آن مهارت و تجربه است. کارکنان نیز باید براساس سطح اشتغال آنها بازنگری شوند. به عنوان مثال، کارکنان با دسترسی به داده‌های مالی و معاملات باید تحت کنترل‌های اعتباری دوره‌ای قرار گیرند.

تاریخچه اعتبار تضمین می‌کند که پرسنل که در انجام تراکنش‌های مالی برای این سازمان شرکت کرده، خطر کلاهبرداری مالی را ندارند. کمیسیون FCRA و فرصت‌های شغلی برابر (EEOC) Equal Employment Opportunity Commission، دستورالعمل‌هایی را ارائه می‌دهد که می‌تواند به منابع انسانی در این زمینه کمک کند. علاوه بر این، ایده خوبی برای درگیر کردن مشاور حقوقی است.

اگر متقاضی یک وسیله نقلیه را بخشی از کار خود قرار دهد سوابق رانندگی ضروری است. اما غالباً این نوع چک کردن برای متقاضیان دیگر می تواند به افشای مسائل مربوط به سبک زندگی، مانند رانندگی تحت تأثیر یا تعلیق پروانه، کمک کند که بعداً باعث ایجاد مشکلات اشتغال شود. آزمایش سوء مصرف مواد، مصرف مواد مخدر را برای کارفرما آشکار می کند. از آنجا که سابقه مصرف مواد مخدر می تواند باعث بهره وری و غیبت شود، بهتر است قبل از ارائه اشتغال، چنین آزمایشاتی انجام شود. با این حال، متخصصان امنیت باید تضمین کنند که هر گونه آزمایش مواد به وضوح به عنوان بخشی از پست شغلی اعلام شده است.

دو نوع بررسی مرجع انجام می شود: کاری و شخصی. بررسی مرجع کار بررسی سابقه اشتغال می باشد. بررسی مرجع شخصی مراجعه به افرادی که توسط متقاضی ارائه شده است و سؤالات مربوط به توانایی ها، مهارت ها و شخصیت متقاضی را ارائه می دهند. تأیید تحصیلات و مجوزها معمولاً انجام آن بسیار آسان است. کارفرمایان می توانند یک نسخه از آن ها را از موسسات آموزشی درخواست کنند. برای مجوز یا گواهینامه صادر شده شخص، می توان توسط برگزار کننده مجوز یا گواهی نامه، تاییدیه گرفت.

تأییدیه صحت و اعتبار شماره امنیت اجتماعی از طریق تماس با بخش امنیت اجتماعی امکان پذیر است. این بررسی، تضمین می کند که اطلاعات امنیت اجتماعی دقیق است. در صورت سوءاستفاده از شماره تأمین اجتماعی، اداره تأمین اجتماعی به شما هشدار می دهد، مثل اینکه این شماره متعلق به یک فرد متوفی یا شخص در بازداشتگاه می باشد.

درست همانطور که شرکت هایی وجود دارند که می توانند بررسی تاریخ جنایی را ارائه دهند، شرکت ها به تازگی خدمات خود را برای جستجوی تروریست های مظنون لیست های فدرال و بین المللی آغاز کرده اند. سازمان های درگیر در زمینه های دفاعی، هواپیمایی، فناوری و بیوتکنولوژی باید چنین بررسی هایی را برای همه متقاضیان در نظر بگیرند.

همانطور که هر متخصص امنیت می داند، حساسیت اطلاعاتی که متقاضی به آن دسترسی خواهد داشت، باید بزرگترین عامل تعیین کننده بررسی عملکردها باشد. هرگز نباید سازمانها فرایندهای غربالگری متقاضیان را قبل از استخدام با سهل انگاری انجام دهند.

توافق نامه و سیاست های کاری Employment Agreement and Policies

مراحل استخدام پرسنل باید شامل امضای اسناد مناسب، از جمله مستندات مورد نیاز دولت، انتظارات از اعلامیه های حفظ حریم خصوصی و موافقت نامه های عدم افشا Non-Disclosure

Agreements (NDAs) باشد. سازمان‌ها معمولاً یک دفترچه‌ی پرسنلی و اطلاعات استخدامی دیگری دارند که باید به کارمند داده شود. مراحل استخدام باید شامل تأییدیه رسمی باشد که کارمند تمام آموزشها را گذرانده است. شناسه‌های کارکنان و گذرواژه‌ها در این زمان صادر می‌شود.

کد رفتار، تضاد منافع و موافقت نامه‌های اخلاقی نیز باید در این زمان امضا شود. همچنین، هر توافقنامه عدم رقابت باید تأیید شود تا تضمین شود که کارکنان سازمان را به خاطر یک رقیب ترک نکنند. به کارکنان باید دستورالعمل‌هایی برای بررسی عملکرد دوره‌ای، جبران خسارت و شناخت دستاوردها داده شود.

خط مشی‌ها یا سیاست‌های خاتمه کاری Employment Termination Policies

خاتمه دادن به کارکنان باید با توجه به اینکه آیا خاتمه دوستانه یا غیر دوستانه است، متفاوت باشد. پروسه (رویه)‌های تعریف شده توسط بخش منابع انسانی می‌توانند تضمین کنند که مالکیت سازمانی باز می‌گردد، دسترسی کاربر در زمان مناسب حذف می‌شود و مصاحبه‌های خروجی کامل می‌شود. با خاتمه غیر دوستانه، مراحل سازمانی باید به صورت پیشگیرانه باشد تا از آسیب دیدن داراییهای سازمان جلوگیری شود. اداره امنیت باید از ابتدای پروسه فسخ غیر دوستانه مطلع شود. پروسه‌های خاتمه‌پذیری دوستانه باید شامل خاتمه دسترسی به سیستم و تاسیسات و یا غیر فعال کردن اطلاعیه خاتمه کارکنان و همچنین اسکورت امنیتی از محل، صورت گیرد.

فروشنده، مشاور و کنترل پیمانکار Vendor, Consultant, and Contractor Controls

سازمان‌ها اغلب با فروشندگان، مشاوران و پیمانکاران کار می‌کنند. هر شخص ثالثی که به تجهیزات یک سازمان دسترسی پیدا کند، باید به تجهیزات و سایر دارایی‌های سازمانی دسترسی محدود داشته باشد. یک سازمان باید کنترل‌های مناسب را برای اطمینان از عدم وجود این مشکلات در اشخاص ثالث اعمال کند. اشخاص ثالث، حتی افرادی که به طور مکرر بازدید می‌کنند، باید در مرکز سازمان همراهی شوند. اگر شخص ثالث دسترسی دائمی بیشتری نیاز داشته باشد، باید یک تحقیق پیش زمینه انجام شود و موافقت نامه‌های عدم افشای اطلاعات نیز پیاده سازی شود.

نظارت بر هرگونه دسترسی به دارایی‌های شبکه و اطلاعات باید با استفاده از نظارت مجازی و گزارش‌های ممیزی صورت گیرد.

انطباق Compliance

مدیریت همچنین باید تضمین کند که سیاست‌های امنیتی مناسبی در حین اشتغال به کار گرفته شده است. در اوایل این فصل، تفکیک وظایف و چرخش شغل تعریف شد، تفکیک وظایف، حداقل امتیاز و چرخش شغلی در فصل ۷ بیشتر تحت پوشش قرار خواهد گرفت. کنترل دیگر مدیریت تعطیلات الزامی است که مستلزم آن است که کارکنان تعطیلات خود را بگذرانند و کارمند دیگری وظایف شغلی وی را در آن زمان تعطیلات انجام دهد. برخی از مواضع ممکن است برای محافظت از سازمان و دارایی‌های آن حتی بعد از اینکه کارمند دیگر با سازمان نباشند، به توافق نامه‌های اشتغال نیاز داشته باشد. این توافق نامه‌ها می‌توانند شامل NDA ها، شروط غیررقابتی غیر رقابت و توافق نامه‌های رفتار و اخلاق باشند.

حریم خصوصی Privacy

پرسنل انتظار دارند حتی در محل کارشان مقدار مشخصی حریم خصوصی داشته باشند. شرکت‌ها نباید انتظار داشته باشند در سیاست حفظ حریم خصوصی، جزئیات کارکنان را به عنوان خصوصی بودن، از جمله ایمیل شرکت، دسترسی به اینترنت و دسترسی به حوزه‌های امنیتی بالا مشخص باشد. دوربین‌های مدار بسته (CCTV) و سایر تجهیزات ضبط ویدئویی در محل کار رایج هستند. این امر برای نظارت تصویری پارکینگ ها، مناطق کار و مناطق با درجه بالای امنیت قابل قبول است. با این حال، استفاده از نظارت تصویری در حمام، اتاق رختکن، و یا دیگر مناطق هرگز ایده خوبی نمی‌باشد. متخصصان امنیت باید اطمینان حاصل کنند که پرسنل به طور منظم هیچ انتظاری از سیاست حفظ حریم خصوصی سازمان ندارند. در بعضی موارد، ممکن است بخواهند علائم و تابلوهایی را در مناطقی که نظارت تصویری روی آنها اتفاق می‌افتد، قرار دهند.

مفاهیم مدیریت ریسک Risk Management Concepts

هنگام اجرای تجزیه و تحلیل ریسک و مدیریت ریسک، مهم است که مفاهیم مختلف مرتبط با این موضوع درک شود. این بخش شرایط زیر را توضیح می‌دهد: آسیب پذیری، تهدید، عامل تهدید، ریسک، قرار گرفتن در معرض خطر، و اقدامات متقابل.

Vulnerability, Threat, Threat agent, Risk, Exposure, Countermeasure

این بخش همچنین سیاست مدیریت ریسک را مورد بحث قرار می‌دهد. تیم مدیریت ریسک، تیم تحلیل ریسک، ارزیابی ریسک، پیاده سازی، دسته‌های کنترل دسترسی، انواع کنترل دسترسی، ارزیابی کنترل، نظارت و اندازه گیری، گزارش و بهبود مستمر، و چارچوب‌های ریسک.

Risk Management Team, Risk Analysis Team, Risk Assessment, Implementation, Access Control Categories, Access Control Types, Control Assessment, Monitoring, Measurement, Reporting and Continuous Improvement, Risk Frameworks.

۱- آسیب پذیری Vulnerability

یک آسیب پذیری، فقدان یا ضعف یک اقدام متقابل است که در آن قرار دارد. آسیب پذیری‌ها در نرم افزار، سخت افزار یا پرسنل رخ می‌دهد. یک نمونه از یک آسیب پذیری، دسترسی نامحدود به یک پوشه (Folder) در رایانه است. اکثر سازمان‌ها ارزیابی آسیب پذیری را برای شناسایی آسیب پذیری‌ها انجام می‌دهند.

۲- تهدید Threat

تهدید پیشرفت منطقی بعدی در مدیریت ریسک است. تهدید زمانی رخ می‌دهد که آسیب پذیری شناسایی یا اجرا شود. یک حمله زمانی رخ می‌دهد که یک مهاجم پوشه‌ای را که رایانه، ACL نامناسب یا غلط دارد شناسایی کند.

۳- عامل تهدید Threat Agent

تهدید توسط عامل تهدید انجام می‌شود. مهاجم که از ACL نامناسب استفاده می‌کند یک عامل تهدید می‌باشد. با این حال، در نظر داشته باشید که عوامل تهدید می‌توانند آسیب پذیری‌ها را کشف و استفاده کنند. در واقع همه عوامل تهدید یک آسیب پذیری شناخته شده نیستند.

۴- ریسک Risk

ریسک احتمالی که یک عامل تهدید در صورت انجام تهدید از آسیب پذیری و تأثیر آن سوء استفاده کند. به عنوان مثال اگر داده‌های موجود در پوشه محرمانه باشد ریسک آسیب پذیری نسبتاً بالا خواهد بود. با این حال، اگر پوشه فقط حاوی اطلاعات عمومی باشد، این ریسک پایین

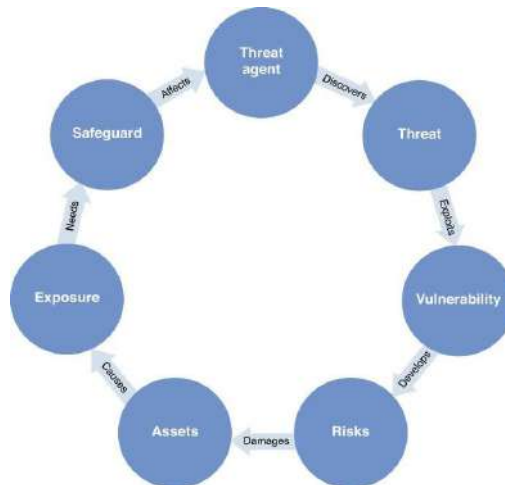
خواهد بود. اغلب برای شناسایی تاثیر بالقوه ریسک، به متخصصان امنیت برای کمک به این موضوع ویژه، نیاز است.

۵- در معرض چیزی قرار گرفتن Exposure

قرار گرفتن در معرض، زمانی رخ می دهد که یک دارایی سازمانی در معرض زیان است. اگر پوشه ای با ACL نامناسب یا غایب توسط یک عامل تهدید به خطر بیافتد، سازمان احتمالا در معرض قرار گرفتن افشا اطلاعات و از دست دادن اطلاعات قرار دارد.

۶- اقدامات متقابل Countermeasure

اقدامات متقابل احتمال ریسک را کاهش می دهد. مقابله با اقدامات نیز به عنوان حراست یا کنترل شناخته می شود. هنگام اجرای یک اقدام متقابل سه چیز باید در نظر گرفته شود: آسیب پذیری، تهدید و ریسک. برای مثال یک اقدام متقابل مناسب اجرای ACL مناسب و رمزگذاری داده ها است. ACL از یکپارچگی داده ها، و رمزگذاری از محرمانه بودن داده ها محافظت می کند. اقدامات متقابل و کنترل ها دارای انواع و اقسامی می باشد. دسته ها و انواع کنترل ها بعدا در این فصل مورد بحث قرار می گیرند. تمام مفاهیم امنیتی فوق الذکر در روابطی که در شکل ۱-۱۳ نشان داده شده است با یکدیگر همکاری می کنند.



شکل ۱-۱۳: چرخه مفهوم امنیت

سیاست مدیریت ریسک Risk Management Policy

مدیران ارشد باید به فرایند مدیریت ریسک متعهد باشند. سیاست مدیریت ریسک یک بیانیه رسمی تعهد مدیریت ارشد به مدیریت ریسک است. این سیاست همچنین جهت گیری مدیریت ریسک را فراهم می کند.

یک سیاست مدیریت ریسک باید شامل طرح کلی مدیریت ریسک و لیست تیم مدیریت ریسک باشد و باید لیست اهداف، مسئولیت ها و نقش های تیم مدیریت ریسک، سطح قابل قبول ریسک، فرایند شناسایی ریسک، نقشه برداری و حراست ریسک، اثربخشی حفاظت، پروسه نظارت و اهداف و برنامه ها و روش های تجزیه و تحلیل ریسک آتی، مشخص باشند.

تیم مدیریت ریسک Risk Management Team

بسته به اندازه سازمان، تیم مدیریت ریسک ممکن است یک تیم واقعی از کارمندان باشد یا فقط از یک عضو تیم تشکیل شده باشد. برای هر سازمان، هدف تیم محافظت از سازمان و دارایی های در معرض خطر با به صرفه ترین روش است. از آنجا که در بیشتر موارد، اعضای تیم مدیریت ریسک صرفاً به مدیریت ریسک اختصاص نمی یابند، مدیریت ارشد باید به طور خاص یک معیار تخصیص منابع را در نظر بگیرد تا از موفقیت فرایند مدیریت ریسک مطمئن شود.

مدیریت همچنین باید از اعضای تیم مدیریت ریسک، بویژه رهبر تیم، آموزش و ابزار لازم برای مدیریت ریسک را بدست آورد. در سازمانهای بزرگتر، رهبر تیم باید بتواند بیشتر وقت خود را به فرایند مدیریت ریسک اختصاص دهد.

تیم تحلیل ریسک Risk Analysis Team

برای انجام جامع ترین تجزیه و تحلیل ریسک، تیم تجزیه و تحلیل ریسک باید در حد امکان شامل یک نماینده از تعدادی دپارتمان و همچنین تعدادی در سطح کارمندان باشد. داشتن یک تیم تجزیه و تحلیل متنوع ریسک تضمین می کند که ریسک های ناشی از همه مناطق سازمان می تواند تعیین شود.

تیم تجزیه و تحلیل ریسک نمیتواند شامل اعضای همه دپارتمان ها باشد، اعضای تیم باید از هر دپارتمان مصاحبه کنند تا همه تهدیدات موجود در آن واحد را درک کنند. در طی فرایند تحلیل

ریسک، تیم تجزیه و تحلیل ریسک باید وقایع تهدیدی را که ممکن است رخ دهد، تأثیر احتمالی تهدیدها، فراوانی تهدیدها و میزان اطمینان در اطلاعات جمع آوری شده را تعیین کند.

ارزیابی ریسک Risk Assessment

ارزیابی ریسک یک ابزار در مدیریت ریسک می باشد که برای شناسایی آسیب پذیری ها و تهدیدات استفاده می شود، تأثیر آسیب پذیری ها و تهدیدها را ارزیابی می کند و تعیین می کند کدام کنترل را برای پیاده سازی انجام دهد. ارزیابی یا تحلیل ریسک چهار هدف اصلی دارد:

- ✓ شناسایی دارایی ها و ارزش دارایی ها.
- ✓ شناسایی آسیب پذیری ها و تهدیدات.
- ✓ محاسبه احتمال تهدید و تأثیر کسب و کار.
- ✓ اثر تهدید تعادلی با هزینه اقدامات متقابل.

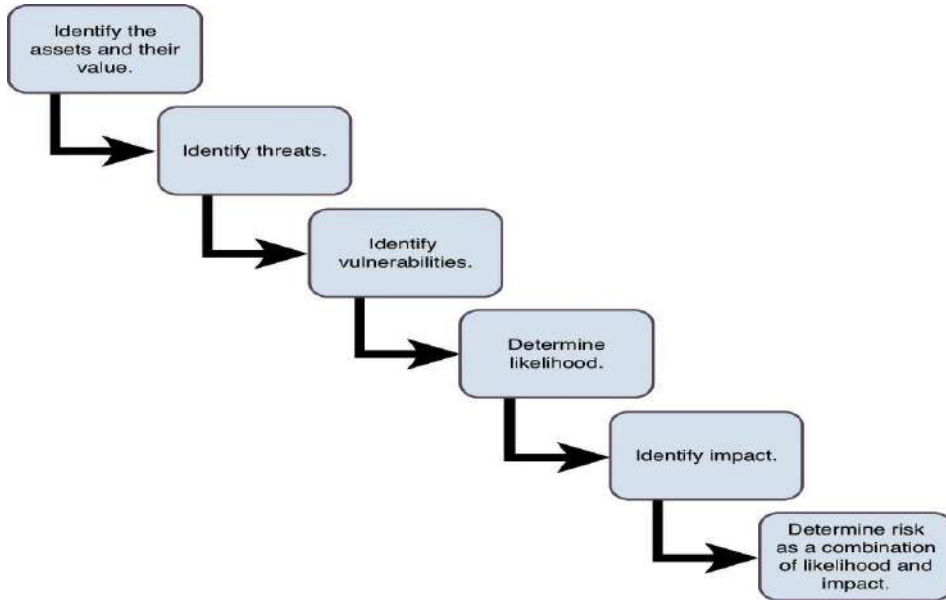
قبل از شروع ارزیابی ریسک، مدیریت و تیم ارزیابی ریسک باید تعیین کنند که چه دارایی ها و تهدیدهایی باید در نظر گرفته شود. این فرایند اندازه پروژه را تعیین می کند، سپس تیم ارزیابی ریسک باید گزارشی را در مورد ارزش دارایی های در نظر گرفته شده را به مدیریت ارائه دهد. سپس مدیریت می تواند فهرست دارایی را بررسی و نهایی کرده، دارایی ها را به همان اندازه که مناسب است اضافه و حذف کرده، و سپس بودجه ارزیابی ریسک را تعیین کند.

اگر ارزیابی ریسک توسط مدیریت ارشد پشتیبانی نشود، به موفقیت دست پیدا نخواهد کرد. مدیریت باید هدف و دامنه ارزیابی ریسک را تعریف کرده و پرسنل، زمان، منابع مالی را به پروژه اختصاص دهد.

طبق NIST SP 800-30 تکنیک های جمع آوری اطلاعات مورد استفاده در تجزیه و تحلیل ریسک عبارتند از: ابزار ارزیابی خودکار ریسک، پرسشنامه ها، مصاحبه ها و بررسی سند سیاست. به خاطر داشته باشید که برای تعیین ریسک ها در یک دارایی، باید از منابع مختلفی استفاده شود. NIST SP 800-30 مراحل زیر را در فرایند ارزیابی ریسک مشخص می کند:

- ۱- شناسایی دارایی ها و ارزش آنها.
- ۲- شناسایی تهدیدها
- ۳- شناسایی آسیب پذیری ها
- ۴- تعیین احتمال
- ۵- شناسایی اثر

۶- ریسک را به عنوان ترکیبی از احتمال و تأثیر تعیین کند.
 شکل ۱-۱۴ فرایند ارزیابی ریسک را با توجه به NIST SP 800-30 نشان می‌دهد.



شکل ۱-۱۴: روند ارزیابی ریسک NIST SP 800-30

متخصصان امنیت همچنین می‌توانند دو نشریه دیگر NIST را بررسی کنند:

SP 800-39 SP 800-66r1

SP 800-39 راهنمایی برای برنامه‌های یکپارچه و سازمانی برای مدیریت ریسک امنیت اطلاعات برای عملیات سازمانی، دارایی‌های سازمانی، افراد، سازمانهای دیگر و کشور حاصل از بهره‌برداری و استفاده از سیستم‌های اطلاعاتی فدرال را فراهم می‌کند.

SP 800-66r1 به طور خاص برای ریسک‌های مربوط به سازمان‌هایی که باید با قانون امنیت HIPAA مطابقت داشته باشند، نوشته شده است. تمام اسناد NIST را می‌توانید در وب سایت

NIST مشاهده کنید: <http://csrc.nist.gov>

هزینه ها و ارزش اطلاعات و دارایی (ملموس / نا ملموس)

Information and Asset (Tangible/Intangible) Value and Costs

همانطور که قبلاً گفته شد، اولین قدم برای ارزیابی ریسک، شناسایی دارایی ها و تعیین ارزش دارایی است. دارایی ها به دو صورت ملموس و نا ملموس هستند. دارایی های ملموس شامل رایانه، تاسیسات، تجهیزات و پرسنل هستند. دارایی های نا ملموس شامل مالکیت معنوی، داده ها و شهرت سازمانی هستند. ارزش دارایی باید از دید صاحب دارایی در نظر گرفته شود. شش مورد زیر می تواند برای تعیین ارزش دارایی استفاده شود:

- ارزش برای مالک
 - فعالیت مورد نیاز برای توسعه یا بدست آوردن دارایی
 - هزینه نگهداری دارایی
 - آسیب هایی که در صورت خرابی دارایی اتفاق می افتد
 - هزینه ای که رقا برای دارایی پرداخت می کنند
 - جریمه هایی که در صورت خرابی و از بین رفتن دارایی حاصل می شود.
- بعد از تعیین ارزش دارایی ها، باید آسیب پذیری ها و تهدیدات هر دارایی تعیین شود.

شناسایی تهدیدها و آسیب پذیری ها Identify Threats and Vulnerabilities

هنگام شناسایی آسیب پذیری ها و تهدیدات یک دارایی، با توجه به عوامل تهدید کننده، عوامل تهدید را می توان به شش دسته زیر تقسیم بندی کرد:

- انسان Human: شامل هر شخص ثالث مخرب و غیر مخرب و بیگانه، تروریست ها، جاسوسان و پرسنل جدا شده از سازمان
- طبیعی Natural: شامل سیل، آتش سوزی، گردبادها، طوفان، زلزله یا دیگر فاجعه طبیعی یا رخداد آب و هوایی.
- فنی Technical: شامل سخت افزار و شکست نرم افزار، کد مخرب و فن آوری های جدید است.
- فیزیکی Physical: مسائل مربوط به دوربین مدار بسته CCTV، مسائل زیست محیطی و شکست بیومتریک را شامل می شود.

- محیط Environmental: شامل اختلالات برق و دیگر ابزارها، مسائل مربوط به ترافیک، جنگ‌های زیست محیطی و مسائل مربوط به مواد خطرناک (از جمله سرریز شدن)
- عملیاتی Operational: شامل هر روش یا فرایندی است که می‌تواند بر CIA تاثیر گذارد.

هنگامی که آسیب پذیری‌ها و تهدیدها شناسایی شده است، پتانسیل شکست باید مشخص شود. این پتانسیل شکست با استفاده از احتمال رخداد شکست همراه با تأثیری که از چنین رخدادی ایجاد شده تعیین می‌شود. یک رخداد با احتمال زیاد و تأثیرات بالا اهمیت بیشتری نسبت به یک رخداد با احتمال کم و تأثیر کم دارد. برای اطمینان از اینکه داده‌هایی که بدست می‌آیند به حداکثر برسد، باید از انواع مختلف تحلیل ریسک، از جمله تجزیه و تحلیل ریسک کمی و تجزیه و تحلیل ریسک کیفی، استفاده شود.

ارزیابی ریسک / تجزیه و تحلیل Risk Assessment/Analysis

هنگامی که تیم تجزیه و تحلیل ریسک شکل می‌گیرد، وقت آن رسیده که در ابتدا تجزیه و تحلیل ریسک یا فرایند ارزیابی آغاز شود. این فرایند شامل دو نوع مختلف تجزیه و تحلیل ریسک است: تجزیه و تحلیل ریسک کمی و تجزیه و تحلیل ریسک کیفی.

تجزیه و تحلیل ریسک کمی Quantitative Risk Analysis

تجزیه و تحلیل ریسک کمی مقدار مقادیر مالی و عددی را به تمامی جنبه‌های فرایند تحلیل ریسک، از جمله ارزش دارایی، فرکانس تهدید، شدت آسیب پذیری، تاثیر، هزینه‌های حفاظت و غیره، اختصاص می‌دهد. معادلات برای تعیین ریسک‌های کلی و باقی مانده استفاده می‌شود. شایع ترین معادلات برای احتمال از دست دادن فردی (SLE) Single loss expectancy و احتمال از دست دادن سالانه (ALE) Annual loss expectancy است.

SLE تاثیر مالی هر رخداد تهدید است. برای تعیین SLE، باید ارزش دارایی AV و ضریب در معرض افشاء (EF) را دانست. EF ارزش درصد یا عملکرد یک دارایی است که وقتی یک تهدید رخ می‌دهد از بین می‌رود. محاسبه برای دستیابی به SLE به شرح زیر است:

$$SLE = AV \times EF$$

به عنوان مثال، یک سازمان دارای وب سرور با AV، 20000 دلار است. اگر ارزیابی ریسک مشخص کرده باشد که خرابی برق عامل تهدید برای وب سرور وب است و میزان قرار گرفتن در معرض خرابی برق ۲۵٪ است، SLE برای این رخداد برابر ۵،۰۰۰ دلار است.

ALE عامل ریسک احتمالی تهدید سالانه است. برای تعیین ALE، باید SLE و نرخ سالانه وقوع (ARO) را دانست. ARO تخمین می‌زند که چند بار یک تهدید خاص در سال رخ می‌دهد. محاسبه برای به دست آوردن ALE به شرح زیر است:

$$ALE = SLE \times ARO$$

با استفاده از مثال قبلا ذکر شده، اگر ارزیابی ریسک تعیین کرده است که ARO برای قدرت خرابی Web Server Farm مزرعه وب سرور ۵۰٪ است، ALE برای این رخداد برابر با ۲۵۰۰ دلار است. متخصصان امنیت باید در نظر داشته باشند که این محاسبه را می‌توان برای مکان‌های مختلف جغرافیایی تنظیم کرد. به عنوان مثال، یک سرور DNS واقع در یک شهر کوچک ممکن است ریسک بیشتر قطعی برق را نسبت به یک شهر بزرگ داشته باشد.

با استفاده از ALE، سازمان می‌تواند تصمیم بگیرد که آیا اجرای کنترل‌ها را انجام می‌دهد یا خیر. اگر هزینه سالانه کنترل برای محافظت از مزرعه وب سرور بیش از ALE باشد، سازمان می‌تواند به راحتی با عدم اجرای کنترل، ریسک‌ها را بپذیرد. اگر هزینه سالانه کنترل برای محافظت از مزرعه وب سرور کمتر از ALE باشد، سازمان باید اجرای کنترل را در نظر بگیرد.

به خاطر داشته باشید اگرچه تجزیه و تحلیل ریسک کمی با استفاده از ارزش عددی انجام می‌شود، اما به طور دقیق نمی‌تواند بدست بیاید زیرا برخی از متغیرها همیشه بخشی از داده‌ها هستند. در مثال فوق، سازمان چگونه می‌داند که آسیب ناشی از خرابی برق ۲۵٪ از دارایی است؟ این نوع برآورد باید بر اساس داده‌های قبلی، تجربه صنعتی و نظر کارشناس باشد.

مزیت کمی در برابر تجزیه و تحلیل ریسک کیفی این است که استفاده کمی از حدس و گمان کمتری نسبت به کیفی برخوردار است. معایب تجزیه و تحلیل ریسک کمی شامل مشکل معادلات، زمان و تلاش مورد نیاز برای تکمیل تجزیه و تحلیل، و سطح داده‌ها که باید برای تجزیه و تحلیل جمع آوری شود.

تجزیه و تحلیل ریسک کیفی Qualitative Risk Analysis

تجزیه و تحلیل ریسک کیفی ارزش مالی و عددی را به تمام جنبه‌های فرایند تحلیل ریسک اختصاص نمی‌دهد. تکنیک‌های تجزیه و تحلیل ریسک کیفی شامل شهود، تجربه و تکنیک‌های

بهتر عمل کردن، مانند طوفان مغزی، گروه‌های متمرکز، نظرسنجی‌ها، پرسشنامه‌ها، جلسات، مصاحبه‌ها و دلفی می‌باشد. اگر چه تمام این تکنیک‌ها می‌توانند مورد استفاده قرار گیرند، اما اکثر سازمان‌ها بهترین روش‌ها را بر اساس تهدیدات ارزیابی می‌کنند، که تجربه و آموزش در مورد تهدیدات مورد نیاز است.

هر عضو گروه که برای تجزیه و تحلیل ریسک کیفی انتخاب شده، از تجربه خود برای ارزیابی احتمال هر تهدید و آسیب احتمالی استفاده می‌کند. هر عضو گروه، احتمال تهدید، پتانسیل خسارت و مزیت حفاظت داده را به صورت ترکیبی از یک گزارش به مدیریت ارائه می‌دهد. تمام سطوح کارکنان باید بخشی از تجزیه و تحلیل ریسک کیفی را ارائه دهند، اما ضروری است شرکت کنندگان در این فرآیند در تحلیل ریسک تخصص داشته باشند.

مزایای تجزیه و تحلیل ریسک کیفی در مقابل کمی شامل اولویت بندی کیفی ریسک‌ها و شناسایی مناطق برای بهبود فوری در رسیدگی به تهدید است. معایب تجزیه و تحلیل ریسک کیفی شامل نتایج ذهنی می‌باشد و دارای ارزش مالی و تجزیه و تحلیل هزینه-سود نبوده یا کمکی به بودجه نمی‌کند.

تذکر:

هنگام انجام تجزیه و تحلیل ریسک، تمام سازمان‌ها مسائل را با هر تخمینی که بدست می‌آورند تجربه می‌کنند. این عدم اطمینان در تخمین به عنوان عدم اطمینان نامیده می‌شود و به صورت درصدی بیان می‌شود. هر گزارش مربوط به ارزیابی ریسک باید شامل عدم اطمینان باشد. بیشتر تحلیل ریسک شامل استفاده ترکیبی از دو تجزیه و تحلیل کمی و کیفی ریسک می‌باشد. اکثر سازمان‌ها از تجزیه و تحلیل ریسک کمی برای دارایی‌های ملموس و تجزیه و تحلیل ریسک کیفی برای دارایی‌های ناملموس استفاده می‌کنند.

اقدام متقابل (حفاظت) منتخب Countermeasure (Safeguard) Selection

رایج ترین معیارها برای انتخاب حفاظت، هزینه یابی حفاظت یا کنترل است. هزینه‌های برنامه ریزی، طراحی، پیاده سازی و نگهداری باید در تعیین هزینه کل حفاظتی safeguard گنجانده شود. برای محاسبه تجزیه و تحلیل هزینه - سود، از معادله زیر استفاده می‌شود:

(هزینه سالانه حفاظت) - (ALE پس از حفاظت) - (ALE قبل از حفاظت) = ارزش حفاظت
برای تکمیل این معادله، بعد از اینکه حفاظت پیاده سازی شد باید تجدید نظر ALE را بدانید. پیاده سازی یک سرویس امنیتی می‌تواند ARO را بهبود بخشد، اما به طور کامل با آن روبرو

نخواهد شد. در مثال ذکر شده در بخش " تجزیه و تحلیل کمی ریسک " ALE برای این رخداد ۲۵۰۰ دلار است. فرض کنیم که اجرای حفاظت، ARO را به ۱۰٪ کاهش می دهد، بنابراین ALE پس از محافظت، محاسبه می شود: $\$5,000 \times 10\%$ یا $\$500$. سپس می توانید ارزش حفاظتی برای کنترل که ۱۰۰۰ دلار هزینه سالانه دارد به شرح زیر محاسبه کنید:

$$\$2,500 - \$500 - \$1,000 = \$1,000$$

دانستن ARO تصحیح شده پس از حفاظت برای تعیین ارزش حفاظتی ضروری است. مسئولیت قانونی وجود دارد اگر هزینه حفاظت کمتر از خسارت تخمین زده شده است در این صورت تهدید مورد سوء استفاده قرار می گیرد.

هزینه های تعمیر و نگهداری حفاظتی اغلب در طول این فرایند در نظر گرفته نمی شود. سازمانها باید هزینه های نگهداری حفاظتی را به طور کامل بررسی کنند. کارمندان جدید و یا کارمندان مشغول به کار باید بارها آموزش گسترده به منظور حفظ ایمنی جدید، ببینند. علاوه بر این، هزینه تلاش کارمند درگیر این فعالیت باید تعیین شود. بنابراین هزینه حفاظت باید شامل هزینه واقعی برای پیاده سازی به همراه هزینه های آموزشی، هزینه های آزمایش، هزینه های تلاش کارمند و غیره می باشد. برخی از این هزینه ها ممکن است دشوار باشد اما یک تحلیل کامل ریسک برای این هزینه ها به حساب می آید.

ریسک کامل در مقابل ریسک باقی مانده Total Risk Versus Residual Risk

ریسک کامل ریسکی است که یک سازمان می تواند در صورت عدم تصمیم به اجرای هرگونه حفاظت با آن روبرو شود. همانطور که از قبل می دانید، هیچ محیطی کاملاً ایمن نیست، بنابراین همیشه باید با ریسک باقی مانده مقابله کنید. ریسک باقیمانده ریسکی است که پس از اجرای اقدامات حفاظتی باقیمانده است. ریسک باقیمانده با استفاده از معادله زیر نشان داده شده است:

$$\text{اقدامات متقابل} - \text{ریسک کامل} = \text{ریسک باقی مانده}$$

این معادله مفهومی تر از محاسبه واقعی در نظر گرفته می شود.

اداره کردن ریسک Handling Risk

کاهش ریسک فرایند تغییر عناصر سازمان در پاسخ به تحلیل ریسک است. بعد از آنکه سازمان ریسک کامل و ریسک باقیمانده خود را درک کرد، باید چگونگی مقابله با این ریسک را تعیین کند. چهار روش اساسی زیر برای مقابله با ریسک استفاده می‌شود:

- اجتناب از ریسک Risk avoidance: پایان دادن به فعالیتهایی که باعث ریسک یا انتخاب یک جایگزین می‌شوند که به اندازه ریسک نمی‌باشد.
- انتقال ریسک Risk transfer: ریسک را به شخص ثالث، از جمله شرکت‌های بیمه انتقال می‌دهد.
- کاهش ریسک Risk mitigation: تعریف سطح ریسک پذیری که سازمان می‌تواند تحمل کند و ریسک را به آن سطح کاهش دهد.
- پذیرش ریسک Risk acceptance: درک و پذیرش میزان ریسک و همچنین هزینه آسیب‌های وارده که می‌تواند اتفاق بیفتد.

پیاده سازی Implementation

قبل از اجرای هرگونه کنترل که به عنوان بخشی از فرآیند تحلیل ریسک انتخاب شده باشد، متخصصان امنیت باید چارچوب‌های مورد استفاده برای مرجع، ابزارهای مستقر شده و معیارهای مربوط به مدیریت کنترل‌ها را در نظر بگیرند. این سه وجه تضمین کننده موفقیت معماری امنیت است. هدف از اجرای اقدامات متقابل ریسک بهبود امنیت سازمان بدون تأثیر منفی بر عملکرد است.

همه پرسنل سازمان باید در بکارگیری اقدامات متقابل برای مدیریت ریسک شرکت کنند. هر فردی که در پیاده سازی قرار دارد، یک دیدگاه منحصر به فرد در مورد ریسک‌ها در آن موقعیت فردی خواهد داشت. مستندات و ارتباطات در همه زمینه‌ها تضمین خواهد کرد که اجرای مدیریت ریسک هر واحد کسب و کار تا حد امکان کامل باشد.

طبقه بندی کنترل دسترسی Access Control Categories

کنترل های دسترسی Access Controls را به عنوان یک اقدام متقابل برای شناسایی آسیب پذیری ها اعمال می شود. مکانیزم های کنترل دسترسی که می توان استفاده کرد به هفت دسته اصلی تقسیم می شوند:

- جبران کننده Compensative
- تصحیح کننده Corrective
- کاراگاه Detective
- مهار Deterrent
- دستورالعمل Directive
- پیشگیرانه Preventive
- بازیابی Recovery

هر کنترل دسترسی که پیاده سازی می شود، در یک یا چند گروه کنترل دسترسی قرار می گیرد. تذکر: کنترل های دسترسی نیز با توجه به نوع حفاظتی که ارائه می دهند تعریف می شوند.

جبران کننده Compensative

کنترل های جبران کننده جایگزینی برای کنترل دسترسی اولیه هستند و عمدتاً به عنوان کاهش ریسک ها عمل می کنند. با استفاده از کنترل های جبرانی، می توان ریسک را به یک سطح قابل کنترل تری کاهش داد. نمونه هایی از کنترل های جبرانی نیاز به دو امضای مجاز برای انتشار اطلاعات حساس یا محرمانه و نیاز به دو کلید متعلق به پرسنل مختلف برای باز کردن صندوق امانات دارند.

تصحیح کننده Corrective

کنترل های اصلاحی یا تصحیح کننده برای کاهش اثر یک حمله یا رخداد های نامطلوب دیگر می باشد. با استفاده از کنترل های اصلاحی موردی که دچاره حمله شده است را اصلاح یا بازیابی می کند. نمونه هایی از کنترل های اصلاح کننده شامل نصب فایروال ها، جدا سازی یا قطع اتصال، اجرای قوانین فایروال جدید و استفاده از تصاویر سرور برای بازگرداندن به حالت قبلی است.

کارآگاه Detective

کنترل‌های کارآگاهی برای تشخیص حمله در زمان وقوع، به پرسنل مختص این کار هشدار می‌دهد. نمونه‌هایی از کنترل‌های کارآگاهی شامل ردیاب‌های حرکتی، IDS ها، گزارش‌های مربوط، محافظان (حراست)، تحقیقات و چرخش شغلی (Motion detectors, IDSs, Logs, Guards, Investigations, Job Rotation)، است.

مهار (بازدارنده) Deterrent

کنترل‌های بازدارنده باعث جلوگیری یا دلسردی مهاجم می‌شود. از طریق کنترل‌های بازدارنده، حملات می‌توانند در مراحل اولیه کشف شوند. کنترل‌های بازدارنده غالباً باعث کنترل‌های پیشگیرانه و اصلاحی می‌شوند. نمونه‌هایی از کنترل‌های بازدارنده شامل شناسایی و احراز هویت کاربر، نرده‌ها یا فنس‌ها، روشنایی و سیاست‌های امنیتی سازمان مانند توافق نامه عدم افشاء یا همان NDA است.

دستورالعمل Directive

نظارت بر دستورالعمل، عملکرد قابل قبولی را در یک سازمان مشخص می‌کند. آنها در محل به طور عمده، دستورالعمل امنیت سازمان را برای کارکنان خود ترسیم می‌کنند. رایج ترین کنترل دستورالعمل، یک سیاست استفاده قابل قبول AUP است که لیست متناسب (اغلب نمونه‌هایی از موارد نامناسب) رویه‌ها و رفتارهایی است که پرسنل باید دنبال کنند. معمولاً هرگونه سیاست یا امنیت سازمانی در این گروه کنترل دسترسی قرار می‌گیرد. باید در نظر داشت که کنترل‌های دستورالعمل فقط در صورتی مؤثر هستند که پیامدی را برای عدم پیروی از دستورالعمل‌های سازمان داشته باشند.

پیشگیرانه Preventive

کنترل‌های پیشگیرانه از وقوع حمله جلوگیری می‌کند. نمونه‌هایی از کنترل‌های پیشگیرانه شامل قفل‌ها، نشان‌ها و بیج‌ها، سیستم‌های بیومتریک، رمزگذاری، سیستم‌های پیشگیری از نفوذ (IPS ها) Intrusion Prevention Systems، نرم افزار آنتی ویروس، پرسنل امنیتی، نگهبانان امنیتی، گذر واژه‌ها و آموزش آگاهی از امنیت است.

بازیابی Recovery

کنترل بازیابی یک سیستم یا دستگاه پس از حمله رخ می دهد. هدف اصلی کنترل های بازیابی، بازگرداندن منابع است. نمونه هایی از کنترل های بازیابی عبارتند از برنامه بهبود فاجعه، پشتیبان گیری از داده ها و تاسیسات خارج از محل یا سایت.

انواع کنترل دسترسی Access Control Types

در حالی که دسته های کنترل دسترسی، بر اساس مکانی که در آن جا قرار می گیرند، طبقه بندی می شوند، انواع کنترل دسترسی، بر اساس روش اجرای آنها تقسیم می شوند. سه نوع کنترل دسترسی وجود دارد.

- کنترل های اداری (مدیریتی)
- کنترل های منطقی (فنی)
- کنترل های فیزیکی

هر سازمانی که دفاع در عمق یک اولویت است، کنترل دسترسی نیاز به استفاده از هر سه نوع کنترل دسترسی دارد. حتی اگر شدیدترین کنترل های فیزیکی و اداری اعمال شود، نمی توان بدون کنترل منطقی از محیط کاملاً محافظت کرد.

▪ کنترل های اداری (مدیریتی) Administrative (Management) Controls

کنترل های اداری یا مدیریتی برای مدیریت دارایی ها و کارکنان سازمان به کار گرفته شده و شامل سیاست های امنیتی، رویه ها، استانداردها، مقدمات و دستورالعمل هایی است که توسط مدیریت ایجاد می شود. این کنترل ها معمولاً به عنوان کنترل های نرم یاد می شوند. نمونه های خاص شامل کنترل پرسنل، طبقه بندی داده ها، برچسب زدن به داده ها، آموزش آگاهی از امنیت و نظارت است.

آموزش آگاهی از امنیت یک کنترل بسیار مهم مدیریتی است. هدف آن بهبود نگرش سازمان در مورد حفاظت از داده ها است. مزایای آموزش آگاهی امنیت عبارتند از: کاهش تعداد و شدت خطاها و اشکالات، درک بهتر ارزش اطلاعات و شناخت مدیریتی برای جلوگیری از تلاش برای مجوزهای غیرمجاز می باشد. یک راه مقرون به صرفه برای اطمینان از اینکه کارکنان، آگاهی امنیت را جدی بگیرند، ایجاد یک برنامه پاداش یا شناسایی است.

جدول ۱-۴ بسیاری از کنترل‌های اداری را ذکر کرده و دسته‌هایی از کنترل دسترسی را در خود جای می‌دهد.

Administrative (Management) Controls	Compensative	Corrective	Detective	Deterrent	Directive	Preventive	Recovery
Personnel procedures						X	
Security policies				X	X	X	
Monitoring			X				
Separation of duties						X	
Job rotation	X		X				
Information classification						X	
Security awareness training						X	
Investigations			X				
Disaster recovery plan						X	X
Security reviews			X				
Background checks			X				
Termination		X					
Supervision	X						

جدول ۱-۴: کنترل‌های اداری (مدیریتی)

متخصصان امنیت باید به تدوین سیاست‌ها و رویه‌ها یا پرونده‌های سازمان کمک کنند تا اطمینان حاصل شود که پرسنل آن چه از آنها انتظار می‌رود و نحوه انجام وظایف خود را درک می‌کنند. ارزیابی متقاضی قبل از استخدام نیز برای حفاظت از سازمان مهم است. امنیت شخصی، ارزیابی و اطمینان کامل حاصل شود که پرسنل فقط به آن منابع یا حوزه‌های مورد نیاز نقش‌های خاص خود در داخل سازمان دسترسی دارند. نظارت و گزارش‌ها تضمین می‌کند که متخصصان امنیت راهی برای تحلیل رفتار دارند. دسترسی کاربر باید از جمله تأیید دسترسی کاربر، شناسه

کاربر منحصر به فرد، بررسی های دوره ای از دسترسی کاربر، فرایندهای گذرواژه کاربر و روشهای اصلاح و ابطال دسترسی مدیریت شود.

• کنترل های منطقی (فنی) Logical (Technical) Controls

کنترل های منطقی یا فنی نرم افزاری است که برای محدود کردن دسترسی استفاده می شود. نمونه های خاصی از کنترل های منطقی شامل فایروال ها، IDS ها، IPS ها، رمزگذاری، سیستم های احراز هویت، پروتکل ها، ممیزی و نظارت، بیومتریک، کارت های هوشمند و گذرواژه ها هستند. گرچه ممیزی نظارت کنترل های منطقی هستند و اغلب در کنار هم قرار گرفته اند، اما در واقع آنها دو کنترل متفاوت هستند. ممیزی یک رخداد یکباره One-time یا دوره ای Periodic برای ارزیابی امنیت است. نظارت Monitoring فعالیتی در حال انجام است که سیستم یا کاربران را مورد بررسی قرار می دهد.

جدول ۱-۵ بسیاری از کنترل های منطقی را ذکر کرده و دسته هایی از کنترل دسترسی را در خود جای می دهد.

Logical (Technical) Controls	Compensative	Corrective	Detective	Deterrent	Directive	Preventive	Recovery
Password						X	
Biometrics						X	
Smart cards						X	
Encryption						X	
Protocols						X	
Firewalls						X	
IDS			X				
IPS						X	
Access control lists						X	
Routers						X	
Auditing			X				
Monitoring			X				
Data backups							X
Antivirus software						X	
Configuration standards					X		
Warning banners				X			
Connection isolation and termination		X					

جدول ۱-۵: کنترل های منطقی (فنی)

دسترسی به شبکه، دسترسی از راه دور، دسترسی به برنامه و دسترسی رایانه یا دستگاه همه در این گروه قرار دارند.

▪ کنترل فیزیکی Physical Controls

کنترل‌های فیزیکی برای حفاظت از تاسیسات و پرسنل سازمان انجام می‌شود. دغدغه‌های پرسنلی باید نسبت به سایر دغدغه‌ها اولویت داشته باشد. نمونه‌های خاصی از کنترل‌های فیزیکی شامل امنیت محیط، نشان‌ها، ربودن کارت‌ها، نگهبانان، سگ‌ها، تله‌های انسانی، بیومتریک و کابل کشی هستند.

جدول ۱-۶ بسیاری از کنترل‌های فیزیکی را نشان می‌دهد و دسته‌هایی از کنترل دسترسی را در خود جای می‌دهد.

Physical (Technical) Controls	Compensative	Corrective	Detective	Deterrent	Directive	Preventive	Recovery
Fencing				X		X	
Locks						X	
Guards			X			X	
Fire extinguisher		X					
Badges						X	
Swipe cards						X	
Dogs			X			X	
Man traps						X	
Biometrics						X	
Lighting				X			
Motion detectors			X				
CCTV	X		X			X	
Data backups							X
Antivirus software						X	
Configuration standards					X		
Warning banner				X			
Hot, warm, and cold sites							X

جدول ۱-۶: کنترل فیزیکی

هنگام کنترل ورود فیزیکی به یک ساختمان، متخصصان امنیت باید تضمین کنند که سیاست‌های مناسب برای کنترل بازدیدکنندگان، از جمله log بازدید کنندگان، اسکورت بازدید کننده و محدودیت دسترسی بازدیدکنندگان به مناطق حساس اعمال شده است.

ارزیابی کنترل، نظارت و اندازه گیری Control Assessment, Monitoring, and Measurement

ارزیابی‌های کنترل امنیتی باید مورد استفاده قرار گیرد تا تأیید شود که اهداف امنیتی یک سازمان یا یک واحد کسب و کار مورد نیاز است. ارزیابی آسیب پذیری و آزمایش‌های نفوذ بخشی از این فرایند در نظر گرفته شده که در فصل ۶ تحت پوشش قرار می‌گیرد. اگر یک کنترل امنیتی اجرا شود که یک هدف امنیتی را برآورده نکند، این کنترل امنیتی بی اثر است. پس از ارزیابی انجام شده، متخصصان امنیت باید از نتایج ارزیابی برای تعیین اینکه کدام کنترل امنیتی دارای نقاط ضعف و یا نقص است استفاده کند. سپس متخصصان امنیت باید برای رفع نواقص و نقاط ضعف تلاش کنند.

کنترل‌های امنیتی باید کنترل شود تا تضمین شود که آنها همیشه به روشی که پیش بینی می‌شود عمل می‌کنند. به عنوان بخشی از این نظارت، متخصصین امنیت باید تمام logها را بررسی کنند. علاوه بر این، گزارش عملکرد باید اجرا شود و با مقیاس‌های عملکردی برای تمام دستگاه‌های امنیتی و کنترل‌ها مقایسه شود. این امر به متخصصان امنیت اجازه می‌دهد تا برخی از مسائل را پیش بینی کرده و آنها را قبل از مواقع بحرانی حل کنند. اندازه گیری‌های عملکردی که باید انجام شود باید با گذشت زمان حفظ شود. اگر رخدادها یا تغییرات مهمی رخ داده باشد، نیاز به خط مبنای جدید لازم می‌باشد. به عنوان مثال، اگر ۲۰۰ کاربر جدید را اضافه کنید که به تأیید اعتبار یا احراز هویت نیاز دارند، باید مقدمات جدید احراز هویت ثبت شود تا تضمین شود که احراز هویت به موقع ممکن است انجام شود. علاوه بر این، اگر شما یک تنظیمات احراز هویت را تغییر دهید، مانند اجرای یک سیاست قفل حساب، شما باید تأثیری را که تنظیمات بر عملکرد و امنیت دارد، نظارت کنید.

گزارش و بهبود مستمر Reporting and Continuous Improvement

متخصصان امنیت هرگز نمی‌توانند فقط بنشینند، استراحت کنند و از آن لذت ببرند. نیازهای امنیتی همیشه در حال تغییر هستند، زیرا "افراد بد" همیشه وجود دارند. بنابراین ضروری است

که متخصصان امنیت به طور مداوم برای بهبود امنیت سازمان خود تلاش کنند. با توجه به این امر، نیاز به بهبود کیفیت کنترل‌های امنیتی در حال اجرا است. بهبود کیفیت معمولاً از یک مدل با کیفیت چهار مرحله‌ای استفاده می‌کند که به عنوان چرخه برنامه - اجرا - بررسی - پیاده سازی Plan-Do-Check-Act شناخته می‌شود. این مراحل در این چرخه هستند:

- ۱- برنامه Plan: شناسایی یک منطقه برای بهبود و ایجاد یک برنامه رسمی برای پیاده سازی آن.
 - ۲- اجرا Do: برنامه را در مقیاس کوچک اجرا کنید.
 - ۳- بررسی Check: نتایج حاصل از اجرای تجزیه و تحلیل را بررسی کرده تا مشخص شود آیا تغییراتی ایجاد شده است.
 - ۴- پیاده سازی Act: اگر پیاده سازی تغییر مثبتی ایجاد کرد، در مقیاس وسیع تری اجرا می‌شود و به طور مداوم نتایج تجزیه و تحلیل شود.
- سایر دستورالعمل‌های مشابه عبارتند از: شش سیگما، لین، مدیریت کیفیت جامع. مهم نیست که سازمان‌ها از کدام یک استفاده می‌کنند، نتیجه باید یک چرخه بهبود مستمر سازمان باشد.

چارچوب‌های ریسک Risk Frameworks

چارچوب‌های ریسک می‌تواند به عنوان راهنمایی برای هر سازمان که در تجزیه و تحلیل ریسک و مدیریت فرایند دخیل است، باشد. سازمانها باید از این چارچوب‌ها به عنوان راهنما استفاده کنند، اما باید به راحتی هر گونه برنامه‌ها و رویه‌هایی را به تناسب نیازهایشان پیاده سازی کنند، را سفارش دهند. چارچوب اصلی که متخصصان امنیت برای امتحان CISSP باید درک کنند، در ابتدای این فصل، در زیر بخش "چارچوب‌های کنترل" بخش "اصول حاکمیت امنیتی" مورد بحث قرار گرفت.

مدل سازی تهدید Threat Modeling

در ابتدای این فصل، در بخش «مفهوم مدیریت ریسک»، آسیب پذیری، تهدید، عوامل تهدید و سایر مفاهیم را تعریف کردیم. مدل سازی تهدید به یک سازمان امکان می‌دهد تا از یک رویکرد ساختار یافته برای امنیت استفاده کند و با تهدیدهای بزرگی که بیشترین تأثیر بالقوه را برای

سازمان به همراه دارد مقابله کند. از مدل سازی تهدید برای شناسایی و رتبه بندی تهدیدهایی که به احتمال زیاد بر سازمان تأثیر می گذارند استفاده می شود.

مدل سازی تهدید را می توان با استفاده از سه دیدگاه مختلف انجام داد:

- مدل سازی تهدید کاربرد محور Application-centric threat modeling: این دیدگاه شامل استفاده از اپلیکیشن نمودارهای معماری برای تجزیه و تحلیل تهدیدات می باشد.
 - مدل سازی تهدید دارایی محور Asset-Centric Threat Modeling: این دیدگاه شامل شناسایی دارایی های یک سازمان و طبقه بندی آنها با توجه به حساسیت داده ها و ارزش ذاتی آنها برای یک مهاجم احتمالی (بالقوه) برای تعیین اولویت بندی سطوح ریسک است. این روش از درختان حمله، گراف های حمله یا نمایش الگوها برای تعیین چگونگی حمله به یک دارایی استفاده می کند.
 - مدل سازی تهدیدات مهاجم محور Attacker-Centric Threat Modeling: این دیدگاه شامل پروفایل، ویژگی ها و انگیزه یک مهاجم برای سوء استفاده از آسیب پذیری ها می باشد. سپس از پروفایل های مهاجم برای درک نوع مهاجمی استفاده می شود که به احتمال زیاد می تواند انواع خاصی از سوء استفاده ها را انجام دهد و بر این اساس یک استراتژی کاهش را اجرا کند. اغلب از نمودارهای درختی استفاده می شود.
- مهم نیست از کدام روش مدل سازی تهدید استفاده شود، مراحل اساسی در فرآیند مدل سازی تهدید به شرح زیر است:

- ۱- شناسایی دارایی ها
- ۲- شناسایی عوامل تهدید و حملات احتمالی.
- ۳- تحقیق در مورد اقدامات متقابل موجود در سازمان.
- ۴- شناسایی هر گونه آسیب پذیری که می تواند مورد سوء استفاده قرار گیرد.
- ۵- اولویت بندی ریسک های شناسایی شده.
- ۶- شناسایی اقدامات متقابل برای کاهش ریسک سازمان.

شناسایی تهدیدات Identifying Threats

شناسایی تهدیدات و بازیگران تهدید به عنوان بخشی از مدل سازی تهدید تفاوت چندانی همانطور که در ابتدای این فصل مورد بحث قرار گرفت با شناسایی تهدیدات و آسیب پذیریها ندارد، در بخش "ارزیابی ریسک".

با این وجود، هنگام انجام مدل سازی تهدید، ممکن است تصمیم گرفته شود لیست کاملی از بازیگران تهدید برای کمک به توسعه سناریو تهیه شود. متخصصان امنیت باید تمام تهدیدات را شناسایی کرده تا همه بازیگران که تهدیدی جدی برای این سازمان می‌باشند، تجزیه و تحلیل شوند. نمونه هایی از بازیگران تهدید شامل بازیگران داخلی و خارجی مانند موارد زیر است:

بازیگران داخلی

- کارمند بی پروا Reckless employee
- کارمند بدون آموزش Untrained employee
- شریک Partner
- کارمند ناراضی Disgruntled employee
- جاسوسی داخلی Internal spy
- جاسوسی دولتی Government spy
- فروشندگان Vendor
- دزد Thief

بازیگران خارجی External actors

- هرج و مرج طلب Anarchist
- رقیب Competitor
- مقام دولتی فاسد Corrupt government official
- شخصی که وظیفه داده کاوی دارد Data miner
- جنگجوی سایبری دولتی Government cyber warrior
- فرد غیر منطقی Irrational individual
- مخالف قانونی Legal adversary
- عضو دسته جنایتکاران Mobster
- فعال Activist
- تروریست Terrorist
- خرابکار Vandal

این بازیگران را می توان به دو دسته تقسیم کرد:

۱- غیر خصمانه یا Non-Hostile ۲- خصمانه یا Hostile. از بازیگران ذکر شده در بالا، معمولاً سه بازیگر غیر خصمانه هستند: کارمند بی پروا، کارمند بدون آموزش و شریک. تمام بازیگران دیگر خصمانه می باشند.

یک سازمان باید هر یک از این بازیگران تهدید را مطابق معیارهای تعیین شده تجزیه و تحلیل کند. این سازمان باید هر یک از بازیگران تهدید را رتبه بندی کند تا بتواند تعیین کند کدام یک از آنها باید تجزیه و تحلیل شوند. نمونه هایی از معیارهای متداول که استفاده می شود شامل موارد زیر است:

- سطح مهارت Skill level : هیچ، حداقل، عملیاتی، متخصص
 - منابع Resources : فرد، تیم، سازمان، دولت
 - دید Visibility: آشکار، راز و پوشش، مخفی، اهمیت ندادن
 - هدف Objective : کپی کردن، نابود کردن، آسیب رسیدن، گرفتن، مراقبت نکردن
 - نتیجه Outcome : کسب / سرقت، مزیت کسب و کار، آسیب، شرمندگی، مزیت فنی
- بر اساس این معیارها، سازمان باید تعیین کند کدام یک از بازیگران را می خواهد تجزیه و تحلیل کند. به عنوان مثال، سازمان ممکن است تصمیم بگیرد که تمام بازیگران خصمانه را که دارای مهارت و مهارت سازمانی و یا دولتی هستند، تحلیل کند. سپس لیست جمع آوری می شود تا فقط بازیگران تهدید کننده متناسب با همه این معیارها باشند.
- در مرحله بعد، سازمان باید تعیین کند که واقعاً از چه چیزی محافظت می کند. اغلب این تعیین با استفاده از نوعی تجزیه و تحلیل تأثیر کسب و کار انجام می شود. پس از مشخص شدن دارایی های حیاتی، سازمان باید با استفاده از مقادیر هدف و پیامد تجزیه و تحلیل بازیگران تهدید و ارزش دارایی و اطلاعات مربوط به تأثیر کسب و کار، سناریوهایی را که می تواند تأثیر فاجعه بار در سازمان داشته باشد، انتخاب کند.

حمله های بالقوه Potential Attacks

برای شناسایی حملات بالقوه که ممکن است رخ دهد، سازمان باید سناریوهایی را ایجاد کند که بتوان آنها را کاملاً تجزیه و تحلیل کرد. به عنوان مثال، یک سازمان ممکن است تصمیم به تجزیه و تحلیل وضعیتی بگیرد که در آن یک گروه هکتیویسمی (گروهی که با استفاده از رایانه و شبکه های رایانه ای در جهت اعتراض و مقاصد سیاسی فعالیت می کنند) حملات بلند مدت DoS

را انجام می‌دهند و باعث خسارت‌های پایدار شده که باعث آسیب به اعتبار سازمان می‌شود. سپس هر سناریو باید تعیین ریسک شود.

هنگامی که تمام سناریوها تعیین می‌شوند، سازمان باید یک درخت حمله برای هر حمله بالقوه ایجاد کند. درخت حمله باید شامل تمام مراحل و یا شرایطی باشد که باید برای حمله انجام شود. پس از آن سازمان باید کنترل‌های امنیتی را بر روی درخت‌های حمله انجام دهد. برای تعیین اینکه چه کنترل‌های امنیتی می‌تواند مورد استفاده قرار گیرد، سازمان باید به استانداردهای صنعتی توجه کند، از جمله NIST SP 800-53 که قبلاً در این فصل بحث شده است. در نهایت، کنترل‌ها باید به درخت حمله بازگردانده شوند تا تضمین شود که کنترل‌ها در سطوح مختلف حمله انجام می‌شود.

فرایندها و فن آوری‌های ترمیم Remediation Technologies and Processes

متخصصان امنیت باید به عنوان بخشی از هر الگوی تهدید آمیز آماده شوند تا تهدیدها را مورد تجزیه و تحلیل قرار دهند، کنترل‌های امنیتی موجود را بررسی کرده و در مورد فرایندها و فن آوری‌های ترمیم توصیه کنند. از فن آوری‌های ترمیم فقط می‌توان برای محافظت بیشتر در برابر تهدید شناسایی شده استفاده کرد. با این حال، فرآیندهای ترمیم در حال توسعه، متخصصان امنیت یا ممیزها نیاز به تجزیه و تحلیل فرآیندهای داخلی، شناسایی نقاط ضعف در فرایندهای فعلی و تجدید نظر در فرآیندهای فعلی یا توسعه موارد جدیدی دارند که بهتر در برابر تهدیدهای شناسایی شده محافظت می‌کنند. به عنوان مثال، پس از تجزیه و تحلیل فرایند صدور گذرواژه جدید، یک متخصص امنیت ممکن است متوجه شود که یک مهاجم بتواند گذرواژه کاربر داخلی را بازنشانی یا ریست کند. در این حال امکان دارد یک متخصص امنیت فرایندی را ایجاد کند که به موجب آن کاربران باید قبل از بازنشانی گذرواژه، برخی از عوامل شناسایی را ارائه دهند.

ریسک‌های امنیتی در اکتساب Security Risks in Acquisitions

پیش از این ما در مورد اکتساب شرکت صحبت کردیم. در این بخش ریسک‌های امنیتی در دستیابی به سخت افزار، نرم افزار و خدمات مورد بحث قرار می‌گیرد. بخشی از این بحث، حاکمیت شخص ثالث، حداقل الزامات امنیتی و حداقل نیازهای سطح خدمات را شامل می‌شود.

سخت افزار، نرم افزار، خدمات Hardware, Software, Services

سازمانها به عنوان بخشی از کسب و کار روزانه سخت افزار، نرم افزار و خدمات را بدست می آورند. زنجیره تامین اموال ملموس برای هر سازمان ضروری است. یک سازمان باید تمام ریسک های مربوط به زنجیره تامین را درک کند و یک برنامه مدیریت ریسک که متناسب با آن است را، اجرا کند. اما زنجیره تامین فقط شامل اموال ملموس، مانند سخت افزار نیست. همچنین می تواند شامل اطلاعات، نرم افزار و خدمات نیز باشد.

برخی از این تمهیدات دارای سازوکارهای امنیتی داخلی هستند. با این حال، این سازوکارهای امنیتی برای محافظت کامل از مالکیت، کافی نیستند. علاوه بر این، هر مکانیسم امنیتی باید به طور مرتب به روز شود و احتمالاً با مکانیسم های امنیتی اخیر و قوی تر نیز جایگزین شود. متخصصان امنیت باید در هر گونه سخت افزار، نرم افزار و خدمات درگیر شوند تا تضمین شود که امنیت بخش مهمی از تصمیم است. اگر هیچ مدافع امنیتی، بخشی از فرآیند اکتساب نباشد، معمولاً تمهیداتی حاصل می شود که سازمان را در معرض ریسک قرار می دهد. به عنوان بخشی از ملاحظات مربوط به امنیت، متخصصان امنیت باید مقدمات اولیه برای اکتساب را آموزش دهند، پرسنل را آموزش داده تا تغییرات امنیتی با تدارکات جدید سازگار شوند، از اصطلاحات و تعاریف امنیتی مشترک برای اکتساب استفاده کرده و یک استراتژی تهیه کنند تا تضمین شود که از حداقل اکتساب استفاده شده است.

شخص ثالث Third Party

برای بسیاری از سازمان ها، شخص ثالث تضمین می کند که یک سازمان مطابق با استانداردها و مقررات مربوط به صنعت یا دولت است. این شخص ثالث تجزیه و تحلیل عملکردهای سازمانی و هر حوزه دیگری را که توسط سازمان صدور گواهینامه یا تنظیم کننده دیجیتالی شده است انجام می دهد. شخص ثالث تمام نتایج حاصل از یافته های خود را به سازمان صدور گواهینامه یا تنظیم کننده گزارش می دهد. قرارداد با شخص ثالث باید تصریح کند که هر گونه یافته یا نتایج فقط باید با سازمان مورد بررسی و با سازمان تنظیم مقررات، ارتباط برقرار کند. یک عضو مدیریت سطح بالا معمولاً این فرایند را مدیریت می کند به طوری که شخص ثالث به موارد مورد نیاز دسترسی پیدا کند. به عنوان بخشی از این تجزیه و تحلیل، شخص ثالث ممکن است نیاز به انجام ارزیابی در محل، مبادله اسناد یا بررسی فرایند / سیاست داشته باشد.

ارزیابی در محل Onsite Assessment

ارزیابی در محل شامل یک تیم از شخص ثالث است. این تیم نیاز به دسترسی به تمامی جنبه‌های سازمان را تحت قوانین دارد. این ارزیابی ممکن است شامل مشاهده انجام وظایف روزانه کارمندان، بررسی سوابق، بررسی اسناد و سایر فعالیت‌ها باشد. مدیریت باید یکی از اعضای مدیریتی را که تیم می‌تواند از طریق وی درخواست‌های رسمی دهد، تفویض کند.

بررسی / تبادل اسناد Document Exchange/Review

یک بررسی / تبادل اسناد شامل انتقال مجموعه‌ای از اسناد به شخص ثالث است. روند مورد استفاده برای مبادله اسناد باید در هر دو طرف مبادله امن باشد.

بررسی سیاست / فرآیند Process/Policy Review

بر یک فرایند یا سیاست واحد درون سازمان متمرکز است و تضمین می‌کند که روند یا سیاست از مقررات پیروی می‌کند.

سایر موارد مربوط به حاکمیت شخص ثالث Other Third-Party Governance Issues

حاکمیت شخص ثالث ممکن است در شرایطی اعمال شود که سازمان از اشخاص ثالث برای ارائه خدمات به یک سازمان استفاده کند. یک مثال از این موارد، استفاده از یک راه حل ابری عمومی مانند زیرساخت به عنوان سرویس Infrastructure as a Service (IaaS) پلت فرم به عنوان یک سرویس Platform as a Service (PaaS)، یا نرم افزار به عنوان یک سرویس Software as a Service (SaaS) است.

هنگام استفاده از شخص ثالث مثل این، یک متخصص امنیت باید تضمین کند که سازمان SLA مناسب را بدست می‌آورد. علاوه بر این، متخصص امنیت باید به سازمان اطمینان دهد که شخص ثالث در تمام جنبه‌هایی که در سازمان تأثیر می‌گذارد دقت لازم را انجام می‌دهد. این اطمینان فقط با بازرسی، بررسی و ارزیابی ارائه دهنده شخص ثالث قابل ارائه است. سرانجام، یک متخصص امنیت باید از کشورها یا اشخاصی که در سیستم‌های شخص ثالث صلاحیت دارند آگاهی داشته باشد.

حداقل الزامات امنیتی Minimum Security Requirements

متخصصان امنیت باید حداقل الزامات امنیتی را برای هرگونه دستاوردی که توسط سازمان انجام می شود تعریف کنند. برای رایانه ها، این امر می تواند به بهترین وجه با استفاده از کنترل دسترسی به شبکه NAC اعمال شود، که سیاست هایی را تعریف می کند که چگونگی اطمینان از دسترسی به گره های (نودها) شبکه را توسط دستگاه ها در هنگام تلاش برای دسترسی به شبکه توصیف می کند. اگر دستگاه سعی در اتصال دارد و حداقل شرایط را برآورده نکند، دسترسی ممنوع است یا برای محافظت از شبکه سازمانی داخلی، در یک شبکه قرنطینه قرار می گیرد.

برای هر نوع اکتساب مختلف، ممکن است لازم باشد که سیاست های امنیتی جداگانه تعریف شود. به عنوان مثال، دستگاه های تلفن همراه که مورد استفاده قرار نگرفته اند ممکن است نیاز به قفل شدن در فایل یا کابینت امن داشته باشند. کلیدهای وسایل نقلیه شرکت نباید خارج از محل نگهداری شوند، که بتوان راحت به آن دسترسی داشت. رایانه هایی که در یک منطقه شلوغ قرار دارند ممکن است نیاز به مکانیسم خاصی داشته که در آنجا دستگاه به میز قفل شود. کنترل های امنیتی دقیقاً به اندازه انواع اکتساب تغییر می کنند.

حداقل الزامات سطح سرویس Minimum Service-Level Requirements

SLAها توافق در مورد توانایی یک سیستم پشتیبانی برای پاسخگویی به مشکلات در یک بازه زمانی مشخص در عین ارائه سطح خدمات توافق شده است. این توافقات می توانند بین بخش ها با ارائه دهندگان خدمات داخلی یا خارجی باشند. توافق با سرعتی که در آن به مشکلات مختلفی رسیدگی می کند، پیش بینی پاسخ به مشکلات را می تواند انجام دهد، و در نهایت از نگهداری دسترسی به منابع پشتیبانی می کند. در زیر مواردی که ممکن است در SLA شامل شود:

- از دست دادن اتصال به سرور DNS باید طی یک دوره ۳۰ دقیقه ای بازسازی شود.
 - از دست دادن اتصال به خدمات اینترنت باید در یک دوره ۵ ساعته بازسازی شود.
 - از دست دادن اتصال یک ماشین میزبان باید در یک دوره ۸ ساعته بازسازی شود.
- قبل از نوشتن و امضای SLA، سازمان ها باید در مورد الزامات سطح خدمات مذاکره کنند. اگر سازمان نیازی به دقت مستند نداشته باشد، نمیتواند مطمئن باشد که SLA فروشنده، نیازهایش را برآورده می کند. الزامات مورد نیاز برای مستند سازی عبارتند از:

- شرح خدمات Description of service

- ساعات‌های سرویس مورد نیاز Hours of service needed
 - فرایند وقفه سرویس Service interruption process
 - الزامات دسترسی Availability requirements
 - الزامات تعمیر و نگهداری و خرابی مجاز Maintenance requirements and allowed downtime
 - حجم کاری مورد انتظار Workload expected
 - عملکرد مورد انتظار Performance expected
- متخصصان امنیت هنگام دستیابی به خدمات شخص ثالث، باید با مدیران واحد کسب و کار همکاری کنند تا تضمین شود که نیازهای سطح خدمات مستند شده است.

آموزش امنیت، پرورش و آگاهی Security Education, Training, and Awareness

پرورش آگاهی امنیت، پرورش امنیت و آموزش امنیت Awareness Training, Security Education, Security Training سه اصطلاح است که اغلب به جای هم استفاده می‌شوند اما در واقع سه چیز متفاوت است. پرورش آگاهی، این واقعیت را تقویت می‌کند که با استفاده از اقدامات امنیتی، منابع با ارزش باید محافظت شوند.

سطح مورد نیاز Levels Required

پرورش امنیتی Security Training مهارت‌های حرفه‌ای را آموزش می‌دهد تا آنها بتوانند به طور ایمن شغل خود را انجام دهند. پرورش آگاهی و پرورش امنیت Awareness Training and Security Awareness Training، معمولاً به عنوان پرورش آگاهی امنیت ترکیب شده اند که آگاهی کاربر را از امنیت افزایش می‌دهد و اطمینان می‌دهد که کاربران می‌توانند برای اقدامات خود پاسخگو باشند. آموزش امنیت Security Education مستقل است و برای متخصصان امنیت که به تخصص امنیتی نیاز دارند تا به عنوان کارشناسان داخلی برای مدیریت برنامه‌های امنیتی فعالیت کنند.

- Awareness Training در واقع به معنی امنیت چیست WHAT
- Security Training در واقع به معنی امنیت چگونه است HOW
- Security Education در واقع به معنی چرا امنیت WHY

پرورش آگاهی امنیتی باید براساس مخاطب تدوین شود. علاوه بر این، مربیان باید فرهنگ سازمانی و چگونگی تأثیر آن بر امنیت را درک کنند. مخاطبان مورد نظر شما در هنگام طراحی پرورش باید برای مدیریت سطح بالا، مدیریت میانی، پرسنل فنی و کارمندان تنظیم شده باشد. برای مدیریت سطح بالا، پرورش آگاهی امنیتی باید درک روشنی از ریسک ها و تهدیدات بالقوه، تأثیرات مسائل امنیتی بر شهرت سازمان و وضعیت مالی و هرگونه قوانین و مقررات مربوط به برنامه امنیتی سازمان داشته باشد. پرورش مدیریت میانی باید در مورد سیاست ها، استانداردها، پایه ها، دستورالعمل ها و رویه ها بویژه در مورد چگونگی اجرای این اجزا در بخش های مختلف، بحث شود. همچنین مدیریت میانی باید مسئولیت های خود را در رابطه با امنیت درک کند. کادر فنی باید در مورد پیکربندی و نگهداری کنترل های امنیتی، از جمله نحوه تشخیص حمله زمانی که رخ می دهد، پرورش فنی داشته باشند. علاوه بر این، کادر فنی باید تشویق شوند تا گواهینامه های صنعت و درجه تحصیلات عالی را دنبال کنند. کارکنان عادی باید وظایف خود را در رابطه با امنیت درک کنند تا کارهای روزانه خود را به شیوه ای مطمئن انجام دهند. برای کارکنان عادی، ارائه مثال های دنیای واقعی برای تأکید بر روال های امنیتی مناسب موثر است. پرسنل باید یک سند را امضا کنند که نشان می دهد که آموزش ها را کامل کرده و تمام موضوعات را درک کرده اند. اگر چه آموزش ابتدایی باید در هنگام استخدام پرسنل صورت گیرد، آموزش آگاهی امنیتی باید یک فرآیند مداوم در نظر گرفته شود و جلسات آموزشی آینده حداقل به صورت سالیانه برگزار شود.

بررسی دوره ای Periodic Review

مسائل امنیتی و تهدیدات جدید همیشه در جامعه امروز به چشم می خورد. در نتیجه، متخصصان امنیت باید تمام آموزش های مربوط به آگاهی امنیتی را بررسی کنند و تضمین شود که آنها برای رسیدگی به مسائل و تهدیدات امنیتی جدید به روز می باشند. این بررسی باید برنامه ریزی شده و در فواصل منظم رخ دهد.

فصل ۲

امنیت دارایی
(Asset Security)

این فصل موضوعات زیر را پوشش می دهد:

❖ مفاهیم امنیت دارایی Asset Security Concepts: مفاهیم مورد بحث شامل سیاست های داده ها، نقش ها و مسئولیت ها، کیفیت داده ها و اسناد داده ها و سازمان است.

❖ طبقه بندی اطلاعات و دارایی ها Classify Information and Assets: موضوعات طبقه بندی مورد بحث شامل حساسیت و بحران، طبقه بندی مشاغل تجاری، طبقه بندی نظامی و دولتی، چرخه عمر اطلاعات، نگهداری پایگاه داده و ممیزی داده ها.

❖ مالکیت دارایی Asset Ownership: افراد مورد بحث شامل صاحبان داده ها، صاحبان سیستم، صاحبان کسب و کار / مأموریت و مدیریت دارایی می باشند.

❖ دارایی خصوصی Asset Privacy: ترکیبات شامل پردازشگرهای داده، ذخیره سازی و بایگانی داده ها، امنیت داده ها، نگهداری داده ها و محدودیت جمع آوری است.

❖ نگهداری دارایی Asset Retention: مفاهیم حفظ شامل رسانه، سخت افزار و پرسنل است.

❖ کنترل های داده های امنیتی Data Security Controls: موضوعات شامل داده های باقی مانده، داده ها در حال انتقال، امنیت داده ها، دسترسی به داده ها و به اشتراک گذاری، خط مبنا، دامنه و اتصالات، بقیه داده ها، انتخاب استانداردها و رمزنگاری.

❖ ملزومات اداره کردن دارایی Asset Handling Requirements: موضوعات شامل نشانه گذاری، برچسب گذاری، ذخیره سازی، و تخریب است.

دارایی ها هر موجودیتی که برای سازمان باارزش هستند و شامل دارایی های ملموس و غیرملموس می باشند. همانطور که در فصل ۱ "امنیت و مدیریت ریسک" ذکر شده است، دارایی های ملموس شامل رایانه، تاسیسات، منابع و پرسنل می باشد. دارایی های نا ملموس شامل مالکیت معنوی، داده ها و شهرت سازمانی هستند. تمام دارایی های یک سازمان باید محافظت شود تا تضمینی برای موفقیت سازمان در آینده باشد. در حالی که تضمین برخی دارایی ها به راحتی قفل کردن آنها در صندوق امانات است، دارایی های دیگر به اقدامات امنیتی پیشرفته تری نیاز دارند. یک متخصص امنیت باید با تمام جنبه های امنیت دارایی مواجه شود. مهمترین عامل در تعیین کنترل استفاده شده برای اطمینان از امنیت دارایی، ارزش آن دارایی است. در حالی که برخی از دارایی های موجود در سازمان ممکن است مهم تر قلمداد شوند زیرا ارزش بیشتری دارند، اما باید

مطمئن شد که هیچ دارایی فراموش نمی‌شود. این فصل کلیه جنبه‌های امنیت دارایی را که شما به عنوان یک متخصص امنیت فناوری اطلاعات باید درک کنید را در بر می‌گیرد.

مفاهیم امنیت دارایی Asset Security Concepts

مفاهیم امنیت دارایی عبارتند از:

- ❖ سیاست داده‌ها Data policy
- ❖ نقش‌ها و مسئولیت‌ها Roles and responsibilities
- ❖ کیفیت داده Data quality
- ❖ مستندسازی و سازماندهی داده‌ها Data documentation and organization

سیاست داده‌ها Data policy

به عنوان یک متخصص امنیت، باید اطمینان حاصل شود که سازمان سیاست‌های داده‌ای را اجرا می‌کند و اهداف بلند مدت را برای مدیریت داده تعیین می‌کند. به احتمال زیاد لازم است برای هر واحد کسب و کار منحصر به فرد در سازمان، سیاست داده‌ای خود را بر اساس سیاست کلی داده سازمان تعریف کند. در سیاست داده‌ها، وظایف و مسئولیت‌های فردی باید تعریف شود تا تضمین شود که پرسنل وظایف شغلی خود را که مربوط به سیاست داده است، درک می‌کنند. هنگامی که سیاست کلی داده‌ها ایجاد می‌شود، شیوه‌های مدیریت داده‌ها و مراحل باید مستند شوند تا تضمین شود که وظایف روزانه مربوط به داده‌ها تکمیل شده است. علاوه بر این، برای تضمین کیفیت داده‌ها باید روشهای مناسب تضمین کیفیت و کنترل کیفیت اعمال شود. برای اطمینان از بازیابی داده‌ها باید مراحل ذخیره سازی و تهیه نسخه پشتیبان تعریف شود. به عنوان بخشی از سیاست داده، هر پایگاه داده‌ای که در یک سازمان اجرا می‌شود، باید با دقت بر اساس نیاز کاربر و نوع داده ذخیره شود. تمام پایگاه‌های داده باید با سیاست‌های داده‌ای که اجرا می‌شوند، مطابقت داشته باشند.

قبل از ایجاد یک سیاست داده، باید چندین مسئله را که می‌تواند بر آن تاثیر بگذارد، در نظر گرفت. این مسائل شامل هزینه، مسئولیت، الزامات قانونی و مقررات، حریم خصوصی، حساسیت و مالکیت است.

هزینه هر مکانیزم مدیریت داده معمولاً مورد توجه اصلی هر سازمان است. اغلب سازمانها یک سیاست داده را پیاده سازی نمی‌کنند زیرا فکر می‌کنند که اجازه به ذخیره داده‌ها به هر نحوی

در هر واحد کسب و کار یا کاربر مورد نظر آسان تر است. با این حال، اگر یک سازمان سیاست‌ها و خط مشی‌ها و روش‌های رسمی داده‌ها را قبول نکند، به دلیل روش‌های ذخیره سازی مختلف مورد استفاده، باعث مشکلات امنیتی داده‌ها می‌شود. به عنوان مثال، فرض کنید یک گروه تحقیقاتی سازمان تصمیم به پیاده سازی یک پایگاه داده Microsoft SQL Server برای ذخیره تمام داده‌های تحقیقاتی داشته باشند، اما سازمان هیچ سیاست داده‌ای نداشته باشد. اگر پایگاه داده بدون درک کاملی از انواع داده‌های ذخیره شده و نیاز کاربر انجام شود، ممکن است بخش تحقیقات به یک پایگاه داده ختم شود که امکان حرکت و مدیریت آن دشوار است.

مسئولیت (Liability) شامل حمایت از سازمان در برابر مسائل حقوقی است. مسئولیت مستقیماً تحت تأثیر الزامات قانونی و نظارتی است که برای سازمان اعمال می‌شود. مسائل داده‌ای که می‌توانند باعث ایجاد مسئولیت شوند شامل سوءاستفاده از داده‌ها، عدم صحت داده‌ها، نقض داده‌ها و از بین رفتن داده‌ها است.

حریم خصوصی داده‌ها به عنوان بخشی از تجزیه و تحلیل داده‌ها تعیین می‌شود. طبقه بندی داده‌ها باید بر اساس ارزش داده‌ها در سازمان تعیین شود. هنگامی که طبقه بندی داده‌ها تعیین می‌شود، کنترل داده‌ها باید اجرا شود تا تضمین شود که کنترل‌های امنیتی مناسب براساس طبقه بندی داده‌ها اجرا می‌شوند. قوانین و مقررات حفظ حریم خصوصی باید در نظر گرفته شود.

داده‌های حساس هر داده‌ای است که در صورت انتشار به عموم یا بدست آوردن مهاجمان، می‌تواند بر سازمان یا فرد تأثیر منفی بگذارد. هنگام تعیین حساسیت، باید نوع تهدیداتی را که ممکن است رخ دهد، آسیب پذیری داده‌ها و نوع داده‌ها را درک کرد. به عنوان مثال، شماره‌های امنیت اجتماعی حساس تر از اطلاعات آدرس فیزیکی هستند.

مالکیت داده‌ها مسئله نهایی می‌باشد که باید در بخشی از طراحی سیاست داده‌ها در نظر گرفته شود. این امر بسیار مهم است اگر سازمان‌های متعدد اطلاعات خود را در یک پایگاه داده ذخیره کنند. یک سازمان ممکن است کنترل‌های امنیتی کاملاً متفاوت را برای حفاظت از داده‌های خود دنبال کند.

فهم مالکیت قانونی داده‌ها برای اطمینان از اینکه یک سیاست داده را طراحی کرده که نیازهای مختلف صاحبان (مالکان) داده‌های مختلف را در نظر گرفته است، مهم است. در حالی که بیشتر مورد توجه سازمان‌های چندگانه است، اما می‌تواند در واحدهای کسب و کار مختلف در یک سازمان نیز مشکلی ایجاد کند. به عنوان مثال، صاحبان مختلف داده‌های دپارتمان منابع انسانی نیازهای متفاوتی نسبت به داده‌های دپارتمان تحقیق دارند.

نقش‌ها و مسئولیت‌ها Roles and Responsibilities

نقش‌هایی که معمولاً به امنیت دارایی مرتبط هستند، صاحبان داده‌ها و نگهبانان داده‌ها هستند. صاحبان داده‌ها، پرسنلی هستند که در واقع یک مجموعه داده خاص را دارند. این دارندگان داده میزان دستیابی هر کاربر به داده‌های خود را تعیین می‌کنند. نگهبانان داده‌ها پرسنلی هستند که در واقع دسترسی به مجموعه‌ای از داده‌ها را مدیریت می‌کنند. در حالی که صاحبان داده سطح دسترسی داده را تعیین می‌کنند، نگهبانان داده کنترل‌های مناسب را برای اعطا یا رد دسترسی کاربر بر اساس تایید صاحب داده (مالک داده) انجام می‌دهند.

صاحب داده (مالک داده) Data Owner

صاحبان داده‌ها (مالکان داده) باید درک کنند که کدام داده‌ها مسئول هستند و چه زمانی داده‌ها باید منتشر شوند. آنها همچنین باید ارزش داده‌ها را برای سازمان تعیین کنند و بر آن تاثیر بگذارند. مالک داده باید درک کند که چه چیزی برای بازگرداندن یا جایگزینی داده‌ها و همچنین هزینه‌هایی که در طی این فرآیند رخ می‌دهد را وارد کند. در نهایت، مالکان داده باید درک کنند که داده‌ها نادرست است یا دیگر سازمان نیازی به آنها ندارد. در اغلب موارد، هر واحد کسب و کار در یک سازمان یک مالک داده تعیین می‌کند که چه کسی مسئول است که مجوز به میزان سطح مناسب برای دسترسی به داده‌ها، بدهد. صاحبان داده‌ها باید هر گونه حقوق مالکیت معنوی و مسائل مربوط به حق نسخه برداری را برای داده‌ها درک کنند. صاحبان داده‌ها وظیفه دارند تضمین کنند که در صورت دسترسی شخص ثالث به داده‌ها، توافق مناسب وجود دارد.

نگهبان داده Data Custodian

نگهبانان داده باید سطوح دسترسی به داده‌ها را که می‌توانند به کاربران داده شوند، درک کنند. نگهبانان داده با صاحبان داده همکاری می‌کنند تا سطح دسترسی مورد نیاز را تعیین کنند. این یک نمونه عالی از کنترل‌های تقسیم شده است. با داشتن نقش‌های جداگانه‌ای مانند صاحبان داده‌ها و نگهبانان داده، یک سازمان می‌تواند تضمین کند که هیچ نقش واحدی مسئولیت دسترسی به داده‌ها را ندارد.

نگهبانان داده باید خط مشی ها و سیاستها و دستورالعمل های داده را درک کنند. آنها باید ساختار داده ها را در سازمان و سطوح دسترسی داده شده را مستند کنند. آنها همچنین مسئول ذخیره داده، بایگانی و پشتیبان گیری هستند. در نهایت، آنها باید به کیفیت داده توجه داشته باشند و بنابراین باید کنترل های ممیزی مناسب را پیاده سازی کنند.

نگهبانان داده متمرکز رایج هستند. صاحبان داده ها به نگهبانان داده همان اندازه سطح دسترسی کاربران و گروه ها می دهند. نگهبانان داده عملاً لیست کنترل دسترسی (ACL ها) را برای دستگاه ها، پایگاه های داده، پوشه ها و فایل ها پیاده سازی می کنند.

کیفیت داده Data Quality

کیفیت داده ها به عنوان مناسب بودن داده ها برای استفاده تعریف شده است. کیفیت داده ها باید در طول چرخه عمر داده ها، از جمله در سراسر ضبط داده ها، اصلاح داده ها، ذخیره سازی داده ها، توزیع داده ها، استفاده از داده ها و آرشیو داده ها حفظ شود. متخصصان امنیت تضمین کنند که سازمانشان کنترل کیفیت و تضمین کیفیت را به گونه ای تنظیم کرده تا کیفیت داده ها از بین نروند و اختلالی ایجاد نشود.

متخصصان امنیت باید برای مستند سازی استانداردهای داده، فرایندها و رویه ها برای نظارت و کنترل کیفیت داده ها تلاش کنند. علاوه بر این، فرایندهای داخلی باید برای ارزیابی دوره ای کیفیت داده ها طراحی شوند. هنگامی که داده ها در پایگاه های داده ذخیره می شوند، اطمینان از کنترل کیفیت و اطمینان از استفاده از کنترل داده های داخلی در پایگاه داده آسان تر می شود. به عنوان مثال، می توانید یک شماره فیلد را پیکربندی کنید تا فقط اجازه ورود مقادیر ارز خاص را داشته باشد. با انجام این کار، مطمئن شوید که تنها مقادیری که از دو رقم اعشار استفاده می شود می توانند وارد فیلدهای داده شوند. این یک نمونه از اعتبار ورودی است.

آلودگی داده ها هنگام معرفی خطاهای داده رخ می دهد. خطاهای (Error) داده ها می تواند از طریق اجرای مکانیزم های کنترل کیفیت و اطمینان مناسب کاهش یابد. تأیید داده ها، بخش مهمی از فرآیند، ارزیابی کامل و صحیح داده ها و تطابق با استانداردها را ارزیابی می کند. تأیید داده ها می تواند توسط پرسنل انجام شود که مسئولیت ورود داده ها را دارند. اعتبار سنجی داده ها پس از تایید داده ها ارزیابی می شود و داده ها را آزمایش می کند تا تضمین شود که استانداردهای کیفیت داده ها برآورده شده اند. اعتبار سنجی داده ها باید توسط پرسنلی انجام شود که آشنایی بیشتری با داده ها دارند.

سازمان‌ها باید روش‌ها و فرایندهایی را توسعه دهند که دو موضوع داده کلیدی را در پیش رو حفظ کند: پیشگیری از خطا و تصحیح. پیشگیری از خطا هنگام ورود داده‌ها ارائه می‌شود، در حالی که تصحیح خطا معمولاً هنگام تأیید و اعتبار سنجی داده‌ها رخ می‌دهد.

سازماندهی و مستندسازی داده‌ها Data Documentation and Organization

مستندسازی داده‌ها اطمینان می‌دهد که داده‌ها در سطح پایینی درک می‌شوند و می‌توانند به طور مناسب در مجموعه داده‌ها سازماندهی شوند. مجموعه داده‌ها تضمین می‌کند که داده‌ها بصورت رابطه‌ای مرتب شده و ذخیره می‌شوند تا داده‌ها برای چندین منظور استفاده شوند. مجموعه داده‌ها باید نام‌های منحصر به فرد و توصیفی داشته باشند که محتوای آنها را نشان می‌دهد.

با مستندسازی داده‌ها و سازماندهی مجموعه داده‌ها، سازمان‌ها همچنین می‌توانند از حفظ داده‌های تکراری در چندین مکان مطمئن شوند. به عنوان مثال، اداره فروش می‌تواند تمام اطلاعات جمعیت شناختی را برای همه مشتریان ضبط کند. با این حال، اداره حمل و نقل نیز ممکن است به این اطلاعات جمعیتی دسترسی داشته باشد تا مطمئن شود که محصولات به آدرس صحیح ارسال می‌شود. علاوه بر این، بخش حسابداری برای اهداف صورتحساب به اطلاعات جمعیتی مشتری نیاز دارند. نیازی نیست برای هر واحد کسب و کار مجموعه داده‌های جداگانه‌ای برای این اطلاعات وجود داشته باشد.

شناسایی داده‌های آماری مشتری که به وسیله واحدهای کسب و کار متعدد مورد نیاز است، مانع تکثیر تلاش‌ها در بخش‌های کسب و کار می‌شود.

در هر مجموعه داده، هر نوع داده باید مستندسازی شود. در مثال مشتری مجموع داده‌های آماری مشتری، نام، آدرس، و شماره تلفن مشتری جمع آوری می‌شوند. برای هر نوع داده، پارامترهای فرد برای هر نوع داده باید ایجاد شوند. در حالی که آدرس ممکن است ترکیبی از اعداد و حروف مجاز باشد، در یک شماره تلفن فقط باید اعداد مجاز باشد. علاوه بر این، هر نوع داده ممکن است حداکثر طول داشته باشد. در نهایت، مهم است که سندی که از داده‌ها بدست می‌آید، بدان معنی است که باید آن را جمع آوری و وارد کرد. به عنوان مثال، یک سازمان ممکن است تصمیم بگیرد که شماره فکس مورد نیاز نباشد، اما شماره تلفن مورد نیاز است. به خاطر داشته باشید بهتر است که هر یک از این تصمیمات توسط کارکنانی که بیشتر با داده‌ها سر و کار دارند، صورت گیرد.

پس از اتمام تمام مستندات، سازماندهی داده‌ها باید نقشه برداری شوند. این سازماندهی کلیه روابط متقابل بین مجموعه داده‌ها را در بر می‌گیرد. همچنین باید شامل اطلاعاتی باشد که در آن واحدهای کسب و کار، دسترسی به مجموعه داده‌ها یا زیر مجموعه‌های یک مجموعه داده را نیاز دارند.

توجه داشته باشید

داده‌های بزرگ Big data یک اصطلاح برای مجموعه‌های بزرگ یا پیچیده‌ای است که به اندازه‌ای بزرگ یا پیچیده هستند که نمی‌توانند با برنامه‌های پردازش داده‌های سنتی تحلیل شوند. برنامه‌های تخصصی برای کمک به سازمان‌ها با داده‌های بزرگ طراحی شده‌اند. چالش‌های بزرگ داده‌ای که ممکن است با آن روبرو شوند عبارتند از: تجزیه و تحلیل داده‌ها، ضبط داده‌ها، جستجو در داده‌ها، اشتراک گذاری داده‌ها، ذخیره سازی داده‌ها و حفظ حریم خصوصی داده‌ها هستند.

طبقه بندی اطلاعات و دارایی‌ها Classify Information and Assets

داده‌ها باید بر اساس ارزش آن در سازمان و حساسیت به افشای آن طبقه بندی شوند. اختصاص یک مقدار به داده‌ها به یک سازمان امکان می‌دهد منابعی را که باید برای محافظت از داده‌ها مورد استفاده قرار گیرد، تعیین کند. منابع مورد استفاده برای محافظت از داده‌ها عبارتند از منابع پرسنلی، منابع مالی، منابع کنترل دسترسی و غیره. طبقه بندی داده‌ها این امکان را می‌دهد که اقدامات محافظتی مختلفی اعمال شود. طبقه بندی داده‌ها برای همه سیستم‌ها برای حفظ محرمانه بودن، یکپارچگی و دسترسی به داده‌ها یا همان CIA حیاتی است.

پس از طبقه بندی داده‌ها، داده‌ها می‌توانند براساس سطح حفاظت لازم آن تقسیم بندی شوند. سطوح طبقه بندی اطمینان می‌دهد که داده‌ها با مقرون به صرفه ترین روش ممکن اداره و محافظت می‌شوند. یک سازمان باید سطوح طبقه بندی مورد استفاده خود را بر اساس نیازهای سازمان تعیین کند. تعدادی از طبقه بندی‌های اطلاعات کسب و کار تجاری و نظامی و دولتی به صورت رایج مورد استفاده قرار می‌گیرند.

چرخه عمر اطلاعات، که در ادامه در این فصل با جزئیات بیشتر توضیح داده می‌شود، همچنین باید بر اساس طبقه بندی داده‌ها باشد. سازمانها ملزم به حفظ اطلاعات خاص، به ویژه داده‌های مالی، بر اساس قوانین و مقررات محلی، ایالتی یا دولتی هستند.

در این بخش حساسیت و بحران داده ها، طبقه بندی های کسب و کار تجاری، طبقه بندی های نظامی و دولتی، چرخه عمر اطلاعات، نگهداری پایگاه داده ها و ممیزی داده ها مورد بحث قرار می گیرد.

حساسیت و بحران Sensitivity and Criticality

حساسیت Sensitivity سنجشی است که نشان می دهد چگونه داده ها آزادانه می توانند مورد استفاده قرار گیرند. بعضی از داده ها نیاز به مراقبت ویژه و بررسی ویژه دارند، به ویژه هنگام عدم رسیدگی نامناسب می تواند منجر به مجازات، سرقت هویت، ضرر مالی، حمله به حریم خصوصی یا دسترسی غیرمجاز توسط شخص یا افراد زیادی شود. برخی از داده ها همچنین تحت قوانین ایالتی یا قوانین فدرال تنظیم می شوند و در صورت افشاء، نیاز به اطلاع رسانی دارند.

داده ها یک سطح حساسیت دارند بر مبنای اینکه چه کسی باید به آن دسترسی داشته باشد و در صورت افشا به چه میزان آسیب وارد می شود، این تخصیص حساسیت را طبقه بندی داده ها Data classification می نامند.

Criticality معیار سنجش اهمیت داده ها است. داده هایی که حساس در نظر گرفته شده لزوماً به اندازه بحرانی بودن یا همان Criticality حیاتی تلقی نمی شوند. اختصاص سطح بحرانی به یک مجموعه داده خاص، نیاز به در نظر گرفتن پاسخ به چند سوال دارد:

- آیا می توان داده ها را در صورت بروز فاجعه بازیابی کرد؟
- چه مدت طول خواهد کشید تا داده ها بازیابی شود؟
- تأثیر این خرابی از جمله از بین رفتن جایگاه عمومی چیست؟

داده ها زمانی ضروری هستند برای کسب و کار که سازمان بحرانی باشد. وقتی داده های ضروری در دسترس نیست، حتی برای یک دوره کوتاه، یا وقتی یکپارچگی آن زیر سوال می رود، سازمان قادر به عملکرد نیست. داده ها در صورت مهم بودن برای سازمان ضروری در نظر گرفته می شوند اما فعالیت سازمانی برای مدت زمانی از پیش تعیین شده حتی اگر داده ها در دسترس نباشد ادامه می یابد. اگر سازمان قادر به فعالیت بدون داده در مدت زمان طولانی باشد، داده غیر ضروری است.

هنگامی که حساسیت و بحرانی بودن داده ها درک و مستند شد، سازمان باید پس از ایجاد یک سیستم طبقه بندی داده ها به فعالیت خود ادامه دهد. اکثر سازمان ها از یک سیستم طبقه بندی کسب و کار تجاری یا سیستم طبقه بندی نظامی و دولتی استفاده می کنند.

طبقه بندی کسب و کار تجاری Commercial Business Classifications

کسب و کارهای تجاری معمولاً داده‌ها را با استفاده از چهار سطح اصلی طبقه بندی می‌کنند، از بالاترین سطح حساسیت تا پایین ترین سطح آنها:

۱- محرمانه بودن Confidential

۲- خصوصی بودن Private

۳- حساس بودن Sensitive

۴- عمومی بودن Public

داده‌های محرمانه شامل اسرار تجاری، داده‌های فکری، کد برنامه نویسی اپلیکیشن و سایر داده‌ها است که در صورت عدم افشای اطلاعات غیرمجاز می‌تواند به طور جدی بر سازمان تاثیر بگذارد. داده‌ها در این سطح فقط متعلق به کارکنانی از سازمان می‌باشند که فعالیت آنها مربوط به موضوع داده است. دسترسی به داده‌های محرمانه معمولاً برای هر دسترسی نیاز به مجوز دارد. طبق قانون آزادی اطلاعات، داده‌های محرمانه از افشای اطلاعات مستثنی هستند. در بیشتر موارد، تنها راه دسترسی اشخاص خارجی به اطلاعات محرمانه به شرح زیر است:

▪ پس از امضای یک توافق محرمانه

▪ هنگام رعایت یک حکم دادگاه

▪ به عنوان بخشی از یک پروژه دولتی یا توافق تهیه قرارداد

داده‌های خصوصی عبارتند از هر گونه اطلاعات مربوط به پرسنل، از جمله پرونده‌های منابع انسانی، مدارک پزشکی، و اطلاعات حقوق و دستمزد، که تنها در داخل سازمان استفاده می‌شود. داده‌های حساس شامل اطلاعات مالی سازمان است که نیاز به اقدامات اضافی برای اطمینان از صحت CIA آن در سازمان دارد. داده‌های عمومی داده‌هایی هستند که تاثیر منفی بر سازمان ندارند.

طبقه بندی نظامی و دولتی Military and Government Classifications

مؤسسات نظامی و دولتی معمولاً داده‌ها را با استفاده از پنج سطح اصلی طبقه بندی می‌کنند که از بالاترین حساسیت تا پایین ترین سطح موارد ذکر شده اند:

۱- فوق سری Top Secret

۲- سری Secret

۳- محرمانه بودن Confidential

۴- حساس اما بدون طبقه بندی Sensitive but unclassified

۵- طبقه بندی نشده Unclassified

داده‌های فوق سری شامل نقشه‌های سلاح، مشخصات فناوری، اطلاعات ماهواره جاسوسی و سایر اطلاعات نظامی است که در صورت افشای آنها می‌تواند به شدت به امنیت ملی آسیب برساند. داده‌های سری شامل برنامه‌های استقرار، قرار دادن موشک و سایر اطلاعاتی است که در صورت افشای آنها می‌تواند به امنیت ملی آسیب جدی وارد کند. داده‌های محرمانه شامل ثبت اختراعات، اسرار تجاری و سایر اطلاعاتی است که در صورت بروز افشای غیرمجاز می‌تواند به طور جدی بر دولت تأثیر بگذارد. داده‌های حساس اما طبقه بندی نشده شامل داده‌های پزشکی یا سایر داده‌های شخصی است که ممکن است آسیب جدی به امنیت ملی وارد نکند اما می‌تواند باعث شود که اعتبار دولت در مقابل شهروندان زیر سؤال برود. اطلاعات نظامی و دولتی که در هر چهار گروه دیگر قرار نمی‌گیرند، غیرقابل طبقه بندی تلقی می‌شوند و معمولاً براساس قانون آزادی اطلاعات باید به مردم اعطا شود.

چرخه عمر اطلاعات Information Life Cycle

سازمانها باید تضمین کنند که هر گونه اطلاعاتی که جمع آوری و ذخیره می‌کنند در طول دوره زندگی این اطلاعات مدیریت می‌شود. اگر هیچ چرخه عمر اطلاعات دنبال نشود، ذخیره سازی مورد نیاز برای اطلاعات در طول زمان افزایش می‌یابد تا منابع ذخیره سازی بیشتری مورد نیاز باشد. متخصصان امنیت باید تضمین کنند که صاحبان داده‌ها و نگهبانان داده‌ها چرخه عمر اطلاعات را درک می‌کنند.

برای اکثر سازمانها، پنج مرحله چرخه عمر اطلاعات به شرح زیر است:

۱- ایجاد / دریافت Create/receive

۲- توزیع کردن Distribute

۳- استفاده کردن Use

۴- حفظ Maintain

۵- دفع / ذخیره Dispose/store

در مرحله ایجاد / دریافت، داده‌ها یا توسط پرسنل سازمانی ایجاد می‌شوند یا از طریق پورتال ورود داده‌ها توسط سازمان دریافت می‌شوند. اگر داده‌ها توسط پرسنل سازمانی ایجاد شوند،

معمولاً در محلی که توزیع می شود، استفاده می شود و نگهداری می شود اما اگر داده از طریق مکانیسم دیگری دریافت شود، ممکن است لازم باشد داده ها را در یک مکان مناسب کپی یا وارد شود. در این حالت، داده ها پس از کپی، برای توزیع، استفاده و نگهداری در دسترس خواهند بود. پس از مرحله ایجاد / دریافت، پرسنل سازمان باید تضمین کنند که داده ها به درستی توزیع شده اند. در بیشتر موارد، شامل قرار دادن داده ها در مکان مناسب و احتمالاً پیکربندی مجوز دسترسی توسط مالک داده ها تعریف شده است. با این حال، به خاطر داشته باشید که در بسیاری موارد، محل ذخیره سازی و مجوزهای کاربر و گروه مناسب ممکن است قبلاً پیکربندی شده باشد. در چنین مواردی، فقط اطمینان از اینکه، داده ها در مکان توزیع صحیح قرار دارند.

مکان های توزیع شامل پایگاه های داده، پوشه های به اشتراک گذاشته شده، ذخیره سازی ضمیمه شبکه (NAS) Network-Attached Storage، شبکه های ذخیره سازی منطقه ای Storage Area Networks (SANs) و کتابخانه های داده Data libraries هستند.

هنگامی که داده ها توزیع شده اند، پرسنل درون سازمان می توانند از داده ها در عملیات روزانه خود استفاده کنند. در حالی که برخی از پرسنل فقط دسترسی خواندن داده ها را دارند، ممکن است پرسنل دیگر مجوزهای نوشتن یا کنترل کامل را داشته باشند. به خاطر داشته باشید که مجوزهای مجاز یا رد شده توسط صاحب داده تعیین شده، و توسط نگهبان داده پیکربندی شده است.

اکنون که داده ها در عملیات روزانه استفاده می شود، نگهداری داده ها کلید اطمینان از دسترسی داده ها و امنیت داده ها است. تعمیر و نگهداری شامل ممیزی، انجام پشتیبان گیری، نظارت بر عملکرد و مدیریت داده ها می باشد.

هنگامی که داده ها به پایان چرخه عمر رسیدند، باید به درستی از آنها استفاده کرد یا مطمئن شد که به صورت ایمن ذخیره شده اند. بعضی از سازمانها بایستی سوابق داده ها را برای چندین سال طبق قوانین یا مقررات محلی، ایالتی یا فدرال نگهداری کنند. علاوه بر این، هر گونه داده ای که بخشی از دادخواست باشد باید طبق درخواست دادگاه محفوظ نگه داشته شود، و سازمانها باید مراحل زنجیره مراقبت و مستندسازی مدارک را دنبال کنند. بایگانی داده ها و مراحل تخریب باید به روشنی توسط سازمان تعریف شود.

همه سازمان ها نیاز به روشی برای نگهداری و تخریب داده ها دارند. حفظ و تخریب داده ها باید از قوانین و مقررات محلی، ایالتی و دولتی پیروی کند. مستند سازی رویه های مناسب اطمینان می دهد که اطلاعات در مدت زمان مورد نیاز برای جلوگیری از جرمه های مالی و ممنوعیت

احتمالی افسران سازمانی سطح بالا نگهداری می‌شود. این روشها باید شامل دوره نگهداری و فرایند تخریب باشد.

شکل ۱-۲ چرخه عمر اطلاعات را نشان می‌دهد.



شکل ۱-۲: چرخه عمر اطلاعات

پایگاه داده‌ها Databases

پایگاه داده‌ها تبدیل به تکنولوژی انتخابی برای ذخیره، سازماندهی و تجزیه و تحلیل مجموعه‌ای از داده‌ها می‌شوند. کاربران از طریق واسط مشتری (Client Interface) به یک پایگاه داده دسترسی دارند. با ارائه دسترسی به اشخاص خارج از شرکت، فرصت برای سوء استفاده افزایش می‌یابد. در این بخش مفاهیم لازم برای بحث در مورد امنیت پایگاه داده و همچنین اهمیت موارد امنیتی پیرامون مدیریت و نگهداری از پایگاه داده پوشش داده شده است.

معماری و مدل‌های DBMS (DBMS Architecture and Models)

پایگاه داده‌ها حاوی داده‌ها هستند و تفاوت اصلی در مدل‌های پایگاه داده در نحوه ذخیره و سازماندهی اطلاعات است. این مدل روابط بین عناصر داده، نحوه دسترسی به داده‌ها، نحوه اطمینان از یکپارچگی و عملیات قابل قبول را توصیف می‌کند. پنج مدل یا معماری عبارتند از:

- ارتباطی Relational
- سلسله مراتبی Hierarchical
- شبکه Network
- شی گرا Object-oriented
- شی - رابطه‌ای Object-relational

مدل رابطه‌ای با استفاده از ویژگی (ستون) و چندتایی (ردیف) برای سازماندهی داده‌ها در جداول دوبعدی استفاده می‌شود. تقاطع یک ویژگی و یک چندتایی، یک رکورد را نشان می‌دهد. هنگام کار با سیستم‌های مدیریت پایگاه داده رابطه‌ای، باید شرایط زیر را درک کنید: رابطه Relation: یک موجودیت بنیادی در یک پایگاه داده رابطه‌ای در قالب یک جدول.

چندتایی Tuple: یک ردیف در یک جدول.

ویژگی Attribute: یک ستون در یک جدول.

طرح Schema: شرح یک پایگاه داده رابطه ای.

رکورد Record: مجموعه ای از اقلام داده های مرتبط.

رابطه پایه Base relation: در SQL، در واقع رابطه ای که در پایگاه داده وجود دارد.

مشاهده View: مجموعه ای از داده های موجود که به یک کاربر داده می شود. امنیت از طریق استفاده از این قوانین پیاده سازی می شود.

درجه Degree: تعداد ستون ها در یک جدول

اعداد اصلی Cardinality: تعداد ردیف ها در رابطه.

دامنه Domain: مجموعه ای از مقادیر مجاز که یک ویژگی می تواند بگیرد.

کلید اصلی Primary key: ستون هایی که هر ردیف را منحصر به فرد می کنند.

کلید خارجی Foreign key: یک ویژگی در یک رابطه است که دارای مقادیر مطابق با کلید اصلی در رابطه دیگر است. تطابق بین کلید خارجی با کلید اصلی از این جهت حائز اهمیت است زیرا آنها نمایانگر منابع از یک رابطه به رابطه دیگر و ایجاد ارتباط بین این روابط هستند.

کلید کاندید Candidate key: یک ویژگی در یک رابطه است که دارای مقادیر مطابق با کلید اصلی در رابطه دیگر است.

یکپارچگی یا جامعیت ارجاعی Referential integrity: لازم است که برای هر ویژگی کلیدی خارجی، رابطه ارجاع شده باید دارای مقداری با همان مقدار برای کلید اولیه آن باشد.

یک عنصر مهم طراحی پایگاه داده که تضمین می کند که ویژگی ها در یک جدول تنها به کلید اصلی بستگی دارند، فرآیند نرمال سازی Normalization نام دارد. نرمال سازی شامل:

- حذف گروه های تکراری با قرار دادن آنها در جداول جداگانه
- از بین بردن داده های بیش از حد (در بیش از یک جدول رخ می دهد)
- پاک کردن صفات در یک جدول که به کلید اصلی آن جدول وابسته نیستند

در مدل سلسله مراتبی، داده ها به صورت سلسله مراتبی سازماندهی شده اند. یک شیء می تواند یک فرزند (یک شیء که یک زیر مجموعه از شی والدین است)، چند فرزند یا بدون فرزند باشد. برای حرکت در این سلسله مراتب، باید شاخه ای را که در آن شی قرار دارد شناخته شود. یک مثال از استفاده از این سیستم، رجیستری ویندوز و دایرکتوری دسترسی پروتکل سبک (LDAP) Lightweight Directory Access Protocol است.

در مدل شبکه ای، همانند مدل سلسله مراتبی، داده‌ها به صورت سلسله مراتبی سازماندهی می‌شوند اما بر خلاف مدل سلسله مراتبی، اشیاء می‌توانند چندین والدین داشته باشند. به همین دلیل، دانستن اینکه کدام شاخه برای یافتن یک عنصر داده ضروری نیست، زیرا معمولاً مسیرهای متعددی برای آن وجود دارد.

مدل شی گرا توانایی اداره انواع مختلف داده را دارد و پویاتر از یک پایگاه داده رابطه‌ای است. سیستم پایگاه داده شی گرا (Object-oriented database (OODB برای ذخیره و دستکاری داده‌های پیچیده مانند تصاویر و گرافیک مفید است. در نتیجه، برای اپلیکیشن‌های پیچیده شامل Multimedia، طراحی کامپیوتری (Computer-aided design (CAD، ویدیو، گرافیک و سیستم‌های خبره مناسب‌تر هستند. همچنین دارای ویژگی‌های سهولت استفاده مجدد از کد و تجزیه و تحلیل و کاهش نگهداری هستند.

اشیاء را می‌توان در صورت نیاز ایجاد کرده و داده‌ها و رویه (یا روش‌ها) هنگام درخواست به هدف می‌رسند. یک روش یا همان Method کد مشخص کننده‌ای است که شی در پاسخ به یک پیام انجام می‌دهد. این مدل از مفاهیم یک مدل رابطه‌ای استفاده می‌کند. در مدل شی گرا، یک رابطه، ستون و چندتایی (اصطلاحات رابطه‌ای) را در اشیاء (کلاس، صفت و نمونه) گفته می‌شود. مدل شیء-رابطه‌ای، اتصال با فناوریهای شی گرا و رابطه‌ای است که ترکیبی از ویژگی‌های هر دو هستند. این یک پایگاه داده رابطه‌ای با نرم افزار واسط که در زبان برنامه نویسی شی گرا Object-Oriented Programming نوشته شده است. منطق و رویه‌ها از نرم افزار Front-End به جای پایگاه داده استخراج می‌شوند، و به این معنی است که هر برنامه Front-End می‌تواند روش خاص خود را داشته باشد.

زبانهای واسط پایگاه داده Database Interface Languages

دسترسی به اطلاعات در پایگاه داده توسط برنامه‌ای که به آسانی امکان می‌دهد داده‌ها را بدست آورده و تعامل برقرار کرد. این واسط‌ها می‌توانند به چندین زبان مختلف نوشته شوند. این بخش در مورد برخی از مهمترین زبان‌های برنامه نویسی داده بحث می‌شود:

- ODBC (Open Database Interconnection) ODBC: اتصال به پایگاه داده باز یک

API است که اجازه برقراری ارتباط با پایگاه داده را به صورت محلی یا از راه دور می‌دهد.

یک API مشتری، درخواست‌ها را به API ODBC ارسال می‌کند. ODBC API پایگاه

داده را پیدا می کند و یک درایور خاص درخواست را به یک دستور پایگاه داده تبدیل می کند که پایگاه داده خاص درک کند.

- JDBC : همانطور که از اسم آن انتظار می رود، اتصال به پایگاه داده جاوا Java Database Connectivity (JDBC) امکان می دهد برنامه های جاوا با یک پایگاه داده ارتباط برقرار کنند. API جاوا همان چیزی است که برنامه های Java را قادر می سازد دستورات SQL را اجرا کنند. JDBC پایگاه داده ای است که امکان ارتباط با انواع مختلفی از پایگاه داده ها را فراهم می آورد و قابلیتی همانند ODBC را فراهم می کند.
- XML : در حال حاضر می توان داده ها را در فرمت XML ایجاد کرد، اما XML: DB API به برنامه های XML اجازه می دهد تا با پایگاه داده های سنتی مانند پایگاه داده های رابطه ای، ارتباط برقرار کنند. لازم است که پایگاه داده دارای یک درایور اختصاصی پایگاه داده باشد که کلیه دسترسی منطقی پایگاه داده را کپسوله کند.
- OLE DB: پایگاه داده پیوند و تعبیه شده شی Object Linking Embedding Database (OLE DB) جایگزینی برای ODBC است که عملکرد آن را به پایگاه های داده غیر مرتبط گسترش می دهد. اگرچه مبتنی بر COM است و به ابزارهای مبتنی بر ویندوز مایکروسافت محدود است، اما دسترسی یکنواخت به انواع منابع داده از جمله سرویس از طریق اشیاء ActiveX را در اختیار برنامه های مختلف قرار می دهد.

انبار داده ها و داده کاوی Data Warehouses and Data Mining

انبار کردن داده ها فرایند ترکیب داده ها از چندین پایگاه داده یا منابع داده در یک مکان مرکزی به نام انبار است. انبار برای انجام تجزیه و تحلیل استفاده می شود. داده ها به سادگی ترکیب نشده اند بلکه به روشی مفیدتر و قابل درک تر پردازش و ارائه می شوند. انبارهای داده به امنیت دقیق نیاز دارند زیرا داده ها پراکنده نمی شوند بلکه در یک مکان مرکزی قرار دارند.

داده کاوی فرایند استفاده از ابزارهای ویژه برای سازماندهی داده ها به شکل مشخص است که باعث می شود تصمیمات کسب و کار بر اساس محتوا آسان تر شود. این مجموعه داده های بزرگ را در یک انبار داده تجزیه و تحلیل می کند تا الگوهای غیر آشکار را پیدا کند. این ابزار ارتباط بین داده ها را ایجاد می کند و این ارتباطات را به ابرداده Metadata مرتبط می کند. داده کاوی اجازه می دهد در مورد داده ها با نتیجه های پیچیده تر گاهی اوقات با نام کسب و کارهوشمند

[BI] business intelligence انجام شود. هنگام استفاده از برنامه‌های انبارداری داده‌ها باید سه اقدام انجام شود:

- کنترل ابرداده یا همان Metadata به صورت استفاده تعاملی.
- نظارت بر طرح (Plan) پاکسازی داده‌ها.
- داده‌های وفق داده شده بین محیط عملیات و انبار داده منتقل می‌شوند.

نگهداری پایگاه داده Database Maintenance

مدیران پایگاه داده باید به طور منظم نگهداری پایگاه داده را انجام دهند. پایگاه داده‌ها باید به طور منظم پشتیبان گیری شوند. تمام نکات امنیتی و بروز رسانی سخت افزار و نرم افزار، از جمله نرم افزار پایگاه داده، باید به روز شود. با افزایش نیازهای سازمانی و پیشرفت فناوری، ارتقاء سخت افزار و نرم افزار ضروری است.

متخصصان امنیت باید با مدیران پایگاه داده فعالیت کنند تا تضمین شود که تجزیه و تحلیل تهدید برای پایگاه داده‌ها حداقل به صورت سالانه انجام می‌شود. آنها همچنین باید تلاش کنند تا اقدامات مقابله و کنترل مناسبی را برای محافظت در برابر تهدیدهای شناسایی شده انجام دهند.

تهدیدات پایگاه داده Database Threats

تهدیدات امنیتی به پایگاه داده‌ها معمولاً در حوالی دسترسی ناخواسته به داده‌ها بوجود می‌آیند. دو تهدید امنیتی که در مدیریت پایگاه‌های داده وجود دارد شامل فرآیند جمع آوری و استنتاج Aggregation , Inference است. جمع آوری (Aggregation) قانون ترکیب اطلاعات از منابع مختلف است. این روش می‌تواند یک مسئله امنیتی با پایگاه داده‌ها باشد، زمانی که کاربر به یک مجموعه داده خاص از داده مورد هدف دسترسی ندارد، اما دسترسی به آنها را به صورت جداگانه یا حداقل برخی از آنها بدست می‌آورد و قادر به جمع آوری اطلاعاتی است که نباید دسترسی داشته باشد.

این فرآیند جمع آوری اطلاعات با هم، استنتاج (Inference) نامیده می‌شود. برای جلوگیری از دسترسی به اطلاعات قابل اطمینان، می‌توان از دو نوع اقدامات دسترسی استفاده کرد:

▪ **پایگاه‌های کنترل دسترسی وابسته به محتوای Content-dependent access**

control کنترل دسترسی وابسته به محتوا باعث ایجاد حساسیت در داده‌ها می‌شود. به

عنوان مثال، یک مدیر بخش ممکن است به حقوق کارمندان بخش خود دسترسی داشته باشد، اما نه به حقوق کارمندان سایر ادارات. هزینه این اندازه گیری افزایش سربار پردازش است.

- **کنترل دسترسی وابسته به متن** *Context-dependent access control* دسترسی به داده ها را بر روی عوامل متعدد برای جلوگیری از استنتاج پایه گذاری می کند. کنترل دسترسی می تواند یک عامل از قبیل مکان، زمان روز و سابقه دسترسی قبلی باشد.

مشاهدات پایگاه اطلاعاتی Database Views

دسترسی به اطلاعات در یک پایگاه داده معمولاً از طریق استفاده از مشاهده پایگاه داده کنترل می شود. یک نمایه یا view به مجموعه داده ها که کاربر یا گروهی از کاربران می توانند در هنگام دسترسی به پایگاه داده مشاهده کنند. قبل از اینکه کاربر بتواند از یک نمایه استفاده کند، باید هم در نمایه و هم برای همه اشیاء وابسته مجوز داشته باشد. نمایه ها مفهوم حداقل امتیاز را پیاده سازی می کند.

قفل های پایگاه داده Database Locks

قفل پایگاه داده هنگامی استفاده می شود که یک کاربر به یک رکورد دسترسی پیدا کند و مانع از دسترسی کاربر دیگر به این رکورد در همان زمان برای ویرایش تا زمانی که کار کاربر اول تمام شود. قفل نه تنها امکان نوشتن را فراهم می کند بلکه همچنین خواندن اصلاحات ناتمام یا داده های غیر متعهد را کنترل می کند.

چند منظوره Polyinstantiation

فرآیندی است که برای جلوگیری از نقض استنتاج داده ها مانند تهدیدات پایگاه داده که قبلاً در این فصل بحث شد، استفاده می شود. این کار را با ایجاد یک رابطه برای یک ردیف جدول چندگانه (Tuple) با همان کلیدهای اصلی انجام می دهد، که هر نمونه با یک سطح امنیت مشخص می شود. از کاربران پایگاه داده سطح پایین برای استنتاج داده های سطح بالاتر جلوگیری می شود.

تست OLTP ACID

یک سیستم پردازش تراکنش آنلاین Online Transaction Processing برای نظارت بر مشکلاتی مانند فرآیندهای متوقف کردن عملکرد، استفاده می‌شود. هدف اصلی آن جلوگیری از انجام تراکنشها Transactions است که به درستی انجام نمی‌شود و یا کامل نیستند. تست ACID تضمین می‌کند که هر تراکنش قبل از انجام این کار دارای خواص زیر است:

- اتمی Atomicity: تمام عملیات تمام شده است، یا تغییرات پایگاه داده به عقب رانده شده است.
- ثبات Consistency: تراکنش از یک فرآیند یکپارچگی پیروی می‌کند که تضمین می‌کند داده‌ها در همه مکان‌هایی که وجود دارند سازگاری باشند.
- جداسازی Isolation: یک تراکنش با سایر تراکنش‌ها تا زمان تکمیل، تعاملی ندارد.
- دوام Durability: پس از تأییدیه، تراکنشهای صورت گرفته، نمی‌تواند بازگردانده شود.

ممیزی داده‌ها Data Audit

در حالی که یک سازمان ممکن است برنامه مدیریت داده‌های جدید را به روز نگه دارد، مدیریت داده‌ها به تنهایی به اندازه کافی برای محافظت از داده‌ها کامل نیست. سازمانها همچنین باید یک مکانیزم ممیزی داده را ایجاد کنند که به مدیران کمک می‌کند تا آسیب پذیری‌ها را قبل از وقوع حملات شناسایی کنند. مکانیزم‌های ممیزی را می‌توان برای کنترل تقریباً هر سطح دسترسی به داده‌ها پیکربندی کرد. با این حال، مکانیزم ممیزی بر عملکرد سیستم‌های ممیزی تأثیر می‌گذارد. همیشه تأثیر عملکردی که در نتیجه مکانیزم ممیزی ممکن است رخ دهد را به دقت در نظر بگیرید. در حالی که ممیزی ضروری است، مهم نیست که بسیاری از رخدادهایی را که حساب‌های ممیزی با اطلاعات بی‌فایده و یا استفاده نشده بکار برده اند، کنترل شود. داده محرمانه یا حساس باید با دقت بیشتری نسبت به اطلاعات عمومی بررسی شود. در حقیقت، ممکن است لازم باشد که دسترسی به اطلاعات عمومی نیز ممیزی شود. اما با توجه به ممیزی داده‌های محرمانه، یک سازمان ممکن است تصمیم بگیرد تمام دسترسی به آن داده‌ها را بررسی کند یا فقط تلاش کند که داده‌ها را تغییر دهد. تنها سازمان و پرسنل آن قادر به ایجاد بهترین طرح ممیزی هستند.

در نهایت، ممیزی فقط اگر یک بررسی منظم از logهای تولید شده وجود داشته باشد ایده آل است. مدیران و یا متخصصان امنیت باید آموزش های لازم را در مورد بررسی logهای ممیزی بدست آورند. علاوه بر این، هشدارهای مناسب باید در صورت وقوع رخدادهای بحرانی پیکربندی شوند. به عنوان مثال، اگر چندین حساب کاربری به علت تلاش نامعتبر برای مدت زمان کوتاه قفل شده باشند، ممکن است نشانه ای از این باشد که سیستم ها یک فرهنگ لغت یا حملات گذرواژه را تجربه می کنند. اگر یک هشدار به منظور اطلاع مدیران در هنگام یک تعداد مشخصی از قفل در طی یک دوره زمانی رخ داده باشد، مدیران ممکن است قادر به محدود کردن مسئله باشند قبل از اینکه دسترسی موفقیت آمیز توسط مهاجم بدست آید.

مالکیت دارایی Asset Ownership

در حالی که دارایی های یک سازمان در نهایت متعلق به سازمان است، معمولاً قابل درک است که دارایی های موجود در سازمان متعلق به واحدهای کسب و کار مختلف می باشند. این واحدهای کسب و کار باید برای اطمینان از دستیابی به مأموریت سازمانی و محافظت از داراییها، با یکدیگر همکاری کنند.

به همین علت، متخصصان امنیت باید درک این را داشته باشند که دارایی های مختلف در کجا قرار دارند و با صاحبان مختلف همکاری می کنند تا تضمین شود که از دارایی ها و داده ها محافظت می شود. صاحبانی که متخصصان امنیت باید با آنها همکاری کنند شامل صاحبان داده، صاحبان سیستم و صاحبان مشاغل / مأموریت ها هستند. به عنوان بخشی از مالکیت دارایی، متخصصان امنیت باید تضمین کنند که رویه های مدیریت دارایی مناسب، توسعه یافته و دنبال می شوند.

صاحبان داده (مالکان داده) Data Owners

همانطور که قبلاً ذکر شد صاحبان داده ها اطلاعات خود را دارند. متأسفانه، در اکثر موارد، صاحبان داده ها سیستم های مربوط به داده های خود را ندارند. بنابراین، مهم است که صاحب داده همکاری نزدیک با مالک سیستم داشته باشد حتی اگر ACLهای مناسب برای داده ها پیکربندی شوند، اگر سیستم که داده ها در آن مستقر است، به درستی ایمن نباشد، می تواند داده ها را به خطر اندازد.

مالکان سیستم System Owners

مالکان سیستم مسئول سیستم هایی هستند که داده ها در آن قرار دارند. در حالی که صاحب داده مالک داده است و نگهدارنده داده مجوز مناسب برای دسترسی کاربر به داده را تنظیم می کند، مالک سیستم باید سیستم را اداره کند، که شامل مدیریت تمام کنترل های امنیتی در سیستم، استفاده از پچها (Patch)، پیکربندی فایروال مبتنی بر میزبان (در صورت وجود)، و همچنین تهیه نسخه پشتیبان است.

صاحبان ماموریت / کسب و کار Business/Mission Owners

صاحبان ماموریت / کسب و کار باید تضمین کنند که تمام عملیات متناسب با اهداف و ماموریت های کسب و کار است، که شامل تضمین عملکرد داده های جمع آوری شده برای عملکرد کسب و کار است. جمع آوری داده های غیر ضروری باعث اتلاف وقت و منابع می شود. از آنجا که صاحب ماموریت / کسب و کار در درجه اول به کسب و کار کلی مربوط می شود، ممکن است درگیری بین صاحبان داده، نگهدارندگان داده و مالکان سیستم توسط صاحب ماموریت / کسب و کار حل شود، که باید بهترین تصمیم را برای سازمان اتخاذ کنند. به عنوان مثال، می گویند که یک صاحب داده، فضای بیشتری را در یک سیستم برای ذخیره داده ها درخواست می کند. صاحب داده به شدت معتقد است که جمع آوری داده های جدید به تیم فروش کمک خواهد کرد که کارایی بیشتری داشته باشد. اگرچه، ذخیره سازی دارایی مالک سیستم، حق وی می باشد. مالک سیستم تمایلی به اجازه دادن به صاحب داده برای استفاده از مقدار فضای درخواست شده خود ندارد. در این حالت، صاحب ماموریت / کسب و کارها باید هر دو طرف را بررسی کند و تصمیم بگیرند که آیا جمع آوری و ذخیره کردن داده های جدید منجر به افزایش درآمد کافی برای توجیه هزینه اجازه دادن به فضای ذخیره بیشتر برای صاحب داده خواهد شد یا خیر. در این صورت ممکن است سرمایه گذاری در رسانه های ذخیره سازی بیشتر برای سیستم یا انتقال داده ها به سیستم دیگری که منابع بیشتری در اختیار دارد، لازم باشد. اما به خاطر داشته باشید که انتقال داده ها احتمالاً مالک سیستم دیگری را درگیر خواهد کرد.

متخصصان امنیت همیشه باید بخشی از این تصمیمات باشند زیرا آنها کنترل های امنیتی را برای هر سیستم درگیر و کنترل های امنیتی مورد نیاز برای محافظت از داده ها را درک می کنند. انتقال داده ها به سیستمی که دارای کنترل های مناسب نیست ممکن است صرفاً باعث بروز مشکلات

بیشتر روزرسانی سیستمی شود که در حال حاضر داده ها در آن قرار دارد. فقط یک متخصص امنیت قادر است به صورت عینی نیازهای امنیتی داده ها را ارزیابی کرده و تضمین کند که نیازها برآورده شده اند.

مدیریت دارایی Asset Management

در فرآیند مدیریت این دارایی ها، باید به چندین موضوع پرداخته شود. بدیهی است که دسترسی به دارایی باید به طور دقیق کنترل شود تا از حذف، سرقت، یا فساد (در مورد دارایی های دیجیتال) آن و از آسیب فیزیکی (در مورد دارایی های فیزیکی) جلوگیری شود. علاوه بر این، دارایی باید در صورت لزوم در دسترس باشد. در این بخش روشهایی را برای اطمینان از دسترسی، مجوز و یکپارچگی ارائه می شود.

افزونگی و تحمل خطا Redundancy and Fault Tolerance

یکی از راه های دسترسی بی وقفه به دارایی های اطلاعاتی، از طریق افزونگی و تحمل خطا است. افزونگی به ارائه چند نمونه از یک مولفه فیزیکی یا منطقی اشاره دارد، به طوری که یکی از مولفه های دوم در صورت عدم موفقیت مولفه اولی در دسترس است. تحمل خطا مفهوم وسیع تری است که افزونگی را شامل می شود اما به هر حال به فرایندی اطلاق می شود که به سیستم اجازه می دهد در صورت شکست، دارایی های اطلاعاتی را در دسترس قرار دهد.

در بعضی موارد، افزونگی در لایه فیزیکی مدل مرجع Open Systems Interconnection (OSI) اعمال می شود، مانند افزونگی شبکه که توسط ستون فقرات دوگانه Dual Backbone در محیط شبکه محلی یا با استفاده از کارت های شبکه چندگانه در یک سرور بحرانی، اعمال می شود. در موارد دیگر، افزونگی به صورت منطقی اعمال می شود، مانند زمان عدم موفقیت، روتر مسیرهای چندگانه به مقصد را شناسایی می کند.

اقدامات متقابل تحمل خطا برای مبارزه با تهدیدات برای طراحی قابلیت اطمینان طراحی شده است. اگرچه تحمل خطا میتواند شامل افزونگی باشد، اما همچنین به سیستمهایی نظیر آرایه دیسک مستقل یا همان Redundant Array of Independent Disks (RAID) اشاره دارد که در آن داده ها در چندین دیسک نوشته شده، به گونه ای که دیسک نتواند خراب شود و داده ها از دیسک های موجود در آرایه بدون استفاده از نوار پشتیبان به سرعت از باقیمانده قابل تهیه باشند. با تعدادی از انواع RAID آشنا شوید زیرا همه آنها تحمل خطا را ندارند. RAID بعداً در این

بخش پوشش داده می‌شود. صرف نظر از تکنیک مورد استفاده برای تحمل خطا، یک سیستم باید قابلیت تشخیص و اصلاح خطا را داشته باشد.

سیستم‌های پشتیبان گیری و بازیابی Backup and Recovery Systems

اگرچه در فصل ۷ "عملیات امنیتی" پوشش کاملی از سیستم‌های پشتیبان و بازیابی بحث می‌شود، اما مهم است که در اینجا بر نقش عملیات در انجام این فعالیت‌ها تاکید شود. پس از طراحی برنامه زمانی تهیه نسخه پشتیبان، کارهای روزانه‌ای در رابطه با اجرای طرح انجام خواهد شد. یکی از مهمترین قسمت‌های این سیستم یک فرآیند تست مداوم است تا تضمین شود که در صورت نیاز به بازیابی، کلیه نسخه‌های پشتیبان قابل استفاده است. زمان کشف اینکه یک پشتیبان گیری موفق نشده است، در حین تست می‌باشد نه در طول بازیابی.

هویت و مدیریت دسترسی Identity and Access Management

هویت و مدیریت دسترسی به طور کامل در فصل ۵ "هویت و دسترسی" پوشش داده می‌شود. مدیریت از دیدگاه عملیاتی، مهم است بدانیم که مدیریت این موارد یک فرآیند مداوم است که ممکن است نیاز به ایجاد حساب‌ها، حذف حساب‌ها، ایجاد و پرورش گروه‌ها و مدیریت مجوزهای مرتبط با همه این مفاهیم داشته باشد. حصول اطمینان از اینکه حقوق انجام این اقدامات به شدت کنترل می‌شود و انجام یک فرایند رسمی برای از بین بردن مجوزها هنگامی که آنها دیگر لازم نیستند و غیرفعال کردن حساب‌های مورد نیاز دیگر، ضروری است.

زمینه دیگر برای تمرکز، کنترل استفاده از حساب‌های ممتاز، و یا حساب‌هایی است که دارای حقوق و مجوزهایی هستند که فراتر از حساب یک کاربر معمولی است. اگرچه این امر به طور واضح در مورد حساب‌های ادمین یا همان Administrator و سرپرست یا همان Supervisor (به نام‌های حساب‌های ریشه (Root) در برخی از سیستم عامل‌ها) وجود دارد که دارای مجوزهای گسترده‌ای هستند، همچنین برای حساب‌هایی مانند حساب کاربری قوی Power User account ویندوز که قبل از ویندوز ۷ استفاده می‌شد، نیز اعمال می‌شود.

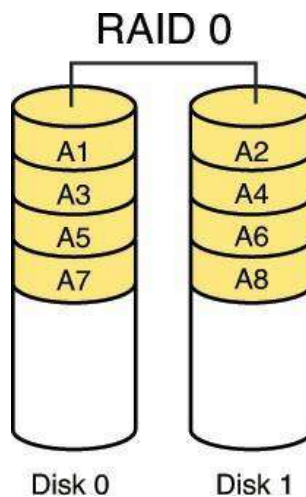
علاوه بر این، همان کنترل دقیق در مورد گروه‌های متعدد ساخته شده در ویندوز وجود دارد تا حقوق ویژه‌ای را به اعضای گروه اعطا کند. هنگام استفاده از این گروه‌ها، به هر گونه امتیازات گروه‌های پیش فرض که برای اهداف شما مورد نیاز نیست، توجه داشته باشید. ممکن است

بخواهید بعضی از امتیازات از گروههای پیشفرض حذف شود تا مفهوم حداقل امتیاز را پشتیبانی کند.

RAID

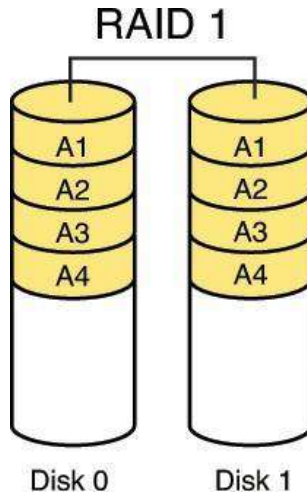
آرایه افزونه دیسکهای مستقل Redundant Array of Independent Disks به سیستمی اطلاق می شود که در آن از چندین درایو سخت استفاده می شود تا یک تقویت عملکرد یا تحمل خطا برای داده ها فراهم شود. هنگامی که در مورد تحمل خطا در RAID صحبت می کنیم، منظور ما حفظ دسترسی به داده ها حتی در خرابی درایو بدون بازیابی داده ها از رسانه پشتیبان است. موارد زیر انواع RAID می باشد که باید با آنها آشنا باشید.

RAID 0، که به آن نوار دیسک (Disk Striping) نیز گفته می شود، داده ها را در درایوهای مختلف می نویسد. اگر چه عملکرد را بهبود می بخشد، اما تحمل خطا را ارائه نمی دهد. شکل ۲-۲ RAID 0 را نشان می دهد.



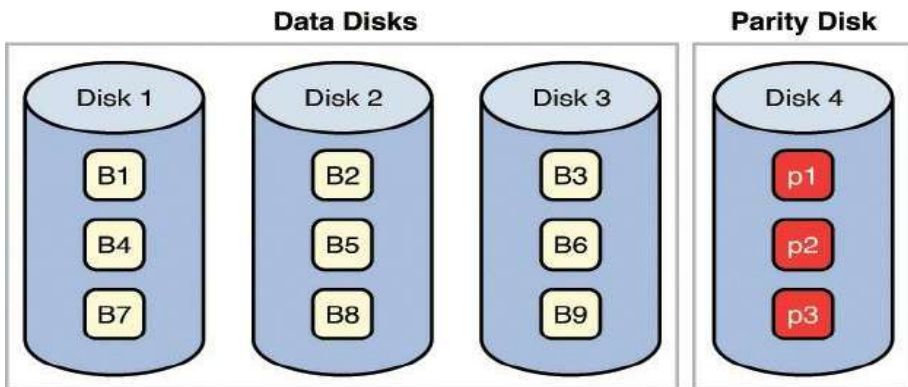
شکل ۲-۲: RAID 0

RAID 1، همچنین همانندسازی دیسک (Disk Mirroring) نامیده می شود، از دو دیسک استفاده می کند و یک نسخه از داده ها را در هر دو دیسک می نویسد و تحمل خطا را در صورت شکست یا خرابی یک درایو فراهم می کنند. شکل ۲-۳ RAID 1 را نشان می دهد.



شکل ۲-۳: RAID 1

RAID 3، که نیاز به حداقل سه درایو دارد، همچنین نیاز دارد که داده‌ها در همه درایوها مانند نوار نوشته و سپس اطلاعات یکسان (Parity Information) در یک درایو اختصاصی نوشته شوند. از اطلاعات یکسان برای بازیابی اطلاعات در صورت خرابی تک درایو استفاده می‌شود. نقطه ضعف این است که درایو یکسان اگر بدعمل کند یا خراب شود یک نقطه شکست محسوب می‌شود. شکل ۲-۴ RAID 3 را نشان می‌دهد.

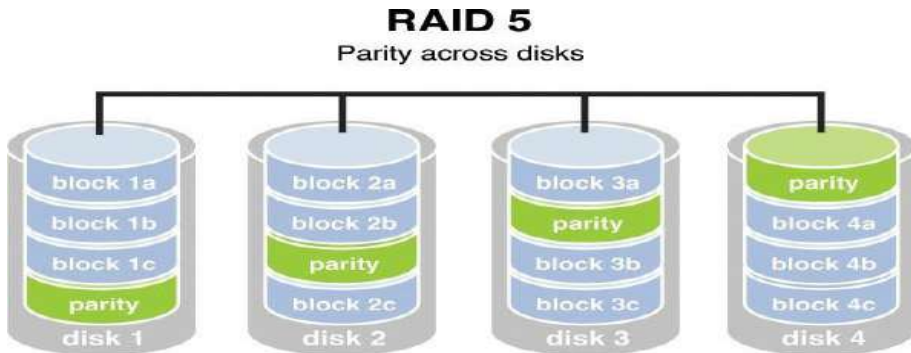


RAID 3 – Bytes Striped (and Dedicated Parity Disk)

شکل ۲-۴: RAID 3

RAID 5، نیاز به حداقل سه درایو دارد، همچنین نیاز به این دارد که داده‌ها در تمام درایوها مانند نوار نوشته شده و سپس اطلاعات یکسان در تمام درایوها نیز نوشته شود. اطلاعات یکسان

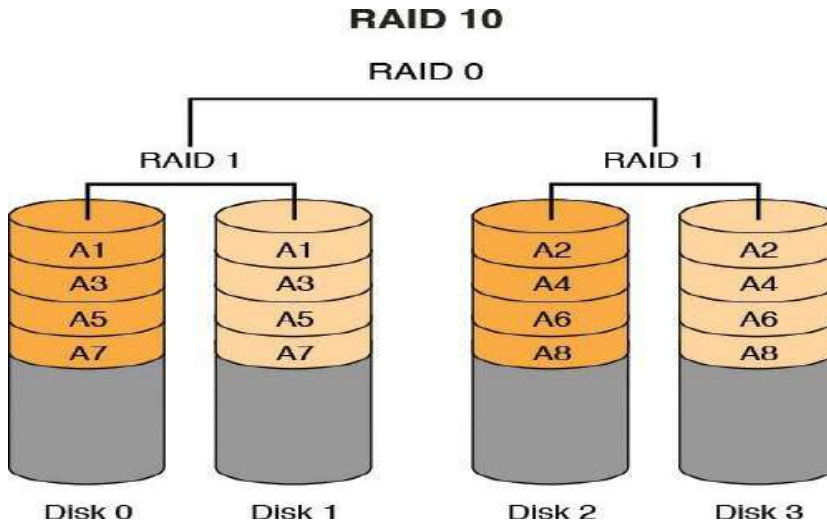
به همان شیوه RAID 3 استفاده می شود، اما بر روی یک درایو منفرد ذخیره نمی شود، بنابراین هیچ نقطه ای از خرابی برای داده های یکسان وجود ندارد. با وجود سخت افزار RAID سطح ۵، درایوهای جایگزین (Spare Drives) که جایگزین درایوهای خراب شده می شوند معمولاً قابل تعویض هستند، به این معنی که در هنگام کار می توان آنها را روی سرور جایگزین کرد. شکل ۲-۵ تصویر RAID 5 را نشان می دهد.



شکل ۲-۵: RAID 5

RAID 7 که یک استاندارد نیست بلکه یک پیاده سازی اختصاصی است، همان اصول RAID 5 را در خود جای داده است اما در صورت عدم موفقیت هر دیسک یا هر راهی برای دیسک، درایو را قادر به ادامه کار می کند. دیسک های چندگانه در آرایه به صورت یک دیسک مجازی عمل می کند.

RAID 10 ترکیبی از RAID 1 و RAID 0 است که حداقل به دو دیسک نیاز دارد. با این حال، بسیاری از پیاده سازی RAID 10 دارای چهار یا درایوهای بیشتر هستند. استقرار RAID 10 حاوی یک نوار دیسک است که روی یک نوار دیسک جداگانه نشان داده شده است. شکل ۲-۶ RAID 10 را نشان می دهد.



شکل ۲-۶: RAID 10

اگر چه RAID را می‌توان با نرم افزار یا سخت افزار اجرا کرد، انواع خاصی از RAID با سخت افزار سریعتر اجرا می‌شوند. هنگام استفاده از RAID نرم افزار، که عملکردی از سیستم عامل است. هر دو RAID 3 و RAID 5 نمونه‌ای از انواع RAID می‌باشد که سریعتر با سخت افزار اجرا می‌شوند. با این حال، (Striping, Mirroring) نوار کردن و یا همانندسازی (RAID 0 and 1)، در نرم افزار به خوبی عمل می‌کند، زیرا آنها از درایوهای پارتیتی یا همان یکسان سخت افزاری استفاده نمی‌کنند. جدول ۲-۱ انواع RAID را خلاصه می‌کند.

RAID Level	Min. Number of Drives	Description	Strengths	Weaknesses
RAID 0	2	Data striping without redundancy	Highest performance	No data protection; one drive fails, all data is lost
RAID 1	2	Disk mirroring	Very high performance; very high data protection; very minimal penalty on write performance	High redundancy cost overhead; because all data is duplicated, twice the storage capacity is required
RAID 3	3	Byte-level data striping with dedicated parity drive	Excellent performance for large, sequential data requests	Not well-suited for transaction-oriented network applications; single parity drive does not support multiple, simultaneous read and write requests
RAID 5	3	Block-level data striping with distributed parity	Best cost/performance for transaction-oriented networks; very high performance, very high data protection; supports multiple simultaneous reads and writes; can also be optimized for large, sequential requests	Write performance is slower than RAID 0 or RAID 1
RAID 10	2	Disk striping with mirroring	High data protection, which increases each time to add a new striped/mirror set	High redundancy cost overhead; because all data is duplicated, twice the storage capacity is required

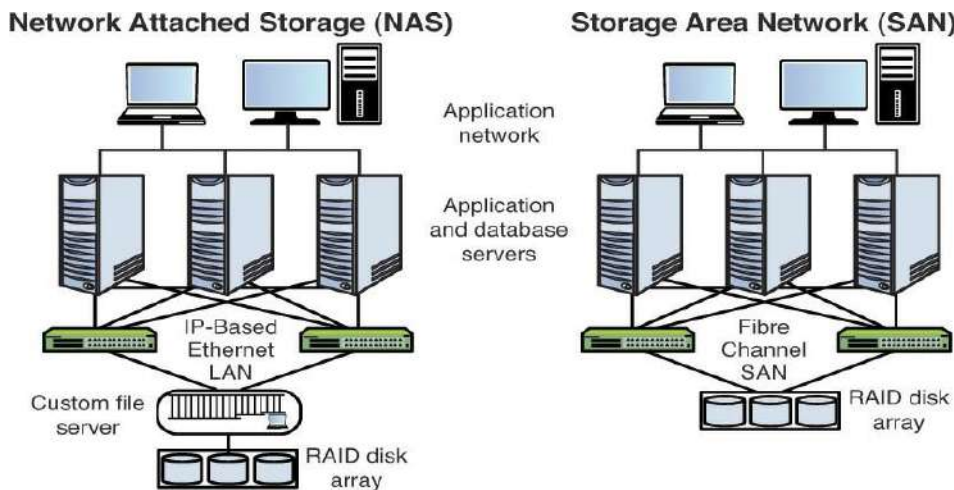
جدول ۱-۲: RAID

SAN

شبکه‌های ذخیره سازی منطقه‌ای (SAN) Storage-area networks شامل دستگاه‌های ذخیره سازی با ظرفیت بالا هستند که توسط یک شبکه خصوصی با سرعت بالا (جدا از شبکه LAN) با استفاده از سوئیچ‌های ذخیره سازی خاص متصل می‌شوند. این معماری اطلاعات ذخیره سازی، جمع آوری داده ها، مدیریت داده‌ها و استفاده از داده‌ها را پاسخ می‌دهد.

NAS

ذخیره سازی ضمایم شبکه (NAS) Network-attached storage همانند SAN عمل می کند، اما مشتریان (Clients) به شیوه ای دیگر به ذخیره سازی دسترسی پیدا می کنند. در یک NAS، تقریباً هر دستگاهی که می تواند به LAN متصل شود (یا از طریق یک شبکه WAN به شبکه متصل شود) می تواند از پروتکل هایی مانند NFS، CIFS، HTTP برای اتصال به NAS استفاده کند و فایل ها را به اشتراک بگذارد. در یک SAN فقط دستگاه هایی که می توانند از کانال فیبرنوری، iSCSI، ATA از طریق اترنت یا شبکه HyperSCSI استفاده کنند، می توانند به داده ها دسترسی پیدا کنند، بنابراین این کار معمولاً با وجود این سرور انجام می شود. شکل ۲-۷ مقایسه دو سیستم را نشان می دهد.



شکل ۲-۷: NAS و SAN

HSM

یک سیستم مدیریت ذخیره سازی سلسله مراتبی Hierarchical Storage Management یک نوع سیستم مدیریت پشتیبان است که یک پشتیبان آنلاین مستمر را با استفاده از دستگاه های jukeboxes - نوری (Optical) - یا نواری (Tape) فراهم می کند. این دستگاه با حرکت خودکار داده ها بین رسانه های ذخیره سازی با هزینه بالا و هزینه پایین به عنوان عمر داده ها عمل می کند. زمانیکه در دسترس بودن مداوم (پردازش ۲۴ ساعته روزانه) مورد نیاز می باشد، HSM یک جایگزین مناسب برای پشتیبان گیری نواری (Tape) است. همچنین از رسانه مناسب برای سناریو

استفاده می‌کند. به عنوان مثال، دیسک‌های نوری دیجیتال (DVD) گاهی برای پشتیبان‌گیری استفاده می‌شوند که برای داده‌های قابل تغییر نیاز به ذخیره سازی کوتاه مدت دارند و نیاز به دسترسی سریعتر فایل نسبت به نوار دارند.

توسعه سریال ATA (SATA) موجب پیشرفت بیشتر در HSM شده است. HSM سه مرحله‌ای می‌تواند اجرا شود که آرایه‌های SATA ارزان اما کند تر را می‌نویسد. برخی از پیاده سازی‌های HSM حتی از درایوهای سخت مغناطیسی و درایوهای حالت جامد Solid-State استفاده می‌کنند. سازمانها همیشه باید در زمینه آخرین فن آوری‌ها به تحقیق بپردازند برای بررسی اینکه آیا می‌توانند در زمان و هزینه صرفه جویی کنند.

مدیریت شبکه و منابع Network and Resource Management

اگر چه عملیات امنیتی توجه را به ارائه محرمانه بودن و یکپارچگی اطلاعات متمرکز می‌کند، دسترسی به اطلاعات نیز یکی از اهداف آن می‌باشد. این به معنی طراحی و نگهداری فرایندها و سیستم‌هایی است که دسترسی به منابع را در صورت عدم دسترسی به سخت افزار یا نرم افزار در محیط حفظ می‌کنند. اصول و مفاهیم زیر در حفظ دسترسی به منابع کمک می‌کنند:

- **افزودگی سخت افزاری Redundant hardware:** خرابی مولفه‌های فیزیکی مانند دیسک‌های سخت و کارت‌های شبکه می‌تواند دسترسی به منابع را مختل کند. فراهم کردن موارد اضافی از این مولفه‌ها می‌تواند به اطمینان بازگشت سریع تر دسترسی‌ها کمک کند. در بیشتر موارد، تغییر یک مولفه ممکن است مستلزم اقدام مداخله دستی باشد، حتی با استفاده از دستگاه‌های با قابلیت جابجایی (می‌توان آنها را با دستگاه تغییر داد و اجرا کرد)، در این صورت ممکن است باعث کاهش لحظه‌ای عملکرد در مقایسه با اختلال دسترسی کامل شود.
- **فناوری تحمل خطا Fault-tolerant technologies:** انتقال ایده‌های افزودگی به سطح بعدی، فناوری‌هایی هستند که مبتنی بر چندین سیستم محاسباتی هستند که با هم کار می‌کنند تا حتی در صورت خرابی یکی از سیستم‌ها، دسترسی بدون وقفه را فراهم کنند. خوشه بندی سرورها و محاسبات شبکه هر دو نمونه عالی از این رویکرد است.

- **توافقات سطح سرویس (SLAs) Service-level agreements** توافقات در مورد توانایی سیستم پشتیبانی برای پاسخگویی به مشکلات در یک بازه زمانی خاص در حالی که سطح سرویس مورد توافق را ارائه می‌دهند. آنها می‌توانند بین دپارتمان‌های داخلی و یا یک ارائه دهنده سرویس خارجی باشند. با توافق در مورد سرعت بخشیدن به مشکلات مختلف، برخی از موارد قابل پیش بینی، پاسخ به مشکلات معرفی شده است که در نهایت از نگهداری دسترسی به منابع پشتیبانی می‌کند.
- **MTBF و MTTR**: اگر چه SLAها برای خدماتی که ارائه می‌شوند، مناسب هستند، می‌توان از رویکرد کمی متفاوت برای معرفی قابلیت پیش بینی با توجه به اجزای فیزیکی خریداری شده استفاده کرد. فروشندگان به طور معمول مقادیر میانگین زمان محصول بین خرابی، Mean Time Between Failure (MTBF) را منتشر می‌کنند، که توصیف می‌کند اغلب یک مولفه به طور متوسط چگونه از کار می‌افتد. یکی دیگر از معیارهای ارزشمند که به طور معمول ارائه می‌شود، میانگین زمان تعمیر (MTTR) Mean Time to Repair است که میانگین زمان لازم برای دریافت تعمیر دستگاه را به صورت آنلاین نشان می‌دهد.
- **تنها نقطه شکست (SPOF) Single point of failure**: اگر چه یک استراتژی نیست، لازم به ذکر است که هدف نهایی هر یک از این روش‌ها جلوگیری از SPOF در یک سیستم است. تمام مولفه‌ها و گروه‌های مولفه‌ها و دستگاه‌ها باید مورد بررسی قرار گیرد تا بتواند هر عنصر انفرادی را شناسایی کرده و در صورت وقوع خرابی امکان دسترسی به منابع را قطع کند. سپس هر SPOF باید به نحوی تعدیل شود.

حریم خصوصی دارایی Asset Privacy

حریم خصوصی دارایی شامل اطمینان از اینکه تمام دارایی‌های سازمانی دارای سطح حریم خصوصی مورد نیاز هستند. اما وقتی امنیت دارایی‌ها مطرح می‌شود، باید چگونگی محافظت از حریم خصوصی دارایی درک شود. این بخش در مورد پردازنده داده‌ها، ذخیره سازی داده‌ها و بایگانی داده‌ها، بازنمایی باقیمانده داده و محدودیت جمع آوری بحث می‌کند.

• پردازشگرهای داده Data Processors

پردازشگرهای داده، پرسنلی در یک سازمان هستند که داده هایی را که در طی کل چرخه عمر داده ها جمع آوری شده، پردازش می کنند. اگر هر فردی به هر روشی به داده ها دسترسی پیدا کند، می تواند یک فرد پردازشگر داده محسوب شود. با این حال، در برخی از سازمان ها، پردازشگرهای داده فقط می توانند داده ها را وارد یا تغییر دهند.

مهم نیست که یک سازمان از چه تعریفی استفاده کند، مهم است که متخصصان امنیت برای ارائه آموزش به کلیه پردازشگرهای داده در مورد اهمیت حفظ حریم خصوصی دارایی ها، به خصوص حفظ حریم خصوصی داده ها تلاش کنند. این معمولاً به عنوان بخشی از پرورش آگاهی امنیتی محسوب می شود. همچنین حائز اهمیت است که هر استاندارد یا سیاست حفظ حریم خصوصی بر اساس قوانین و مقررات باشد. هنگامی که کارکنان آموزش های مناسب را دریافت کردند، باید بیانیهای را امضا کنند که می گوید از سیاست حفظ حریم خصوصی سازمان پیروی می کنند.

• ذخیره سازی و بایگانی داده ها Data Storage and Archiving

ذخیره سازی و بایگانی داده ها به نحوی است که داده های ذخیره شده سازمان، داده های دیجیتال و داده های فیزیکی را به صورت نسخه های سخت Hard Copy ذخیره می کنند. برای داده های منسوخ شده بسیار آسان می باشد. هنگامی که داده ها منسوخ شده اند، دیگر برای سازمان مفید نیست.

با افزایش حجم داده ها، ذخیره سازی داده ها بسیار هزینه بر می شود. متخصصان امنیت باید با صاحبان داده ها و نگهبانان داده ها برای کمک به ایجاد یک سیاست بازنگری داده ها به فعالیت بپردازند تا تضمین شود که داده ها به طور دوره ای بررسی می شوند تا تعیین شود که آیا برای سازمان مفید هستند. داده هایی که دیگر برای سازمان ضروری یا مفید نیستند باید بایگانی شوند. با توجه به ذخیره سازی و بایگانی داده ها، متخصصان امنیت باید اطمینان حاصل کنند که جنبه های مختلف ذخیره سازی به درستی مورد تجزیه و تحلیل قرار گرفته تا تضمین شود که به طور مناسب استقرار یافته اند. این شامل تجزیه و تحلیل سرور سخت افزار و نرم افزار، نگهداری پایگاه داده، تهیه نسخه پشتیبان داده ها و زیرساخت های شبکه است. هر بخشی از دنباله دیجیتال

که داده‌ها انتقال می‌یابند باید درک شود تا سیاست‌ها و رویه‌های مناسب بتواند درجایی قرار گیرد که برای حریم خصوصی اطمینان ایجاد کند.

داده‌هایی که هنوز مورد نیاز و مفید برای سازمان هستند برای دسترسی آسان کاربران باید در حافظه اولیه باقی بمانند. داده‌های مشخص شده برای بایگانی باید به نوعی به رسانه پشتیبان یا مخزن ذخیره ساری ثانویه منتقل شوند. سازمانها باید شکل ذخیره بایگانی داده‌ها را متناسب با نیازهای آنها تعیین کنند. برای بعضی از واحدهای کسب و کار در سازمان، ممکن است برای ذخیره داده‌ها، نوار مغناطیسی یا رسانه‌های نوری، مانند دی وی دی‌ها، مناسب باشد. با استفاده از این اشکال ذخیره سازی، بازگرداندن داده‌ها از بایگانی می‌تواند فرآیند دشواری باشد. برای واحدهای کسب و کار که نیاز به یک روش ساده تر برای دسترسی به داده‌های بایگانی باید باشد، نوعی از فن آوری حالت جامد Solid-State یا درایو با قابلیت جاسازی Hot-Pluggable ممکن است راه بهتری باشد.

مهم نیست که سازمان برای اهداف بایگانی چه رسانه‌ای را انتخاب می‌کند، متخصصان امنیت باید هزینه‌های مکانیزم‌های مورد استفاده و امنیت بایگانی را در نظر بگیرند. ذخیره سازی داده‌های بایگانی شده در دی وی دی که توسط یک فایل قفل نشده پشتیبانی می‌شود ممکن است برای یک واحد کسب و کار راحت تر باشد، اما هیچ گونه حفاظتی از داده‌ها در دی وی دی را فراهم نمی‌کند. در این مورد، ممکن است یک متخصص امنیت نیاز داشته باشد تا با واحد کسب و کار فعالیت کند تا یک مکانیزم ذخیره سازی امن تر برای بایگانی داده‌ها بوجود آورد. هنگامی که داده‌ها به طور مرکزی توسط کارمندان IT یا مرکز داده، مدیریت می‌شوند، پرسنل معمولاً مسائل امنیتی مربوط به ذخیره داده‌ها را بهتر درک می‌کنند بنابراین ممکن است به راهنمایی‌های متخصصان امنیت احتیاج نداشته باشند.

• بازنمایی باقیمانده داده Data Remanence

بازنمایی باقیمانده از داده‌های دیجیتال است که حتی پس از تلاش برای حذف یا پاک کردن داده‌ها باقی می‌ماند. این امر می‌تواند وقتی سازمان از رسانه‌ها خارج شود، بازسازی داده‌ها انجام شود و در نتیجه افراد یا گروه‌های غیرمجاز به داده دسترسی پیدا کنند. رسانه‌هایی که متخصصان امنیت باید در نظر بگیرند عبارتند از هارد دیسک‌های مغناطیسی، درایوهای حالت جامد، نوارهای مغناطیسی و رسانه‌های نوری مانند CDها و دی وی دی‌ها هستند. با توجه به حفظ داده‌ها، متخصصان امنیت باید سه اقدام متقابل را درک کنند:

✓ تسویه *Clearing*: این شامل حذف داده‌ها از رسانه‌ها است، به طوری که داده‌ها را نمی‌توان با استفاده از تکنیک‌ها و ابزارهای نرم افزار بازیابی نرمال، بازسازی کرد. با استفاده از این روش، داده‌ها تنها با استفاده از تکنیک‌های قانونی ویژه قابل بازیابی می‌باشند.

✓ پاکسازی *Purging*: همچنین به آن تصفیه کردن (Sanitization) نیز گفته می‌شود، پاکسازی باعث می‌شود داده‌ها حتی با تکنیک‌های پیشرفته قانونی قابل خواندن نباشند. با استفاده از این تکنیک، داده‌ها باید غیرقابل برگشت باشند.

✓ تخریب *Destruction*: تخریب شامل از بین بردن رسانه‌ای است که در آن داده‌ها ساکن است. *Overwriting* یک تکنیک تخریب است که الگوهای داده را روی تمام رسانه‌ها می‌نویسد، در نتیجه هر ردیابی داده را حذف می‌کند. مغناطیس زدایی کردن یا همان *Degaussing*، یک روش تخریب می‌باشد که رسانه‌ها را در یک میدان مغناطیسی قوی و متناوب قرار داده و باعث از بین بردن هر گونه داده‌های قبلاً نوشته شده می‌شود و رسانه‌ها را در حالت مغناطیسی تصادفی (خالی) قرار می‌دهد. رمزگذاری داده‌ها را بر روی رسانه‌ها تقسیم کرده، بدین ترتیب بدون کلید رمزگذاری آن را غیرقابل خواندن می‌کند. تخریب فیزیکی شامل تجزیه فیزیکی رسانه‌ها یا تغییر شیمیایی آن است. برای رسانه‌های مغناطیسی، تخریب فیزیکی نیز ممکن است شامل قرار گرفتن در معرض دمای بالا باشد.

اکثر این اقدامات متقابل برای رسانه‌های مغناطیسی کار می‌کنند. با این حال، درایوهای حالت جامد، چالش‌های منحصر به فردی را ایجاد می‌کنند، زیرا نمی‌توانند رونویسی یا همان *Overwrite* شوند. بیشتر فروشندگان درایو حالت جامد دستورات *Sanitization* را ارائه می‌دهند که می‌توانند برای پاک کردن داده‌های موجود بر روی درایو استفاده شوند. متخصصان امنیت باید این دستورات را بررسی کرده تا اطمینان حاصل شود که موثر هستند. گزینه دیگری برای این درایوها پاک کردن کلید رمزنگاری *Cryptographic* است. اغلب ترکیب کاملی از این روش‌ها باید مورد استفاده قرار گیرد تا تضمین شود که داده‌ها حذف می‌شوند.

بازنمایی باقیمانده داده‌ها هنگام استفاده از هر راه حل مبتنی بر ابر *Cloud-based* برای یک سازمان نیز اهمیت دارد. متخصصان امنیت باید در مذاکره با هر قراردادی با یک ارائه دهنده مبتنی بر ابر همکاری کنند تا تضمین شود که این قرارداد مسائل مربوط به بازنمایی باقیمانده داده‌ها را پوشش می‌دهد، اگرچه تعیین اینکه اطلاعات به درستی حذف شده دشوار است. استفاده

از رمزگذاری داده‌ها یک راه عالی برای اطمینان از بازنمایی باقیمانده داده‌ها هنگام برخورد با ابر است.

• محدودیت مجموعه Collection Limitation

برای هر سازمان، محدودیت جمع آوری داده‌ها بر اساس فضای ذخیره سازی موجود وجود دارد. صاحبان سیستم‌ها و نگهبانان داده باید بر میزان فضای ذخیره سازی رایگان نظارت داشته باشند تا روند را درک کرده و بتوانند نیازهای آینده را قبل از وقوع بحران پیش بینی کنند. بدون نظارت مناسب، داده‌ها می‌توانند تا نقطه‌ای که عملکرد سیستم را تحت تاثیر قرار می‌دهد رشد کند. هیچ سازمانی نمی‌خواهد سیستم ذخیره سازی داده‌های حیاتی را خاموش کند، زیرا هیچ فضای آزادی در دسترس نیست. سهمیه‌های دیسک به ادمین‌ها اجازه می‌دهد محدودیت‌های فضای دیسک را برای کاربران تعیین کنند و سپس به طور خودکار بر استفاده از فضای دیسک نظارت کنند. در اکثر موارد، سهمیه بندی‌ها (Quotas) را می‌توان پیکربندی کرد و به کاربران اطلاع دهند تا در زمان نزدیک شدن به فضای محدود، به کاربران اطلاع دهند. متخصصان امنیت باید با مالکان سیستم و نگهبانان داده‌ها همکاری کنند تا تضمین شود که مکانیزم‌های نظارت و مکانیزم‌های هشدار مناسب تنظیم شده است. مالکان سیستم و نگهبانان داده می‌توانند در صورت نیازهای ذخیره سازی داده، تحریک پذیر باشند.

حفظ داده‌ها Data Retention

الزامات حفظ داده‌ها بر اساس چندین عامل، از جمله نوع داده، سن داده، و الزامات قانونی و مقررات متفاوت است. متخصصان امنیت باید درک کنند که داده‌ها در چه مکانی ذخیره می‌شود و چه نوع داده‌هایی ذخیره می‌شود. علاوه بر این، متخصصان امنیت باید راهنمایی در زمینه مدیریت و بایگانی داده‌ها را ارائه دهند. بنابراین، سیاست‌های حفظ داده‌ها باید با کمک پرسنل سازمانی ایجاد شود.

سیاست حفظ داده‌ها معمولا شامل هدف از سیاست، بخشی از سازمان تحت تاثیر سیاست، هر گونه استثناء در سیاست، پرسنل مسئول نظارت بر سیاست، پرسنل مسئول داده‌ها، انواع داده تحت پوشش این سیاست و همچنین برنامه نگهداری که متخصصان امنیت باید با صاحبان داده‌ها همکاری کند تا سیاست مناسب برای نگهداری داده‌ها را برای هر نوع داده‌ای که سازمان در

اختیار دارد، تهیه کنند. نمونه هایی از انواع داده به داده های منابع انسانی، داده های قابل پرداخت / دریافت، داده های فروش، داده های مشتری و ایمیل محدود نمی شوند.

برای طراحی سیاست های حفظ داده ها، سازمان باید به سوالات زیر پاسخ دهد:

- الزامات قانونی/ مقرراتی و نیازهای کسب و کار برای داده ها چیست؟
- انواع داده ها چیست؟
- دوره های نگهداری و نیازهای تخریب برای داده ها چیست؟

پرسنلی که با هر نوع داده آشنایی بیشتری دارند باید با متخصصان امنیت برای تعیین سیاست حفظ داده ها همکاری کنند. به عنوان مثال، پرسنل منابع انسانی باید به طراحی سیاست های حفظ داده ها برای کلیه داده های منابع انسانی کمک کنند. هنگام طراحی سیاست های حفظ داده ها، سازمان باید رسانه ها و سخت افزار هایی را که برای حفظ داده ها استفاده می شود، در نظر بگیرد. سپس، با در دست داشتن این داده ها، سازمان یا واحد کسب و کار باید سیاست های حفظ داده را تهیه و بطور رسمی اتخاذ نماید.

هنگامی که سیاست حفظ داده ایجاد شد، پرسنل باید آموزش ببینند تا این سیاست ها را رعایت کنند. ممیزی و نظارت باید به منظور اطمینان از انطباق با سیاست حفظ اطلاعات تنظیم شود. به طور دوره ای، صاحبان داده ها و پردازشگرها باید سیاست های حفظ داده ها را بررسی کرده تا تعیین شود آیا باید تغییراتی ایجاد شود یا خیر. تمام سیاست های حفظ داده ها، طرح های اجرایی، آموزش، و ممیزی باید کاملاً مستند شود.

به خاطر داشته باشید که در بیشتر سازمان ها، به دلیل انواع مختلف داده ها، یک راه حل مناسب برای همه داده ها وجود ندارد. تنها افرادی که بیشتر با هر نوع داده ای آشنا هستند می توانند بهترین سیاست حفظ داده های مربوطه را تعیین کنند. در حالی که یک متخصص امنیت باید در طراحی سیاست حفظ داده مشارکت داشته باشد، متخصصان امنیت برای اطمینان از این که امنیت داده ها همیشه در نظر گرفته می شود و سیاست های حفظ داده ها، نیازهای سازمانی را برآورده می کند، حضور دارند. متخصص امنیت باید تنها در نقش مشاور عمل کرده و در صورت لزوم باید تخصص های لازم را ارائه دهد.

کنترل ها و امنیت داده Data Security and Controls

اکنون زمان آن رسیده که درباره امنیت داده ها و کنترل هایی که سازمان ها باید به عنوان بخشی از یک طرح امنیتی جامع در نظر بگیرد بحث شود. متخصصان امنیت باید به عنوان بخشی از

امنیت داده ها، کنترل های زیر را درک کنند: امنیت داده، داده های در حالت استراحت، داده های در حال انتقال، دسترسی به داده ها و به اشتراک گذاری، مبانی اولیه (خط مبنا)، محدوده و اتصال، انتخاب استانداردها و رمزنگاری (Cryptography).

• امنیت داده ها Data Security

امنیت داده شامل رویه ها، فرآیندها و سیستم هایی است که داده ها را از دسترسی غیر مجاز محافظت می کنند. دسترسی غیر مجاز شامل دسترسی دیجیتال و فیزیکی غیر مجاز است. امنیت داده ها همچنین از داده ها در برابر هر گونه تهدیدی که می تواند محرمانه بودن داده ها، یکپارچگی یا دسترسی به داده ها را تحت تاثیر قرار دهد، محافظت می کند.

برای ارائه امنیت داده ها، باید با استفاده از یک استراتژی دفاع در عمق (Defense-in-Depth)، همانطور که در فصل ۱ بحث شد، امنیت را پیاده سازی کرد. اگر تنها یک لایه دسترسی تحلیل نشده باشد، امنیت داده ها در معرض ریسک قرار دارد. به عنوان مثال، می توانید مکانیزم های احراز هویت را اجرا کرده تا اطمینان حاصل شود که کاربران قبل از دسترسی به شبکه مورد احراز هویت قرار می گیرند. اما اگر کنترل های فیزیکی مناسب برای جلوگیری از دسترسی غیرمجاز به تاسیسات خود نداشته باشد، مهاجم فقط با اتصال یک دستگاه غیر مجاز به شبکه می تواند به راحتی به شبکه دسترسی پیدا کند.

متخصصان امنیت باید تضمین کنند که سازمان اقدامات و تهدیدات را برای هرگونه تهدیدی شناسایی کرده است. علاوه بر این، متخصصان امنیت باید هوشیار بوده و دائما مراقب تهدیدهای جدید باشند.

• داده در حالت استراحت Data at Rest

داده در حالت استراحت داده هایی هستند که در یک نقطه معین از زمان ذخیره می شوند و به طور فعال به کار نمی آیند. زمانی که داده ها در حالت استراحت هستند، متخصصان امنیت باید مطمئن باشند که محرمانه بودن، یکپارچگی و دسترسی داده ها تضمین شده است. محرمانه بودن را می توان با استفاده از رمزگذاری داده ها ارائه داد. یکپارچگی را می توان با اجرای مکانیزم های احراز هویت مناسب و ACL ها فراهم کرد تا فقط کاربرانی که مجاز هستند، بتوانند داده ها را ویرایش کنند. در دسترس بودن می تواند با اجرای یک راه حل ذخیره سازی تحمل خطا، مانند RAID قابل ارائه باشد.

• داده‌های در حال انتقال Data in Transit

داده‌های در حال انتقال داده‌هایی است که از طریق شبکه انتقال می‌یابد. در حالی که داده‌ها منتقل می‌شوند، متخصصان امنیت باید مطمئن شوند که محرمانه بودن، یکپارچگی و در دسترس بودن داده‌ها تضمین شده است. محرمانه بودن می‌تواند با استفاده از پیوند رمزگذاری یا رمزگذاری END TO END فراهم شود.

مانند داده‌های در حالت استراحت، احراز هویت و ACLها می‌توانند به یکپارچگی داده‌ها در هنگام انتقال کمک کنند. در دسترس بودن می‌تواند از طریق اجرای مزرعه‌های سرور Server Farms و ستون فقرات دوگانه Dual Backbones قابل دسترسی باشد.

• دسترسی به داده‌ها و به اشتراک گذاری Data Access and Sharing

پرسنل باید قادر به دسترسی و به اشتراک گذاری داده‌ها در وظایف روزمره خود باشند. این دسترسی زمانی شروع می‌شود که صاحب داده دسترسی کاربر را تأیید کند. نگهبان داده سپس مجوزهای مناسب برای داده‌ها را به کاربر می‌دهد. اما این دو مرحله ساده سازی فرآیند هستند. متخصصان امنیت باید تضمین کنند که سازمان موضوعاتی از قبیل موارد زیر را درک می‌کند:

- آیا سیاست‌های مناسب داده برای کنترل دسترسی و استفاده از داده‌ها وجود دارد؟
- آیا صاحبان داده نیازهای دسترسی کاربران را درک می‌کنند؟
- سطوح مختلف دسترسی مورد نیاز کاربران چیست؟
- کدام فرمت‌های داده را کاربران نیاز دارند؟
- آیا زیر مجموعه‌ای از داده‌ها وجود دارد که فقط باید دسترسی کاربران را محدود کند؟
- از داده‌های جمع آوری شده، آیا به طور واضح داده‌های خصوصی در مقابل داده‌های عمومی مشخص شده است؟
- آیا از داده‌ها در زمانی که در حالت استراحت هستند و زمانی که در حال انتقال هستند محافظت می‌شود؟
- آیا مسائل قانونی یا قضایی مربوط به مکان ذخیره داده، انتقال داده یا پردازش داده وجود دارد؟

زمانی که صاحبان داده‌ها و نگهبانان داده‌ها برای پاسخگویی به بسیاری از این سوالات با هم به طور مشترک کار می‌کنند، متخصصان امنیت باید در این مراحل آنها را هدایت کنند. اگر تصمیمی مبنی بر خودداری از داده‌ها گرفته شود، تصمیم‌گیری باید براساس محدودیت‌های حفظ حریم خصوصی، محرمانه بودن، امنیت یا محدودیت‌های قانونی و قضایی صورت گیرد. معیارهایی که این تصمیمات اتخاذ می‌شود باید به عنوان بخشی از یک سیاست رسمی ثبت شود.

• خط مبنا BASE LINE

یک عملی که می‌تواند حفظ امنیت را ساده تر کند، ایجاد و استقرار تصاویر استاندارد است که با استفاده از خطوط امنیتی ایمن شده اند. خط مبنا مجموعه‌ای از تنظیمات پیکربندی است که کف حداقل امنیت را در تصویر مستقر می‌کند. سازمانها باید خط مبنا را برای همه دستگاهها از جمله دستگاههای شبکه، رایانه‌ها، رایانه‌های میزبان و ماشینهای مجازی ضبط کنند. خط مبنا را می‌توان با استفاده از Group Policy در ویندوز کنترل کرد. این سیاست تنظیمات را می‌توان در تصویر ایجاد کرده و برای کاربران و رایانه‌ها اعمال شود. این تنظیمات به صورت دوره‌ای از طریق اتصال به یک کنترل کننده دامنه تجدید می‌شوند و توسط کاربر قابل تغییر نیست. همچنین این تصویر کاملاً رایج است که شامل جدیدترین بروزرسانی‌ها و پچ‌های سیستم عامل است.

وقتی یک شبکه از این نوع فناوری‌ها استفاده می‌کند، ادمین‌ها (Administrators) یک محیط عملیاتی استاندارد ایجاد کرده اند. از مزایای چنین محیطی رفتار مداوم شبکه و مسائل پشتیبانی ساده تر است. برای شناسایی تغییرات از پایه، باید اسکن‌های سیستم به صورت هفتگی انجام شود.

متخصصان امنیت باید در هدایت سازمان خود از طریق فرآیند ایجاد خطوط مبنا کمک کنند. اگر یک سازمان خط مبنای بسیار دقیقی را اجرا کند، سطح امنیتی بالاتری را ارائه می‌دهد که در واقع ممکن است بسیار محدود کننده باشد. اگر سازمانی یک خط مبنای خیلی ناچیز را اجرا کند، سطح امنیتی پایین تری را فراهم کرده که احتمالاً منجر به نقض امنیت خواهد شد. متخصصان امنیت باید تعادل بین حفاظت از دارایی‌های سازمانی و اجازه دسترسی به کاربران را درک کنند، و همچنین باید برای اطمینان از درک هر دو انتهای این طیف تلاش کنند.

• محدوده و تناسب Scoping and Tailoring

محدودیت و تناسب از نزدیک با خط مبنا گره خورده اند، به یک سازمان امکان می دهد تا تمرکز خود را برای شناسایی و رفع ریسک های مناسب محدود کند.

محدوده Scoping به یک سازمان در مورد چگونگی اعمال و اجرای کنترل های امنیتی دستور می دهد. کنترل های امنیتی خط مبنا، حداقل هایی هستند که مورد قبول سازمان است. هنگامی که کنترل های امنیتی بر اساس Scoping انتخاب می شوند، باید مستنداتی ایجاد شود که شامل کنترل های امنیتی در نظر گرفته شده، کنترل های امنیتی اتخاذ شده و ملاحظات صورت گرفته باشد.

تناسب Tailoring به یک سازمان امکان می دهد کنترل های امنیتی را با نیازهای سازمان از نزدیک تطبیق دهد. هنگامی که کنترل های امنیتی بر اساس Tailoring انتخاب می شوند، باید مستنداتی ایجاد شود که شامل کنترل های امنیتی در نظر گرفته شده باشد، و آیا کنترل های امنیتی اتخاذ شده اند و چگونه ملاحظات انجام شده است.

مؤسسه ملی استاندارد و فناوری (NIST) و انتشارات ویژه 800-53 (SP)، که به طور مختصر در فصل ۱ به آن پرداخته شده است، راهنمایی هایی در مورد Tailoring ارائه می دهد. Tailoring شامل چندین مرحله است، از جمله:

۱- کنترل های مشترک را مشخص و تعیین می کند Identify and designate common controls:

اگر یک سیستم اطلاعاتی یک کنترل مشترک مانند کنترل های محیطی را در یک مرکز داده به ارث ببرد، آن سیستم نیازی به اجرای صریح آن کنترل ندارد. تصمیمات سازمانی که در آن کنترل های امنیتی به عنوان کنترل های معمولی تعیین شده اند، ممکن است تا حد زیادی بر مسئولیت های مالکان سیستم های فردی در رابطه با اجرای کنترل ها در یک خط مبنای خاص تأثیر بگذارد.

۲- اعمال ملاحظات مربوط به محدوده کاری Apply scoping considerations:

در صورت استفاده از راهنمایی های مربوط به مدیریت ریسک، ملاحظات مربوط به بررسی محدودیت ها می توانند کنترل های امنیتی غیرضروری را از اولویت های اصلی کنترل امنیتی حذف کنند و تضمین کنند که سازمانها فقط آن دسته از کنترل های مورد نیاز را برای تأمین سطح مناسب حفاظت از سیستم های اطلاعاتی انتخاب می کنند. هنگامی که ملاحظات مربوط در

محدوده Scoping استفاده می‌شود، ممکن است برای تأمین وسایل جایگزین برای دستیابی به الزامات امنیتی، لازم باشد کنترل‌های جبرانی و غرامت انتخاب شود.

۳- خط مبنای مکمل Supplement baselines: کنترل‌های امنیتی اضافی و پیشرفت‌های کنترل در صورت نیاز برای رفع تهدیدات و آسیب پذیری‌های خاص انتخاب می‌شوند.

• انتخاب استاندارد

از آنجا که سازمان‌ها برای محافظت از دارایی‌های خود نیاز به راهنمایی دارند، متخصصان امنیت باید با معیارهایی که ایجاد شده اند آشنا باشند. سازمان‌های استاندارد بسیاری از جمله NIST، وزارت دفاع ایالات متحده (DoD) و سازمان بین‌المللی استاندارد سازی (ISO) تشکیل شده اند. استانداردهای NIST شامل استانداردهای پردازش اطلاعات فدرال Federal Information Processing Standards (FIPS) و انتشارات ویژه Special Publications (SP) است.

FIPS 199 معیارهایی را برای طبقه بندی امنیتی سیستم‌های اطلاعات فدرال تعیین می‌کند. نامگذاری FIPS 199 ممکن است به عنوان امتیاز کلی CIA باشد. این استاندارد دولتی ایالات متحده، مقوله‌های امنیتی سیستم‌های اطلاعاتی را که توسط دولت فدرال مورد استفاده قرار می‌گیرد، ایجاد می‌کند.

FIPS 199 به آژانس‌های فدرال نیاز دارد تا سیستم‌های اطلاعاتی خود را در هر یک از دسته‌های محرمانه بودن، یکپارچگی و در دسترس بودن ارزیابی کرده و هر سیستم را به عنوان کم، متوسط یا زیاد در هر دسته ارزیابی کند. دسته بندی امنیتی کلی سیستم اطلاعات بالاترین امتیاز از هر گروه است.

اگر انتظار می‌رود که از دست دادن هر اصطلاح CIA تأثیر منفی محدود بر عملیات سازمانی، دارایی‌های سازمانی یا افراد داشته باشد، تأثیر بالقوه کم می‌باشد. اگر سازمان قادر به انجام وظیفه اصلی خود باشد اما نه به اندازه‌ی عادی این اتفاق می‌افتد. این دسته فقط شامل خسارت محدود، خسارت مالی یا آسیب می‌شود.

اگر انتظار می‌رود از دست دادن هرگونه اصطلاح CIA تأثیر منفی جدی بر عملیات سازمانی، دارایی‌های سازمانی یا افراد بگذارد، تأثیر بالقوه متوسط است. این اتفاق زمانی می‌افتد که اثربخشی سازمان که قادر به انجام عملکرد اصلی خود است بطور قابل توجهی کاهش یابد. این دسته شامل خسارت زیاد، ضرر مالی یا آسیب می‌شود.

اگر انتظار می رود از دست دادن هرگونه اصطلاح CIA تأثیر منفی فاجعه آمیزی بر عملکردهای سازمانی، داراییهای سازمانی یا افراد داشته باشد، تأثیر بالقوه زیاد است. این اتفاق زمانی می افتد که یک سازمان قادر به انجام یک یا چند وظیفه اصلی خود نباشد. این دسته شامل خسارت های شدید، خسارت مالی یا آسیب شدید است.

FIPS 199 نمودار مفیدی را ارائه می دهد که سطح CIA را برای دارایی های اطلاعاتی رتبه بندی می کند، همانطور که در جدول ۲-۲ نشان داده شده است.

CIA Tenet	Low	Moderate	High
Confidentiality	Unauthorized disclosure will have limited adverse effect on the organization.	Unauthorized disclosure will have serious adverse effect on the organization.	Unauthorized disclosure will have severe adverse effect on the organization.
Integrity	Unauthorized modification will have limited adverse effect on the organization.	Unauthorized modification will have serious adverse effect on the organization.	Unauthorized modification will have severe adverse effect on the organization.
Availability	Unavailability will have limited adverse effect on the organization.	Unavailability will have serious adverse effect on the organization.	Unavailability will have severe adverse effect on the organization.

جدول ۲-۲: محرمانه بودن، یکپارچگی و تعاریف تأثیر بالقوه در دسترس بودن

همچنین مهم است که متخصصان و سازمانهای امنیتی طبقه بندی اطلاعات و چرخه عمر را درک کنند. طبقه بندی بستگی به اینکه این سازمان تجارت کسب و کار است یا یک نهاد نظامی / دولتی متفاوت است.

مطابق جدول ۲-۲، FIPS 199 سه تأثیر (پایین، متوسط و زیاد) را برای سه اصول امنیتی تعریف می کند. اما سطوحی که به نهادهای سازمانی اختصاص می یابد باید توسط سازمان تعریف شود زیرا فقط سازمان می تواند تعیین کند که آیا ضرر خاص محدود، جدی یا شدید است.

با توجه به FIPS 199، دسته امنیتی SC یک نهاد شناسایی شده سه اصطلاح را با ارزش های خود برای یک نهاد سازمانی بیان می کند. سپس مقادیر برای تعیین اینکه کدام کنترل های امنیتی باید اجرا شوند استفاده می شود. اگر یک دارایی خاص از اشخاص مختلف تشکیل شده است، باید SC را برای آن دارایی بر اساس واحدهای تشکیل دهنده آن محاسبه کرد. FIPS 199 همانطور که در اینجا نشان داده شده است، نامی را برای بیان این مقادیر ارائه می دهد:

نوع اطلاعات SC = {(محرمانه بودن، تأثیرگذاری)، (یکپارچگی، تأثیرگذاری)، (در دسترس بودن، تأثیرگذاری)} بیاپید مثالی از این نامگذاری را در یک مثال در دنیای واقعی بررسی کنیم:

سایت عمومی SC = {(محرمانه، کم)، (صداقت، متوسط)، (در دسترس بودن، زیاد)}

سایت شریک SC = {(محرمانه، متوسط)، (صداقت، بالا)، (در دسترس بودن، متوسط)}

سایت داخلی SC = {(محرمانه، زیاد)، (صداقت، متوسط)، (در دسترس بودن، متوسط)}

حال فرض کنیم همه سایتها در همان سرور وب مستقر هستند. برای تعیین نامگذاری سرور وب، باید از بالاترین مقادیر هر یک از دسته ها استفاده کنید:

سرور وب SC = {(محرمانه، زیاد)، (صداقت، بالا)، (در دسترس بودن، زیاد)}

برخی از سازمانها ممکن است تصمیم بگیرند که سایت عمومی را روی یک وب سرور قرار دهند و سایت شریک و سایت داخلی را در یک وب سرور دیگر تفکیک کنند. در این حالت، وب سرور عمومی به همه کنترل‌های امنیتی یکسان احتیاج ندارد و به صرفه تر از آن برای اجرای شریک / وب سرور داخلی می‌باشد.

دستورالعمل DoD ۸۵۱۰,۰۱ ایالات متحده یک پروسه صدور گواهینامه و اعتباربخشی را برای سیستمهای اطلاعاتی وزارت دفاع ایجاد می‌کند که می‌توان آن را در اینجا یافت.

http://www.dtic.mil/whs/directives/corres/pdf/851001_2014.pdf.

سازمان ISO با کمیسیون بین المللی الکتروتکنیک IEC همکاری می‌کند تا استانداردهای زیادی را در مورد امنیت اطلاعات برقرار کند. استانداردهای ISO / IEC که متخصصان امنیت باید درک کنند در فصل ۱ بررسی شد.

متخصصان امنیت همچنین ممکن است نیاز به تحقیق در مورد سایر معیارها از جمله استانداردهای آژانس امنیت شبکه جهانی و اطلاعات اروپا یا همان European Network and Information Security Agency (ENISA)، اتحادیه اروپا European Union (EU) و آژانس امنیت ملی ایالات متحده National Security Agency (NSA) داشته باشند. مهم این است که سازمان بسیاری از استانداردهای موجود را مورد تحقیق قرار داده و براساس نیاز سازمان سودمندترین دستورالعمل‌ها را بکار گیرد.

• رمزنگاری Cryptography

Cryptography، که به آن رمزگذاری (Encryption) نیز گفته می شود، می تواند براساس سطح ارتباطی که استفاده می شود، محافظت متفاوتی را ارائه دهد. دو نوع سطح ارتباط رمزگذاری، رمزگذاری پیوند Link Encryption و رمزنگاری پایان به پایان End-to-End است.

✓ رمزگذاری پیوند Link Encryption

تمام داده هایی را که از طریق لینک یا پیوند منتقل می شوند را رمزگذاری می کند. در این نوع ارتباطات، تنها قسمت بسته که رمزگذاری نشده است، اطلاعات کنترل پیوند داده ها است که برای اطمینان از انتقال صحیح داده ها، لازم است. تمام اطلاعات رمزگذاری می شوند، با استفاده از هر روتر یا دستگاه دیگر، اطلاعات هدر آن رمزگشایی می شود تا بتواند مسیریابی رخ دهد و قبل از ارسال اطلاعات به دستگاه بعدی دوباره رمزگذاری شود.

اگر طرف ارسال کننده تضمین کند که امنیت داده و حفظ حریم خصوصی از طریق یک اتصال عمومی حفظ می شود، باید از رمزگذاری پیوند استفاده شود. این اغلب روشی است که برای محافظت از ارتباطات ایمیلی استفاده می شود یا وقتی بانک ها یا موسسات دیگری که داده های محرمانه دارند باید آن داده ها را از طریق اینترنت ارسال کنند.

رمزگذاری پیوند در برابر بسته اسنیفرها Packet Sniffers و سایر اشکال استراق سمع محافظت شده و در لایه پیوند داده ها و لایه فیزیکی مدل OSI رخ می دهد. مزایای رمزگذاری پیوند شامل: کلیه داده های رمزگذاری می شوند و هیچ گونه تعامل کاربر برای استفاده لازم نیست. معایب رمزگذاری لینک شامل موارد زیر است: هر دستگاهی که داده ها باید از طریق آن منتقل شوند باید کلید (key) را دریافت کنند، تغییرات کلید باید به هر دستگاه در مسیر منتقل شوند و بسته ها در هر دستگاه رمزگشایی شوند.

✓ رمزگذاری پایان به پایان End-to-End Encryption

رمزگذاری End-to-End اطلاعات بسته، رمزگذاری کمتری نسبت به رمزگذاری پیوند می شود. در رمزگذاری End-to-End، اطلاعات مسیریابی بسته و همچنین هدرها و آدرس های مربوط به آن رمزگذاری نمی شوند. این امر به هکرهای بالقوه امکان می دهد اگر یک بسته را از طریق Sniffing یا استراق سمع بدست آورند، اطلاعات بیشتری کسب کنند.

رمزگذاری End-to-End چندین مزیت دارد. کاربر معمولاً رمزنگاری End-to-End را آغاز می‌کند، که به کاربر اجازه می‌دهد دقیقاً چه رمزگذاری و چگونه رمزگذاری را انتخاب کند. این عملکرد هر دستگاه در طول مسیر کمتر از رمزگذاری پیوند را تحت تأثیر قرار می‌دهد زیرا هر دستگاه برای تعیین نحوه مسیری بسته‌بندی به انجام رمزگذاری / رمزگشایی (encryption/decryption) ندارد.

الزامات مدیریت دارایی Asset Handling Requirements

سازمان‌ها باید برای محافظت از دارایی‌های خود، الزامات مناسب مدیریت دارایی‌ها را تعیین کنند. به عنوان بخشی از این الزامات رسیدگی، به پرسنل آموزش داده می‌شود که چگونه می‌توانند مارک، برچسب گذاری، ذخیره و نابودی یا دفع رسانه را علامت گذاری کنند.

علامت گذاری، برچسب زدن و ذخیره سازی Marking, Labeling, and Storing

به طور ساده تمام انواع رسانه‌های ذخیره سازی (نوار tapes، لنز optical و غیره) را برچسب زده و با خیال راحت ذخیره شود. برخی از دستورالعمل‌ها در زمینه کنترل رسانه‌ها:

- با دقت و به موقع تمام رسانه‌های ذخیره داده علامت گذاری شود.
- اطمینان از ذخیره سازی مناسب محیط رسانه‌ها.
- برخورداری از امنیت و اداره رسانه‌ها تضمین شود.
- log رسانه داده برای ارائه یک کنترل موجودی فیزیکی.

محیطی که رسانه در آن ذخیره خواهد شد نیز دارای اهمیت است. به عنوان مثال، آسیب به رسانه مغناطیسی بالاتر از ۱۰۰ درجه شروع می‌شود. Forest Green Book یک کتاب سری Rainbow است که قابلیت استفاده امن از حافظه سیستم اطلاعات خودکار و حساس طبقه بندی شده و رسانه‌های ذخیره سازی ثانویه مانند دزدگیرها، نوارهای مغناطیسی، هارد دیسک‌ها، فلاپی دیسک‌ها و کارت‌ها را تعریف می‌کند. Rainbow با جزئیات بیشتر در فصل ۳ بحث خواهد شد.

تخریب Destruction

در حین دفع رسانه، باید مطمئن شد که هیچ داده‌ای روی رسانه‌ها باقی نمی‌ماند. مطمئن ترین وسیله برای حذف داده‌ها از رسانه‌های ذخیره سازی مغناطیسی، مانند نوار کاست مغناطیسی، از طریق فرسایش یا همان مغناطیس زدایی است که رسانه‌ها را در معرض یک میدان مغناطیسی

قدرتمند و متناوب قرار می دهد. این داده های قبلی را که قبلاً نوشته شده است حذف می کند و رسانه ها را در حالت تصادفی (Rnandom) در مغناطیسی (خالی یا Blank) قرار می دهد.

فصل ۳

مهندسی امنیت
(Security Engineering)

این فصل مباحث زیر را در بر می گیرد:

- ❖ مهندسی با استفاده از اصول طراحی امن: مفاهیم مورد بحث شامل استانداردهای مهندسی سیستم های NIST 800-27, ISO/IEC 15288:2015 می باشد.
- ❖ مفاهیم مدل امنیتی: مفاهیم مورد بحث شامل حالت های امنیتی، دفاع در عمق، انواع مدل های امنیتی، مدل های امنیتی، مراحل معماری سیستم، ISO/IEC 42010:2011، بسترهای رایانشی، خدمات امنیتی، مولفه های سیستم و دستگاه های ورودی / خروجی است.
- ❖ مدل های ارزیابی امنیت سیستم: مفاهیم مورد بحث شامل ITSEC, TCSEC، معیارهای مشترک، استانداردهای اجرای امنیت و کنترلها و اقدامات متقابل می باشد.
- ❖ قابلیت های امنیتی سیستم های اطلاعاتی: مفاهیم مورد بحث شامل حفاظت از حافظه، مجازی سازی، ماژول سیستم عامل قابل اعتماد، واسطها و تحمل خطا است.
- ❖ صدور گواهی نامه و اعتبارسنجی: مفاهیم مورد بحث شامل صدور گواهی نامه، اعتبارسنجی و مراحل اعتبارسنجی است.
- ❖ تعمیر و نگهداری معماری امنیتی: در مورد حفظ معماری امنیتی بحث می کند.
- ❖ آسیب پذیری های معماری امنیتی، طرح ها و راه حل عناصر: مفاهیم مورد بحث شامل مشتری، سرور، امنیت پایگاه داده، سیستم های توزیع شده، سیستم داده های موازی بزرگ مقیاس، سیستم های رمزنگاری و سیستم های کنترل صنعتی می باشد.
- ❖ آسیب پذیری در سیستم های مبتنی بر وب: مفاهیم مورد بحث شامل تله های تعمیر و نگهداری، حملات بررسی زمان / زمان استفاده، حملات مبتنی بر وب، XML, SAML و OWASP است.
- ❖ آسیب پذیری در سیستم های سیار: آسیب پذیری های موجود در هنگام استفاده از سیستم های سیار را پوشش می دهد.
- ❖ آسیب پذیری در دستگاه های تعبیه شده (Embedded) و سیستم های سایبر- فیزیکی: مواردی را که در حال حاضر با پیشرفت ارتباطات ماشین به ماشین و اینترنت اشیا مشاهده می شود، توضیح می دهد.
- ❖ رمزنگاری: مفاهیم مورد بحث شامل مفاهیم رمزنگاری، چرخه عمر رمزنگاری، تاریخ رمزنگاری، ویژگی های رمزنگاری و مدیریت کلید می باشد.

- ❖ انواع رمزنگاری: مفاهیم مورد بحث شامل رمزگذاری کلید و پنهان کردن، رمزهای جایگزینی، رمزهای انتقال، الگوریتمهای متقارن، الگوریتمهای نامتقارن و رمزهای هیبریدی است.
- ❖ الگوریتمهای متقارن: مفاهیم مورد بحث شامل استاندارد رمزگذاری دیجیتال و استاندارد رمزگذاری اطلاعات سه گانه (Triple)، استاندارد رمزگذاری پیشرفته، IDEA، Skipjack، Blowfish، Twofish، RC5، RC6، RC4، CAST می باشد.
- ❖ الگوریتمهای نامتقارن: مفاهیم مورد بحث شامل El Gamal، RSA، Diffie-Hellman، Knapsack، ECC، اثبات دانش صفر است.
- ❖ زیرساخت کلید عمومی: مفاهیم مورد بحث شامل CA، OCSP، گواهینامه ها، CRL، مراحل PKI و گواهینامه متقابل است.
- ❖ روشهای اصلی مدیریت: روشهای اصلی مدیریتی را که سازمانها باید درک کنند را توضیح می دهد.
- ❖ امضاهای دیجیتال: استفاده از امضاهای دیجیتالی را پوشش می دهد.
- ❖ مدیریت حقوق دیجیتال: مدیریت حقوق دیجیتال را توضیح می دهد.
- ❖ یکپارچگی پیام: مفاهیم مورد بحث شامل هش کردن، کد تأیید صحت پیام و salting است.
- ❖ حملات Cryptanalytic مفاهیم مورد بحث شامل حمله به تنها متن رمزگذاری شده، حمله به متن ساده شناخته شده، حمله به متن ساده انتخاب شده، حمله به متن رمزگذاری شده، مهندسی اجتماعی، نیروی بی رحمانه (Brute force)، تشخیص رمزنگاری، رمزنگاری خطی، حمله جبری، تجزیه و تحلیل فرکانس، حمله Birthday، حمله فرهنگ لغت (dictionary)، حمله مجدد، حمله تحلیلی، حمله آماری، حمله فاکتورسازی، مهندسی معکوس و حمله Meet-In-The-Middle.
- ❖ تهدیدات جغرافیایی: مفاهیم مورد بحث شامل تهدیدهای داخلی در مقابل تهدیدهای خارجی، تهدیدهای طبیعی، تهدیدات سیستم، تهدیدهای ناشی از انسان و تهدیدهای سیاسی می باشد.
- ❖ طراحی سایت و تاسیسات: مفاهیم مورد بحث شامل یک الگوی دفاعی لایه ای، CPTED، طرح (Plan) امنیت فیزیکی و موضوعات انتخاب تاسیسات است.

- ❖ ساختمان و امنیت داخلی: مفاهیم مورد بحث شامل درب، قفل، بیومتریک، ورودی‌های شیشه ای، کنترل بازدید کننده، اتاق‌های تجهیزات و مناطق کار می‌باشد.
- ❖ امنیت محیطی: مفاهیم مورد بحث شامل حفاظت از آتش سوزی، منبع تغذیه، HVAC، نشت آب و جاری شدن سیل و هشدارهای محیطی است.
- ❖ امنیت تجهیزات: مفاهیم مورد بحث شامل رویه یا پروسه شرکت‌ها و گاو صندوق‌ها، طاق‌ها و قفل است.

مهندسی امنیت عمدتاً به طراحی، پیاده سازی، نظارت و تأمین دارایی‌های امنیت اطلاعات توجه دارد. این دارایی‌ها شامل رایانه، تجهیزات، شبکه‌ها و اپلیکیشن‌ها هستند. در این منطقه، یک متخصص امنیت باید مدل‌های امنیتی، آسیب پذیری سیستم، رمزنگاری و امنیت فیزیکی را درک کند. اما درک ساده مهندسی امنیت کافی نیست. یک متخصص امنیت باید بداند که چگونه مهندسی امنیت را پیاده سازی کند تا از دارایی‌های محافظت شده مطمئن شود. سازمان‌ها باید آنچه را که برای تأمین امنیت نیاز دارند بدانند، که چرا باید امنیت را تأمین کنند، و چگونه می‌توان امنیت را تأمین کرد.

مهندسی با استفاده از اصول طراحی امن Engineering Using Secure Design Principles

مهندسی سیستم رویکردی برای طراحی، تحقق، مدیریت فنی، عملیات و بازنشستگی یک سیستم است. به طور کلی، سیستم مجموعه‌ای از عناصر است که در کنار هم نتیجه‌ای حاصل می‌کنند که توسط عناصر به تنهایی حاصل نمی‌شود. به طور خاص در فناوری اطلاعات، یک سیستم ممکن است شامل یک یا چند رایانه یا دستگاهی باشد که برای دستیابی به یک نتیجه خاص با یکدیگر فعالیت می‌کنند. به عنوان مثال، یک سیستم سفارش آنلاین می‌تواند شامل یک وب سرور، یک سرور تجارت الکترونیکی و یک سرور پایگاه داده باشد. با این حال، این سیستم‌ها به تنهایی نمی‌توانند امنیت کافی برای معاملات آنلاین را فراهم کنند. یک سازمان ممکن است نیاز به روترها، فایروال‌ها و سایر مکانیسم‌های امنیتی را داشته باشد تا اطمینان حاصل شود. امنیت در کل، راه حل‌های طراحی ادغام شده است.

سازمانها باید با استفاده از اصول طراحی امن، فرآیندهای مهندسی سیستم را پیاده سازی و مدیریت کنند. مهندسی سیستم معمولاً بر اساس چرخه عمر مدل سازی می‌شود. فصل ۱، "امنیت و مدیریت ریسک" درباره دو گروه بحث می‌کند که استانداردها را تعیین می‌کنند: سازمان

بین المللی برای استاندارد ISO کمیسیون بین المللی الکتروتکنیک IEC و مؤسسه ملی استاندارد و فناوری NIST. این گروه‌ها دارای استاندارد هایی برای مهندسی سیستم هستند: ISO/IEC 15288:2015, NIST 800-27

ISO/IEC 15288:2015 چهار دسته از فرآیندها را تعیین می‌کند:

- فرآیندهای توافق Agreement Processes: این دسته شامل اکتساب و عرضه است.
 - فرآیندهای توانمندسازی پروژه‌های سازمانی Organizational Project-Enabling Processes: این گروه شامل مدیریت زیرساخت‌ها، مدیریت کیفیت و مدیریت دانش است.
 - فرآیندهای مدیریت فنی Technical Management Processes: این دسته شامل برنامه ریزی پروژه، مدیریت ریسک، مدیریت پیکربندی و تضمین کیفیت است.
 - فرآیندهای فنی Technical Processes: این دسته شامل تعریف الزامات سیستم، تجزیه و تحلیل سیستم، اجرا، ادغام، بهره برداری، نگهداری و دفع می‌باشد.
- مراحل چرخه عمر سیستم‌های این استاندارد شامل مفهوم، توسعه، تولید، استفاده، پشتیبانی و بازنشستگی (concept, development, production, utilization, support, retirement) است. در حالی که این استاندارد فرآیندهای چرخه عمر سیستم را تعریف می‌کند و به خودی خود امنیت در طی مهندسی سیستم ایجاد نمی‌شود.
- NIST 800-27 Rev A اصول و شیوه‌های مربوط به امنیت سیستم‌های IT را ارائه می‌دهد. این پنج مرحله از برنامه ریزی چرخه عمر تعریف شده در NIST SP 800-14 استفاده می‌شود:
- ۱- شروع Initiation: اهداف سیستم را مستند می‌کند.
 - ۲- توسعه / اکتساب Development/Acquisition: سیستم را طراحی یا خریداری می‌کند.
 - ۳- پیاده سازی Implementation: سیستم را نصب و آزمایش می‌کند.
 - ۴- بهره برداری / نگهداری Operation/Maintenance: خدمات سیستم را ارائه می‌دهد و سیستم را در صورت لزوم حفظ می‌کند.
 - ۵- دفع Disposal: سیستم را از فعالیت خارج می‌کند.

NIST 800-27 Rev A، ۳۳ اصل امنیت فناوری اطلاعات را در ۶ گروه قرار داده است:

- اصول بنیاد امنیتی Security foundation principles:
- یک سیاست امنیتی صحیح را به عنوان پایه و اساس طراحی تنظیم کنید.

- با امنیت به عنوان بخشی تفکیک ناپذیر از طراحی کلی سیستم رفتار کنید.
- به وضوح مرزهای امنیتی فیزیکی و منطقی حاکم بر سیاستهای امنیتی مرتبط را مشخص کنید.
- مطمئن شوید که توسعه دهندگان در مورد چگونگی توسعه نرم افزار امن آموزش دیده‌اند.

• اصول مبتنی بر ریسک Risk-based principles :

- ریسک را تا حد قابل قبول کاهش دهید.
- فرض کنید سیستمهای خارجی ناامن هستند.
- معاملات بالقوه بین کاهش ریسک و افزایش هزینه و کاهش در سایر جنبه‌های اثربخشی عملیاتی را شناسایی کنید.
- اقدامات امنیتی سیستم متناسب با رسیدن به اهداف امنیتی سازمانی را پیاده سازی کنید.
- هنگام پردازش، هنگام انتقال و ذخیره سازی از اطلاعات محافظت کنید.
- برای دستیابی به امنیت کافی، محصولات سفارشی (Custom Product) را در نظر بگیرید.
- از همه کلاسهای احتمالی حملات محافظت کنید.

• اصول سهولت استفاده Ease of use principles :

- در صورت امکان، امنیت را بر اساس استانداردهای باز برای قابلیت حمل و قابلیت عملیاتی بودن انجام دهید.
- در توسعه الزامات امنیتی از زبان مشترک استفاده کنید.
- طراحی امنیت برای اتخاذ منظم فناوری جدید، از جمله فرآیند ارتقاء فناوری مطمئن و منطقی.
- برای سهولت عملکرد تلاش کنید.

• افزایش اصول انعطاف پذیری Increase Resilience Principles :

- اجرای امنیت لایه ای. (هیچ نقطه آسیب پذیری را تضمین نکنید).

- یک سیستم IT را برای محدود کردن آسیب و انعطاف پذیری در هنگام واکنش، طراحی و راه اندازی کنید.
- مطمئن شوید که این سیستم در مقابل تهدیدات مورد انتظار، انعطاف پذیر است.
- محدودکردن نقاطی که حاوی آسیب پذیری هایی می باشد.
- سیستم های دسترسی عمومی را از منابع مهم مأموریت تفکیک کنید. (به عنوان مثال، داده ها، فرآیندها)
- از مکانیسم های مرزی برای جدا کردن سیستم های محاسباتی و زیرساخت های شبکه استفاده کنید.
- مکانیسم های ممیزی را برای کشف استفاده غیرمجاز و پشتیبانی از تحقیقات حوادث طراحی و پیاده سازی کنید.
- برای اطمینان از در دسترس بودن مناسب، روش های احیای شرایط و اضطراب یا حوادث را توسعه داده و استفاده کنید.

• **اصول آسیب پذیری را کاهش دهید Reduce vulnerabilities principles:**

- برای سادگی تلاش کنید.
- عناصر سیستم مورد اعتماد را به حداقل برسانید.
- اجرای حداقل امتیاز.
- مکانیسم های امنیتی غیر ضروری را اجرا نکنید.
- اطمینان از امنیت مناسب در خاموشی سیستم یا دفع سیستم.
- خطاها و آسیب پذیریهای رایج را شناسایی و از آنها جلوگیری کنید.

• **طراحی شبکه با اصول ذهنی Design with network in mind principles:**

- امنیت را از طریق ترکیبی از اقدامات توزیع شده از نظر فیزیکی و منطقی پیاده سازی کنید.
- تدابیر امنیتی را برای پرداختن به چندین دامنه اطلاعات با هم تنظیم کنید.
- تأیید اعتبار کاربران و فرایندها برای اطمینان از تصمیمات مناسب کنترل دسترسی در داخل دامنه و در سراسر دامنه
- برای اطمینان در مسئولیت از هویت های منحصر به فرد استفاده کنید.

برای خواندن همه مطالب درباره NIST 800-27 Rev A به لینک زیر مراجعه کنید.
<http://csrc.nist.gov/publications/nistpubs/http://csrc.nist.gov/publications/nistpubs/80027A/SP800-27-RevA.pdf..>

مفاهیم مدل امنیتی Security Model Concepts

اقدامات امنیتی باید هدف مشخصی داشته باشد تا تضمین شود که این اقدامات موفقیت آمیز است. تمام اقدامات به گونه‌ای طراحی شده اند که یکی از مجموعه‌های اصلی حفاظت را ارائه دهند. در این بخش، سه اصل اساسی امنیت مورد بحث قرار گرفته است. همچنین رویکردی برای تحقق این اهداف پوشش داده شده است. علاوه بر این، انواع مدل‌های امنیتی، حالت‌های امنیتی و معماری سیستم را پوشش می‌دهد. سرانجام، سیستم عامل، سیستم عامل‌های محاسباتی، خدمات امنیتی، اجزای سیستم و دستگاه‌های ورودی / خروجی را در بر می‌گیرد.

محرمانه بودن، یکپارچگی و در دسترس بودن Confidentiality, Integrity, Availability

محرمانه بودن اینگونه می‌باشد که داده‌ها را نمی‌توان از طریق کنترل دسترسی و رمزگذاری داده‌ها خواند زیرا در هارد دیسک از طریق رمزگذاری، انتقال داده‌ها امکان پذیر نیست. با توجه به امنیت اطلاعات، محرمانه بودن مخالف افشای اطلاعات است. اصول امنیتی اساسی محرمانه بودن، یکپارچگی و در دسترس بودن به (سه گانه محرمانه بودن، یکپارچگی و در دسترس بودن) CIA) گفته می‌شود.

اگر اطمینان داشته باشید که داده‌ها به هیچ وجه تغییر نکرده است، یکپارچگی ارائه می‌شود، و به طور معمول با یک الگوریتم هشینگ یا Checksum ارائه می‌شود. هر دو روش عددی را ایجاد می‌کنند که به همراه داده ارسال می‌شود. با رسیدن داده به مقصد، می‌توان از این عدد برای تعیین اینکه آیا یک بیت واحد نیز در محاسبه مقدار هش از داده‌های دریافت شده تغییر کرده است، استفاده کرد. یکپارچگی کمک می‌کند تا از داده‌ها در برابر فساد کشف نشده محافظت شود.

برخی از اهداف یکپارچگی اضافی به صورت زیر می‌باشد:

- ✓ جلوگیری از ایجاد تغییرات در کاربران غیرمجاز
- ✓ حفظ تداوم داخلی و خارجی
- ✓ جلوگیری کاربران مجاز از ایجاد تغییرات نادرست

در دسترس بودن توصیف می‌کند که چه درصدی از زمان، منبع یا داده‌ها در دسترس است. این معمولاً به عنوان درصدی از زمان تا ۹۹,۹٪ نشانگر دسترسی بیشتر از زمان ۹۹٪ زمان اندازه گیری است. اطمینان از اینکه داده‌ها در چه زمانی قابل دسترسی است و در کجا، یک هدف اصلی امنیت است.

حالت‌های امنیتی Security Modes

یک سیستم کنترل دسترسی اجباری (Mandatory Access Control (MAC بر اساس متغیرهایی از قبیل حساسیت داده‌ها، میزان مجوز کاربر و اقدامات کاربر مجاز در حالت‌های مختلف امنیتی در زمان‌های مختلف است. در این بخش توضیحات مربوط به این حالت‌ها ارائه شده است.

حالت امنیتی اختصاصی Dedicated Security Mode

اگر یک سیستم طبقه بندی منفرد داشته باشد، سیستم در حالت امنیتی اختصاصی کار می‌کند. در این سیستم، کلید کاربران می‌توانند به کلید داده‌ها دسترسی پیدا کنند، اما باید توافق نامه عدم افشای (NDA) را امضا کنند و برای دسترسی بر اساس نیاز به دانستن Need-to-Know، رسماً تأیید شوند.

حالت امنیت بالای System High Security Mode

در سیستمی که در حالت امنیت بالا کار می‌کند، کلید کاربران دارای همان ضریب امنیتی (مانند مدل امنیتی اختصاصی) هستند، اما همه آنها نیاز به دانستن تمام اطلاعات موجود در سیستم نیستند. در نتیجه، اگرچه کاربر ممکن است دسترسی به یک شیء را داشته باشد، اما اگر مجوز لازم برای دانستن موضوع را نداشته باشد، محدود می‌شود.

حالت امنیتی تقسیم شده Compartmented Security Mode

در سیستم حالت امنیتی تقسیم شده، کلید کاربران باید دارای بالاترین میزان مجوز امنیتی باشند (اختصاصی و امنیت بالای سیستم)، اما همچنین باید دارای مجوز معتبر برای نیاز به دانستن، NDA امضا شده و تأیید رسمی برای کلید اطلاعات باشند، که به آنها دسترسی دارند. هدف این

است که تضمین شود که حداقل تعداد افراد ممکن به هر سطح یا محفظه به اطلاعات دسترسی دارند.

حالت امنیتی چند سطحی Multilevel Security Mode

هنگامی که یک سیستم اجازه می‌دهد دو یا چند سطح طبقه بندی اطلاعات به طور همزمان پردازش شود، گفته می‌شود که در حالت امنیتی چند سطحی کار می‌کند. کاربران برای داشتن کلیه اطلاعات موجود در سیستم باید دارای NDA امضا شده باشند و براساس سطح مجوز تاییدیه دسترسی، دسترسی رسمی به زیر مجموعه‌ها داشته باشند. این سیستم‌ها بیشترین ریسک را شامل می‌شوند زیرا اطلاعات در بیش از یک سطح از امنیت پردازش می‌شوند، حتی وقتی که همه کاربران سیستم دارای مجوزهای مناسب یا نیاز به دانستن کلیه اطلاعات پردازش شده توسط سیستم نداشته باشند. به این حالت گاهی اوقات حالت کنترل امنیتی نیز گفته می‌شود. در جدول ۱-۳ چهار حالت امنیتی و الزامات آنها مقایسه شده است.

	Signed NDA	Proper Clearance	Formal Approval	Valid Need-to-Know
Dedicated	All information	All information	All information	All information
System high	All information	All information	All information	Some information
Compartmented	All information	All information	Some information	Some information
Multilevel	All information	Some information	Some information	Some information

جدول ۱-۳: خلاصه حالت‌های امنیتی

تضمین Assurance

در حالی که یک سطح اطمینان، محافظت‌هایی را که می‌توان از یک سیستم انتظار داشت، توصیف می‌کند، تضمین به سطح اطمینان خاطر نشان می‌کند که محافظت‌ها طبق برنامه ریزی عمل خواهند کرد. به طور معمول، با اختصاص دادن نظارت بیشتر به امنیت در فرآیند طراحی، سطح تضمین بالاتری حاصل می‌شود. بخش "مدل‌های ارزیابی امنیت سیستم"، در ادامه در این

فصل، روش‌های مختلف سیستم‌های رتبه بندی و درجه بندی برای سطح اطمینان و تضمین را مورد بحث قرار می‌دهد.

دفاع در عمق Defense in Depth

مدیریت و تکنیک‌های امنیتی ارتباطات برای جلوگیری از شناسایی، و تصحیح خطاها به گونه‌ای طراحی شده اند که بتواند CIA را از طریق شبکه حفظ کنند. بیشتر حملات رایانه‌ای منجر به نقض یکی از خصوصیات امنیتی محرمانه بودن، یکپارچگی یا در دسترس بودن می‌شود. یک رویکرد دفاع در عمق به استقرار لایه‌های حفاظتی اشاره دارد. به عنوان مثال، حتی هنگام استقرار فایروال‌ها، لیست‌های کنترل دسترسی باید همچنان روی منابع مورد استفاده قرار گیرند تا در صورت نقض دیوار آتش، از دسترسی به داده‌های حساس جلوگیری کنند.

انواع مدل امنیتی Security Model Types

یک مدل امنیتی تئوری امنیت را توصیف می‌کند که از ابتدا در یک سیستم طراحی شده است. مدل‌های رسمی برای نزدیک شدن به طراحی عملیات امنیتی یک سیستم ایجاد شده است. در دنیای واقعی، استفاده از مدل‌های رسمی غالباً رد می‌شود زیرا روند طراحی را تا حدودی به تأخیر می‌اندازد (گرچه ممکن است هزینه سیستم کمتر باشد). در این بخش برخی از انواع مدل اصلی به همراه برخی مدل‌های رسمی که از رویکردهای مختلف موجود بدست آمده است، بحث می‌شود.

انواع مدل امنیتی

یک مدل امنیتی خواسته‌ها و انتظارات سازندگان سیاست‌های امنیتی را با قوانینی که یک سیستم رایانه‌ای باید دنبال کند، ترسیم می‌کند. انواع مدل‌های مختلف برای دستیابی به این هدف رویکردهای مختلفی از خود نشان می‌دهند. مدل‌های خاصی که در بخش "مدل‌های امنیتی" موجود است، ترکیب‌های مختلفی از این نوع مدل‌ها را شامل می‌شود.

حالت‌های مدل ماشینی State Machine Models

وضعیت یک سیستم، وضعیت آن در هر نقطه خاص از زمان است. فعالیت‌هایی که در فرآیند عملکرد سیستم رخ می‌دهد وضعیت سیستم را تغییر می‌دهد. گفته می‌شود که با بررسی هر وضعیت ممکن، سیستم می‌تواند باشد و تضمین شود که سیستم روابط مناسب بین اشیاء و افراد

را در هر حالت حفظ می کند. مدل Bell-LaPadula که در بخش بعدی "مدل های امنیتی" مورد بحث قرار می گیرد، نمونه ای از حالت مدل ماشینی است.

مدل های شبکه چند سطحی Multilevel Lattice Models

مدل کنترل دسترسی مبتنی بر شبکه عمدتاً برای مقابله با موضوعات محرمانه ساخته شده است و خود را عمدتاً بر جریان اطلاعات متمرکز می کند. به هر موضوع امنیتی یک برچسب امنیتی اختصاص داده شده است که مرزهای بالا و پایین دسترسی موضوعی به سیستم را مشخص می کند. سپس با سازماندهی آنها در سطوح یا شبکه ها، کنترل ها بر روی همه اشیاء اعمال می شود. اشیاء در برخی از فرمت ها حاوی اطلاعات هستند. به این جفت از عناصر (Object, Subject) (موضوع و شی) حداقل حد بالا از مقادیر و حداکثر حد پایین از مقادیر اختصاص داده شده است که کارهایی را که می تواند توسط آن موضوع با آن شی انجام دهد تعیین می کند. برچسب موضوع Subject's Label (به خاطر داشته باشید که موضوع می تواند یک شخص یا یک فرآیند باشد) تعریف می کند که به چه سطحی می توان دسترسی پیدا کرد و چه اقدامی را می توان در آن سطح انجام داد. با استفاده از مدل کنترل دسترسی مبتنی بر شبکه، یک برچسب امنیتی نیز یک کلاس امنیتی نامیده می شود. این مدل هر منبع و هر کاربر یک منبع را با یکی از کلاسهای مرتب شده مرتبط می کند. مدل مبتنی بر شبکه به منظور محافظت در برابر جریان غیرقانونی اطلاعات در بین موجودیت ها می باشد.

مدل های مبتنی بر ماتریس Matrix-Based Models

یک مدل مبتنی بر ماتریس جداول موضوع ها و اشیاء را ترتیب می دهد که نشان می دهد موضوع های فردی چه اقدامی می توانند بر روی اشیاء فردی انجام دهند. این مفهوم در سایر مدلها و همچنین مدل شبکه ای در بخش قبل بیان شد. کنترل دسترسی به اشیاء اغلب به عنوان ماتریس کنترل، پیاده سازی می شود. این یک رویکرد ساده است که حقوق دسترسی به اشخاص را برای اشیاء تعریف می کند. پیاده سازی های رایج این مفهوم، لیست های کنترل دسترسی و قابلیت ها می باشد. در ساختار جدول آن، یک ردیف نشانگر دستیابی یک موضوع به آرایه اشیاء است. بنابراین، یک ردیف می تواند به عنوان یک لیست قابلیت برای یک موضوع خاص مشاهده شود. این مدل از قسمت های زیر تشکیل شده است:

- لیستی از اشیاء

- لیستی از موضوعات
- تابعی که نوع یک شی را برمی گرداند.
- خود ماتریس، با ساخت اشیاء ستون‌ها و موضوعاتی که ردیف‌ها را می‌سازند.

مدل‌های غیر استنباطی Non-inference Models

در مدل‌های امنیتی چند سطحی، مفهوم غیراستنباطی (Non-Inference) آن دسته از اقدامات را که در سطح امنیتی بالاتری صورت می‌گیرد، تعریف می‌کند اما بر عملکردهایی که در سطح امنیتی پایین‌تری رخ می‌دهند تأثیر نمی‌گذارد یا نفوذ نمی‌کند. از آنجا که این مدل کمتر به جریان اطلاعات توجه می‌کند و بیشتر به دانش موضوع در مورد وضعیت سیستم در یک مقطع زمانی توجه می‌کند، تمرکز آن برای جلوگیری از اقداماتی است که در یک سطح انجام می‌شود تا از تغییر حالت ارائه شده به سطح دیگر جلوگیری کند.

یکی از انواع حمله‌ای که این مدل مفهومی باعث جلوگیری از آن می‌شود، استنباط Inference است. این امر زمانی اتفاق می‌افتد که شخصی به یک سطح اطلاعات دسترسی داشته باشد و به وی اجازه می‌دهد اطلاعاتی راجع به سطح دیگری استنباط کنند.

مدل‌های جریان اطلاعات Information Flow Models

به هر یک از مدل‌های مورد بحث در بخش بعدی که سعی در جلوگیری از گردش اطلاعات از یک نهاد به نهاد دیگر که سیاست امنیتی را نقض یا نفی می‌کند، یک مدل جریان اطلاعات گفته می‌شود. در مدل جریان اطلاعات، آنچه ارتباط بین دو نسخه از یک شیء است، جریان نامیده می‌شود. یک جریان نوعی وابستگی است که به دو نسخه از یک شیء مربوط می‌شود، بنابراین تبدیل یک حالت آن شیء به حالت دیگر، در نقاط متوالی در زمان می‌باشد. در یک سیستم امنیتی چند سطحی (Multilevel Security System (MLS))، یک دستگاه جریان اطلاعات یک طرفه به نام پمپ Pump مانع از جریان اطلاعات از سطح پایین‌تر طبقه بندی امنیتی یا حساسیت به سطح بالاتر می‌شود.

به عنوان مثال، مدل Bell-LaPadula که در بخش "مدل‌های امنیتی" مورد بحث قرار می‌گیرد، خود را به جریان اطلاعات در سه مورد زیر مربوط می‌کند:

- هنگامی که یک موضوع یک شیء را تغییر می‌دهد
- هنگامی که یک موضوع به یک شیء دسترسی پیدا می‌کند

- هنگامی که یک موضوع یک شی را مشاهده می کند هدف از یک مدل جریان اطلاعات، جلوگیری از جریان غیرقانونی اطلاعات در بین نهادها و موجودیت ها است.

مدل های امنیتی Security Models

تعدادی از مدل های رسمی که شامل مفاهیم مورد بحث در بخش قبلی هستند، برای راهنمایی در طراحی امنیت سیستم ها تهیه و مورد استفاده قرار گرفته اند. در این بخش برخی از مدل های امنیتی پرکاربرد یا مهم از جمله موارد زیر بحث شده است:

- Bell-LaPadula model
- Biba model
- Clark-Wilson integrity model
- Lipner model
- Brewer-Nash model
- Graham-Denning model
- Harrison-Ruzzo-Ullman model

مدل Bell-LaPadula

اولین مدل ریاضی یک سیستم چند سطحی بود که هم از مفاهیم یک مدل حالت ماشینی و هم از مدل کنترل جریان اطلاعات استفاده می کرد. این سیاست امنیت چندجانبه وزارت دفاع ایالات متحده را رسمیت می بخشید. این یک مدل حالت ماشینی است که جنبه های محرمانه بودن کنترل دسترسی را ضبط می کند. هرگونه انتقال اطلاعات از سطح بالاتر به سطح پایین تر در سیستم باید توسط یک موضوع قابل اعتماد (Trusted Subject) انجام شود.

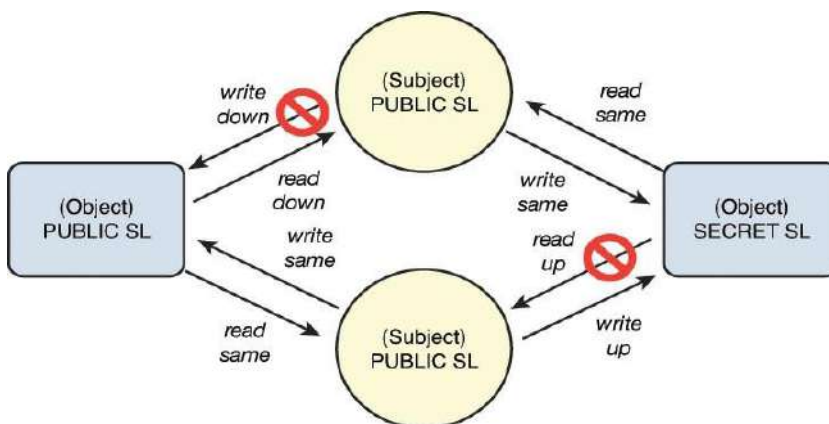
این مدل شامل سه قانون اساسی با توجه به جریان اطلاعات در یک سیستم است:

✓ قانون امنیتی ساده Simple Security Rule: یک موضوع (Subject) نمی تواند داده هایی را که در سطح امنیتی بالاتری قرار دارند، بخواند.

✓ قانون مالکیت-ستاره Star-Property Rule: یک موضوع نمی تواند در سطح پایین تر از آنچه در موضوع وجود دارد، بنویسد (آن را یادداشت کردن Write down یا قاعده حصر (Confinement rule) نمی نامید).

✓ قانون مالکیت ستاره قوی Strong Star Property Rule: یک موضوع می تواند عملیات خواندن و نوشتن را فقط در همان سطح دارای موضوع انجام دهد.

قانون مالکیت- ستاره در شکل ۱-۳ نشان داده شده است.



شکل ۱-۳

دغدغه اصلی مدل امنیتی Bell-LaPadula استفاده از این قوانین محرمانه است. اگرچه مدل اصلی آن یک سیستم کنترل دسترسی اجباری (MAC) است، اما یک قانون خاص دیگر به نام خصوصیت امنیتی اختیاری Discretionary Security Property (خصوصیت DS) باعث می شود امکان ترکیبی از کنترل های اجباری و اختیاری وجود داشته باشد. این ویژگی به یک موضوع اجازه می دهد تا به اختیار خود مجوزها را طی کند. در بخش اختیاری مدل، مجوزها از طریق ماتریس کنترل دسترسی Access Control با استفاده از فرآیندی به نام مجوز (Authorization) تعریف می شوند و سیاست های امنیتی مانع از جاری شدن اطلاعات به سمت پایین و از سطح امنیتی بالا به سطح امنیتی پایین می شوند.

مدل امنیتی Bell-LaPadula محدودیت هایی دارد. از جمله این موارد:

- این مدل هیچ سیاستی را برای تغییر کنترل دسترسی به داده ها ارائه نمی دهد. بنابراین، فقط با سیستم های دسترسی که از نظر طبیعی ایستا هستند، به خوبی کار می کند.
- این مسئله به آنچه کانال های پنهانی Covert channels گفته می شود، نمی پردازد. یک موضوع سطح پایین گاهی اوقات می تواند وجود یک شیء سطح بالا را هنگام محروم بودن از دسترسی تشخیص دهد. بعضی اوقات پنهان کردن محتوای یک شیء کافی نیست. همچنین ممکن است وجودیت آنها پنهان باشد.
- سهم اصلی آن به هزینه سایر مفاهیم، محرمانه بودن است.

این الگوی سیاست امنیتی مبنای کتاب نارنجی Orange Book بود (که در بخش بعدی مورد بحث قرار گرفته است TCSEC)

مدل Biba

پس از مدل Bell-LaPadula آمد و ویژگی های بسیاری را با آن مدل به اشتراک گذاشت. این دو مدل مشهورترین مدل های مورد بحث در این بخش است. همچنین این مدل حالت ماشینی است که از یک سری شبکه ها یا سطوح امنیتی استفاده می کند، اما مدل Biba بیشتر خود را به یکپارچگی اطلاعات تا محرمانه بودن آن اطلاعات مربوط می کند. این کار را با تکیه بر یک سیستم طبقه بندی داده برای جلوگیری از اصلاح غیرمجاز داده ها انجام می دهد. موضوعات بر حسب اعتبار خود در کلاسها طراحی می شوند. اشیاء (objects) براساس ضرری که در صورت اصلاح نادرست داده ها انجام می شود، برچسب های یکپارچگی اختصاص داده می شوند.

مانند مدل Bell-LaPadula، یک سری خواص یا بدیهیات را برای هدایت محافظت از یکپارچگی اعمال می کند. تأثیر آن اینگونه می باشد که داده ها نباید از یکجا با یکپارچگی داده شده به یک دریچه از یکپارچگی بالاتر سرازیر شوند:

- بدیهیات یکپارچگی Integrity Axiom: یک موضوع نمی تواند بالاتر از سطح دسترسی یک شخص، دسترسی داشته باشد (عدم نوشتن).
- بدیهیات یکپارچگی ساده Simple Integrity Axiom: یک موضوع نمی تواند سطح یکپارچگی کمتری را نسبت به آنچه شخص دسترسی دارد (عدم خواندن) بخواند.
- درخواست دارایی Invocation Property: یک موضوع نمی تواند از یکپارچگی سطح بالاتر استعمال کند (عدم درخواست خدمات).

مدل یکپارچگی کلارک-ویلسون Clark-Wilson Integrity Model

این مدل پس از مدل Biba توسعه یافته، خود را به یکپارچگی داده ها مربوط می کند. این مدل مجموعه ای از عناصر را که برای کنترل یکپارچگی داده ها به شرح زیر است، توصیف می کند:

- کاربر: یک عامل فعال
- روش تبدیل (TP) Transformation Procedure: عملی انتزاعی مانند خواندن، نوشتن و اصلاح، از طریق برنامه نویسی پیاده سازی شده است.

- مورد داده محدود شده: Constrained Data Item (CDI) موردی که فقط از طریق TP قابل دستکاری است.
 - مورد داده غیرقابل محدودیت: Unconstrained Data Item (UDI) موردی است که توسط کاربر می‌تواند از طریق عملیات خواندن و نوشتن دستکاری شود.
 - روش تأیید یکپارچگی (Integrity Verification Procedure (IVP): بررسی ثبات داده‌ها با دنیای واقعی
- این مدل فقط با اجازه تغییر داده‌ها از طریق برنامه‌ها نه به طور مستقیم توسط کاربران، این عناصر را اعمال می‌کند. به جای استفاده از یک ساختار شبکه ای، از یک رابطه سه بخشی از موضوع / برنامه / شی (Subject/Program/Object) استفاده می‌کند که به سه گانه Triple معروف است. همچنین مفاهیم تفکیک وظایف و تعاملات به خوبی شکل گرفته را به عنوان هدف خود تعیین می‌کند:
- تفکیک وظایف Separation of duties: این مفهوم تضمین می‌کند که برخی از عملیات‌ها نیاز به تأیید اضافی دارند.
 - تراکنش خوش فرم Well-formed Transaction: این مفهوم اطمینان می‌دهد که تمام مقادیر قبل و بعد از تراکنش با انجام عملیات خاص برای بررسی کامل تغییر داده‌ها از یک حالت به حالت دیگر بررسی می‌شوند.
- برای اطمینان از دستیابی و حفظ یکپارچگی، مدل کلارک- ویلسون ادعا می‌کند، قوانین نظارت بر یکپارچگی و حفظ یکپارچگی مورد نیاز است. به قوانین نظارت بر یکپارچگی، قوانین صدور گواهینامه Certification rules گفته می‌شود و قوانین حفظ یکپارچگی به عنوان قوانین اجرایی Inforcement rules نامیده می‌شوند.

مدل Lipner

مدل Lipner عملیاتی است که عناصر مدل Bell-LaPadula و مدل Biba را با هم ترکیب می‌کند. اولین روش اجرای یکپارچگی با مدل لیپنر از Bell-LaPadula استفاده می‌کند و موضوعات را به یکی از دو سطح حساسیت - مدیر سیستم و هر شخص دیگری - و به یکی از چهار دسته شغلی اختصاص می‌دهد. اشیاء به سطح و دسته بندی معینی اختصاص می‌یابد. دسته‌بندیها به مهمترین مکانیسم یکپارچگی (مانند کنترل دسترسی) تبدیل می‌شوند. اجرای دوم از Bell-LaPadula و Biba استفاده می‌کند. این روش از تغییر کاربران غیرمجاز جلوگیری می‌کند و از کاربران مجاز

برای ایجاد تغییرات نادرست داده جلوگیری می کند. این اجراها و پیاده سازی ها همچنین ویژگی هایی را با مدل Clark-Wilson به اشتراک می گذارند، زیرا اشیاء را به داده ها و برنامه ها تفکیک می کند.

مدل Brewer-Nash (Chinese Wall) Model دیوار چین

مدل Brewer-Nash اجازه می دهد تا مفهوم کنترل های دسترسی به صورت پویا بر اساس اقدامات قبلی کاربر تغییر کنند. یکی از اهداف انجام این مدل محافظت در مقابل تعارض منافع (Conflicts of Interest) است. این مدل همچنین مبتنی بر یک مدل جریان اطلاعات است. پیاده سازی شامل گروه بندی مجموعه داده ها به کلاس های مجزا است که هر کلاس نمایانگر تضاد منافع متفاوتی است. ایزوله کردن مجموعه داده ها در یک کلاس، قابلیت نگه داشتن داده های یک بخش را از بخش دیگر در یک پایگاه داده یکپارچه را فراهم می کند.

Graham-Denning Model

این مدل تلاش می کند تا به مسئله نادیده گرفته شده توسط مدل Bell-LaPadula به استثنای مدل مالکیت DS و Biba بپردازد. با نمایندگی و حقوق واگذاری کار می کند. این مدل روی موضوعات زیر تمرکز دارد:

- ایجاد امنیت و حذف اشیاء و موضوعات
- فراهم کردن امنیت یا انتقال مناسب دسترسی

مدل Harrison-Ruzzo-Ullman

این مدل به حقوق دسترسی نیز می پردازد. این مجموعه از عملیاتی را که می توان در یک شی انجام داد به یک مجموعه متناهی برای اطمینان از یکپارچگی محدود می کند. این مدل توسط مهندسان نرم افزار استفاده می شود تا از بروز آسیب پذیری های پیش بینی نشده توسط عملیات بسیار پیچیده، جلوگیری شود.

مراحل معماری سیستم System Architecture Steps

مدل‌ها و چارچوب‌های مختلفی که در این فصل مورد بحث قرار گرفته اند، ممکن است در مراحل دقیق به منظور توسعه یک معماری سیستم متفاوت باشند اما از یک الگوی اساسی پیروی می‌کنند. مراحل اصلی شامل موارد زیر است:

۱- فاز طراحی سیستم System design phase: در این فاز الزامات سیستم جمع آوری می‌شود و طریقه تحقق الزامات با استفاده از تکنیک‌های مدل سازی که معمولاً به صورت گرافیکی مؤلفه‌های سازگار با هر الزام و روابط متقابل این مؤلفه‌ها ترسیم می‌شود. در این فاز بسیاری از چارچوبها و مدل‌های امنیتی که بعداً در این فصل مورد بحث قرار می‌گیرند، برای کمک به تحقق اهداف معماری استفاده می‌شوند.

۲- فاز توسعه Development phase: در این فاز مؤلفه‌های سخت افزاری و نرم افزاری برای توسعه به تیم‌های جداگانه اختصاص می‌یابد. در این فاز، کارهایی که در فاز اول انجام می‌شود، می‌تواند تضمین شود که این تیم‌های مستقل به سمت مؤلفه‌هایی کار می‌کنند که برای برآورده کردن الزامات در کنار هم قرار می‌گیرند.

۳- فاز نگهداری Maintenance phase: در این فاز سیستم و معماری امنیتی ارزیابی می‌شوند تا تضمین شود که سیستم به درستی کار می‌کند و امنیت سیستم‌ها حفظ می‌شود. سیستم و امنیت باید بطور دوره‌ای بررسی و آزمایش شوند.

ISO/IEC 42010:2011 هنگام بحث درباره چارچوب‌های معماری از اصطلاحات خاص استفاده می‌کند. در زیر مروری بر برخی از مهمترین اصطلاحات است:

- معماری Architecture: سیستم سازمان، از جمله مؤلفه‌ها و روابط متقابل آنها را به همراه اصولی که طراحی و تکامل آن را راهنمایی می‌کند، تشریح می‌کند.
- شرح معماری Architectural Description (AD): مجموعه‌ای از اسناد را که به صورت رسمی، سبک معماری را منتقل می‌کند، جمع آوری می‌کند.
- ذینفعان Stakeholder: افراد، تیم‌ها و دپارتمان‌ها از جمله گروه‌های خارج از سازمان با منافع یا دغدغه‌هایی که باید در نظر بگیرند.
- نما View: دید سیستم از منظر ذینفع یا مجموعه ذینفعان
- دیدگاه Viewpoint: الگویی که برای توسعه دیدگاه‌های فردی استفاده می‌شود که مخاطب، فنون و فرضیات ساخته شده را ایجاد می‌کند.

بسترهای رایانشی (پلتفرم محاسباتی) Computing Platforms

یک بسترهای رایانشی شامل اجزای سخت افزاری و نرم افزاری است که امکان اجرای نرم افزار را فراهم می کند. به طور معمول شامل اجزای فیزیکی، سیستم عامل ها و زبان های برنامه نویسی مورد استفاده می باشد. از منظر فیزیکی و منطقی، تعدادی از چارچوبها یا پلتفرم های ممکن در حال استفاده هستند. در این بخش برخی از رایج ترین بسترها مورد بحث قرار می گیرند.

Mainframe/Thin Clients

هنگامی که از یک سیستم عامل **Mainframe/Thin Clients** استفاده می شود، معماری Client/server وجود دارد. سرور برنامه را نگه داشته و تمام پردازش ها را انجام می دهد. نرم افزار Client روی دستگاه های کاربر اجرا می شود و به سادگی، درخواست هایی را برای عملیات ارسال می کند و نتایج را نمایش می دهد. هنگامی که از یک Thin Clients واقعی استفاده می شود، به غیر از نرم افزاری که به سرور وصل می شود و نتیجه را ارائه می دهد، ماشین کاربر user machine بسیار کمی وجود دارد.

سیستم های توزیع شده Distributed Systems

این پلتفرم توزیع شده همچنین از معماری مشتری / سرور (Client/ server) استفاده می کند، اما راه حل تقسیم کار بین بخش سرور و بخش مشتری ممکن است کاملاً یک طرفه نباشد که در یک سناریوی اصلی Mainframe/Thin client مشاهده شود. در بسیاری از موارد مکانهای مختلف یا سیستم های موجود در شبکه ممکن است بخشی از راه حل باشند. همچنین، داده های حساس به احتمال زیاد در ماشین کاربر قرار دارد، بنابراین کاربران نقش به سزایی در محافظت از آن به بهترین نحو دارند.

ویژگی دیگر یک محیط توزیع شده چندین مکان پردازش است که می تواند در صورت عدم دسترسی سایت، گزینه های دیگری برای محاسبه فراهم کند.

داده ها در مکان های مختلف جغرافیایی به صورت جداگانه ذخیره می شوند. کاربران می توانند به داده های ذخیره شده و منابعی که برای کاربران شفاف است در هر مکان و فاصله ای که از کاربران دارند دسترسی پیدا کنند.

سیستم های توزیع شده می توانند نقاط ضعف امنیتی را در شبکه ایجاد کنند که باید در نظر گرفته شود. موارد زیر چند نمونه از نقاط ضعف آن می باشد:

- سیستمهای رومیزی Desktop systems می‌توانند حاوی اطلاعات حساسی باشند که ممکن است در معرض خطر قرار بگیرند.
- به طور کلی کاربران ممکن است فاقد آگاهی امنیتی باشند.
- مودم، آسیب پذیری در برابر حملات شماره گیری Dial-in Attacks را نشان می‌دهد.
- ممکن است کمبود نسخه پشتیبان مناسب وجود داشته باشد.

میان افزار Middleware

در یک محیط توزیع شده، میان افزار (Middleware) نرم افزاری است که مشتری و سرور را به یکدیگر پیوند می‌دهد. میان افزار نه بخشی از سیستم عامل و نه بخشی از نرم افزار سرور است. میان افزار کدی است که بین سیستم عامل و اپلیکیشن‌ها در هر طرف یک سیستم محاسباتی توزیع شده در یک شبکه قرار دارد. میان افزار ممکن است به اندازه کافی عمومی باشد که بین چندین نوع سیستم مشتری / سرور از یک نوع خاص کار کند.

سیستم‌های تعبیه شده Embedded Systems

یک سیستم تعبیه شده یک قطعه نرم افزاری است که در یک قطعه بزرگتر از نرم افزار ساخته شده است که وظیفه انجام برخی عملکردهای خاص را به نمایندگی از سیستم بزرگتر دارد. قسمت تعبیه شده امکان ارتباطات سخت افزاری خاصی را در بر می‌گیرد و ممکن است درایورها بخواهند بین سیستم بزرگتر و برخی سخت افزارهای خاص ارتباط داشته باشند.

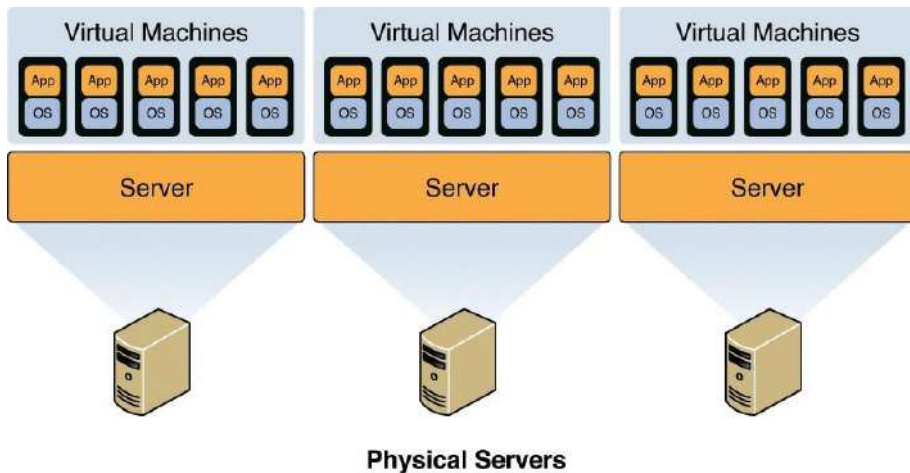
محاسبات (رایانش) سیار Mobile Computing

کد سیار دستورالعمل‌هایی است که از طریق شبکه منتقل شده و بر روی یک سیستم از راه دور اجرا می‌شود. نمونه‌ای از کد سیار کد جاوا و ActiveX است که از طریق شبکه جهانی وب در یک مرورگر وب دانلود می‌شود. هرگونه معرفی کد از یک سیستم به سیستم دیگر یک موضوع با اهمیت امنیتی است و در برخی شرایط لازم است. یک مازول محتوای فعال که سعی در انحصار و بهره برداری از منابع سیستم دارد، یک اپلت خصومت آمیز Hostile applet نامیده می‌شود. هدف اصلی مدل امنیت جاوا (JSM) Java Security Model محافظت از کاربر در برابر Hostile و کد سیار شبکه است. این کار را با قرار دادن کد در Sandbox انجام می‌دهد، که عملکرد آن را محدود می‌کند.

محاسبات مجازی Virtual Computing

محیط های مجازی به طور فزاینده ای به عنوان بستر محاسباتی برای راه حل ها مورد استفاده قرار می گیرند. اکثر موارد امنیتی مشابه که باید در محیط فیزیکی کاهش یابد باید در شبکه مجازی نیز مورد بررسی قرار گیرد.

در یک محیط مجازی، نمونه های یک سیستم عامل که به آن Virtual Machines (VMs) گفته می شود. یک سیستم میزبان می تواند شامل بسیاری از VM ها باشد. نرم افزاری به نام Hyper Visor، توزیع منابع (CPU، حافظه و دیسک) را در VM ها مدیریت می کند. شکل ۲-۳ رابطه بین ماشین میزبان، منابع فیزیکی آن، VM های مقیم و منابع مجازی که به آنها اختصاص داده شده است را نشان می دهد.



شکل ۲-۳: مجازی سازی

خدمات امنیتی Security Services

روند ایجاد معماری سیستم همچنین شامل سیستم طراحی امنیتی است که فراهم خواهد شد. این خدمات بستگی به حمایت هایی که برای ارائه می دهند، می توانند به چند دسته تقسیم شوند. در این بخش به طور خلاصه انواع خدمات امنیت مورد بررسی و مقایسه قرار می گیرد.

• خدمات کنترل مرزی Boundary Control Services

این سرویس‌ها وظیفه قرار دادن مولفه‌های مختلف در مناطق امنیتی و حفظ کنترل مرزی را در بین آنها دارند. به طور کلی، این کار با نشان دادن مؤلفه‌ها و خدمات مورد اعتماد یا عدم اعتماد انجام می‌شود. به عنوان نمونه، فضای حافظه‌ای که از سایر فرآیندهای در حال اجرا در سیستم چند پردازش مجزا می‌شود بخشی از یک مرز محافظ است.

• خدمات کنترل دسترسی Access Control Services

در فصل ۵، "هویت و مدیریت دسترسی Identity and Access Management"، با روشهای مختلف کنترل دسترسی و نحوه استقرار آنها آشنا خواهید شد. یک روش مناسب مستقرشدن کنترل دسترسی به مواد حساس که در دسترس کاربران برای انجام کارهای خود نیاز دارند.

• خدمات یکپارچگی Integrity Services

همانطور که به خاطر دارید، یکپارچگی دلالت بر این دارد که داده‌ها تغییر نکرده اند. هنگامی که خدمات یکپارچگی وجود دارد، اطمینان می‌دهند که داده‌های منتقل شده از طریق سیستم عامل یا اپلیکیشن می‌توانند تأیید شده باشند که در انتقال آسیب ندیده یا خراب نشده اند.

• خدمات رمزنگاری Cryptography Services

اگر این سیستم قادر به ویرایش یا رمزنگاری اطلاعات در هنگام انتقال باشد، گفته می‌شود خدمات رمزنگاری را ارائه می‌دهد. در بعضی موارد، این سرویس بصورت بومی توسط یک سیستم ارائه نمی‌شود و در صورت تمایل باید به روشی دیگر ارائه شود، اما اگر توانایی داشته باشد، بسیار با ارزش است، به خصوص در مواردی که سیستم‌ها توزیع شده و در سراسر شبکه صحبت می‌کنند.

• خدمات ممیزی و نظارت Auditing and Monitoring Services

اگر سیستم روشی برای ردیابی فعالیتهای کاربران و عملیات فرآیندهای سیستم داشته باشد، گفته می‌شود که خدمات ممیزی و نظارت را ارائه می‌دهد. اگرچه تمرکز ما در اینجا روی امنیت است، ارزش این سرویس فراتر از امنیت بوده زیرا این امکان را نیز می‌دهد تا نظارت بر عملکرد خود سیستم انجام شود.

مؤلفه های سیستم System Components

هنگام بحث در مورد نحوه تأمین امنیت در یک معماری، داشتن درک اساسی از مؤلفه ها در تجهیزات محاسباتی کمک کننده است. در این بخش به بحث در مورد مؤلفه ها و برخی از کارکردهای ارائه شده می پردازیم.

پردازنده و چند پردازشی CPU and Multiprocessing

واحد پردازش مرکزی (CPU) سخت افزاری در سیستم است که تمام دستورالعمل های موجود در کد را اجرا می کند. این مجموعه دستورالعمل های خاص خود را برای عملکرد داخلی خود دارد و این دستورالعمل ها سبک معماری آن را تعریف می کنند. نرم افزاری که بر روی سیستم اجرا می شود باید با این معماری سازگار باشد، در واقع به معنی CPU است و نرم افزار می تواند ارتباط برقرار کند.

وقتی بیش از یک پردازنده وجود داشته باشد و در دسترس باشد، سیستم قادر به تبدیل شدن به سیستم چند پردازشی می شود.

چند پردازشی به رایانه اجازه می دهد تا چندین دستورالعمل را به طور موازی اجرا کند. این کار را می توان با پردازنده های فیزیکی جداگانه یا با یک پردازنده منفرد با چند هسته انجام داد. هر هسته به عنوان یک CPU جداگانه عمل می کند.

CPU ها حافظه خاص خود را دارند و CPU قادر است سریعتر از هر حافظه دیگر به این حافظه دسترسی داشته باشد. همچنین CPU معمولاً دارای حافظه کش است که در صورت نیاز دوباره به دستورالعمل هایی که اخیراً اجرا شده اند، در آن نگهداری می شوند. هنگامی که یک پردازنده از حافظه دستورالعمل می گیرد، به آن فرایند واکشی (Fetching) گفته می شود.

یک واحد محاسبه و منطق (Arithmetic Logic Unit (ALU در CPU اجرای واقعی دستورالعمل ها را انجام می دهد. در حالی که دستورالعمل های اپلیکیشن ها و سیستم عامل ها اجرا می شوند واحد کنترل به عنوان مدیر سیستم عمل می کند. ثبات های CPU حاوی مجموعه دستورالعمل اطلاعات و داده ها برای اجرا هستند و شامل ثبات های عمومی، ثبات های ویژه و ثبت پیشخوان برنامه (general registers, special registers, program counter register) می باشند.

CPU ها می توانند در حالت کاربر (User mode) یا حالت ممتاز (Privileged mode) فعالیت کنند که به آن حالت هسته یا سرپرست (Kernel, Supervisor) نیز گفته می شود. وقتی

اپلیکیشن‌ها با CPU ارتباط برقرار می‌کنند، در حالت کاربر قرار دارند. اگر یک دستورالعمل ارسال شده به CPU مشخص شده است که در حالت ممتاز انجام شود، باید سیستم عامل قابل اعتماد باشد و عملکرد در حالت کاربری قرار نداشته باشد.

CPU به یک آدرس bus متصل است. دستگاه‌های حافظه و I/O این آدرس bus را تشخیص می‌دهند. این دستگاه‌ها می‌توانند با CPU ارتباط برقرار کنند، داده‌های درخواستی را بخوانند و آن را روی باس داده ارسال کنند.

هنگامی که میکرو کامپیوترها برای اولین بار توسعه یافتند، زمان واکشی (Fetch Time) دستورالعمل به دلیل سرعت نسبتاً کند دسترسی به حافظه بسیار طولانی تر از زمان اجرای دستورالعمل بود. این وضعیت منجر به طراحی (CISC) (CPU Complex Instruction Set Computer) مجموعه دستورالعمل‌های پیچیده شد. در این چیدمان، برای کمک به کاهش دسترسی نسبتاً کند حافظه، مجموعه دستورالعمل‌ها کاهش یافته اند (در حالی که پیچیده تر شده اند).

پس از اینکه دسترسی به حافظه تا جایی بهبود یافت که اختلاف زیادی در زمان دسترسی به حافظه و زمان اجرای پردازنده وجود نداشت، معماری کاهش مجموع دستورالعمل‌ها Reduced Instruction Set Computer (RISC) معرفی شد. هدف معماری RISC کاهش تعداد چرخه‌های مورد نیاز برای اجرای یک دستورالعمل بود که این امر با پیچیده تر کردن دستورالعمل‌ها انجام شد.

حافظه و ذخیره سازی Memory and Storage

یک سیستم محاسباتی برای ذخیره اطلاعات، به صورت بلند مدت و کوتاه مدت، نیاز به مکانی برای ذخیره سازی دارد. دو نوع مکان ذخیره سازی وجود دارد: حافظه، برای نیازهای ذخیره سازی موقت و رسانه‌های ذخیره سازی بلند مدت. به اطلاعات می‌توان خیلی سریعتر از حافظه و ذخیره سازی بلند مدت دسترسی پیدا کرد، به همین دلیل بیشترین دستورالعمل‌ها یا اطلاعاتی که اخیراً استفاده می‌شود به طور معمول برای مدت زمان کوتاهی در حافظه کش ذخیره می‌شوند، که اطمینان می‌دهد دسترسی دوم و بعدی سریعتر از بازگشت به حافظه بلند مدت خواهد بود. رایانه‌ها می‌توانند حافظه دسترسی تصادفی (RAM) و حافظه فقط خواندنی (ROM) داشته باشند. RAM بی ثبات و فرار است، به این معنی که اطلاعات باید بطور مداوم تجدید شود و در صورت خاموش شدن سیستم از بین می‌رود. جدول ۳-۲ شامل برخی از انواع RAM است که در لپ تاپ‌ها و دسکتاپ‌ها استفاده می‌شود.

Desktop Memory	Description
SDRAM—synchronous dynamic random-access memory	Synchronizes itself with the CPU's bus.
DDR SDRAM—double data rate synchronous dynamic random-access memory	Supports data transfers on both edges of each clock cycle (the rising and falling edges), effectively doubling the memory chip's data throughput.
DDR2 SDRAM—double data rate two (2) synchronous dynamic random-access memory	Transfers 64 bits of data twice every clock cycle and is not compatible with current DDR SDRAM memory slots.
DDR3-SDRAM—double data rate three (3) synchronous dynamic random-access memory	Offers reduced power consumption, a doubled pre-fetch buffer, and more bandwidth because of its increased clock rate.
DDR3-SDRAM—double data rate (4) synchronous dynamic random-access memory	Includes higher module density and lower voltage requirements. Theoretically allows for DIMMs of up to 512 GB in capacity, compared to the DDR3's maximum of 128 GB per DIMM.
Laptop Memory	Description
SODIMM—small outline DIMM	Differs from desktop RAM in physical size and pin configuration. A full-size DIMM has 100, 168, 184, 240, or 288 pins and is usually 4.5 to 5 inches in length. In contrast, a SODIMM has 72, 100, 144, 200, 204, or 260 pins and is smaller—2.5 to 3 inches.

جدول ۳-۲: انواع حافظه

از طرف دیگر، ROM فرار نیست و همچنین بدون انجام یک سری عملیات وابسته به نوع ROM قابل نوشتن نیست. معمولاً حاوی دستورالعملهای سطح پایین است که دستگاهی که روی آن نصب شده را عملیاتی کند. برخی از نمونه‌های ROM شامل:

- حافظه فلش: نوعی از ROM با قابلیت برنامه ریزی الکتریکی
- دستگاه منطق قابل برنامه نویسی (Programmable Logic Device (PLD): یک مدار مجتمع با اتصالات یا دروازه‌های منطق داخلی (Internal logic gates) که می‌تواند از طریق یک فرآیند برنامه نویسی تغییر یابد.
- Field Programable Gate Array (FPGA): نوعی PLD است که با عبور دادن اتصالات فیوز بر روی تراشه یا استفاده از آنتی فیوز که هنگام اتصال ولتاژ بالا به محل اتصال ایجاد می‌شود، برنامه ریزی می‌شود.
- Firmware: نوعی ROM که در آن یک برنامه یا دستورالعمل سطح پایین نصب شده است.

حافظه‌ای که مستقیماً توسط CPU قابل کنترل است، که برای ذخیره سازی دستورالعمل‌ها و داده‌هایی که با اجرای برنامه در ارتباط هستند، حافظه اصلی (Primary memory) نامیده می‌شود. علیرغم از نوع حافظه‌ای که اطلاعات در آن قرار دارد، در بیشتر موارد CPU باید در واکنشی اطلاعات به نمایندگی از سایر مؤلفه‌ها شرکت کند. اگر یک مؤلفه توانایی دستیابی مستقیم به حافظه را بدون کمک CPU داشته باشد، به آن دسترسی مستقیم به حافظه Direct Memory Access (DMA) گفته می‌شود.

برخی از اصطلاحات دیگر که باید با توجه به حافظه با آنها آشنا شوید شامل موارد زیر است:

- ✓ **حافظه انجمنی Associative memory**: به جای استفاده از آدرس حافظه خاص، به جستجوی یک مقدار داده خاص با ارزش در حافظه می‌پردازد.
- ✓ **آدرس دهی ضمنی Implied addressing**: به ثبت‌هایی که معمولاً درون CPU وجود دارد، اشاره دارد.
- ✓ **آدرس دهی مطلق Absolute addressing**: به کل فضای حافظه اصلی آدرس می‌دهد، CPU از آدرسهای حافظه فیزیکی استفاده می‌کند که به آنها آدرسهای مطلق گفته می‌شود.
- ✓ **حافظه کش Cache**: مقدار نسبتاً کمی (در مقایسه با حافظه اصلی) حافظه رم با سرعت بسیار زیاد است که دستورالعمل‌ها و داده‌ها را در حافظه اصلی نگه می‌دارد و احتمال دسترسی در طی بخش اجرایی برنامه جاری بسیار زیاد است.
- ✓ **آدرس دهی غیر مستقیم Indirect addressing**: نوع آدرس دهی حافظه که در آن مکان آدرس که در دستورالعمل برنامه مشخص شده است، حاوی آدرس نهایی محل مورد نظر است.
- ✓ **آدرس منطقی Logical address**: آدرسی که سلول حافظه یا عنصر ذخیره آن از منظر یک اپلیکیشن در حال اجرا باشد.
- ✓ **آدرس نسبی Relative address**: با مشخص کردن فاصله آن از آدرس دیگر، مکان آن را مشخص می‌کند.
- ✓ **حافظه مجازی Virtual memory**: مکانی در هارد سخت که در صورت کم بودن فضای حافظه بطور موقت از آن استفاده می‌شود.

✓ **نشت حافظه Memory leak:** هنگامی رخ می دهد که یک برنامه کامپیوتری به طور نادرست تخصیص حافظه را مدیریت کند، که می تواند حافظه سیستم موجود را با اجرای یک برنامه خالی کند.

دستگاههای ورودی / خروجی Input/Output Devices

از دستگاههای ورودی / خروجی (I / O) برای ارسال و دریافت اطلاعات به سیستم استفاده می شود. نمونه ها شامل صفحه کلید، ماوس، نمایشگرها و چاپگرها هستند. سیستم عامل تعامل بین دستگاههای I / O و سیستم را کنترل می کند. در مواردی که دستگاه I / O نیاز به پردازنده برای انجام برخی اقدامات داشته باشد، به CPU با پیامی به نام وقفه (Interrupt) سیگنال می دهد.

سیستم های عامل Operating Systems

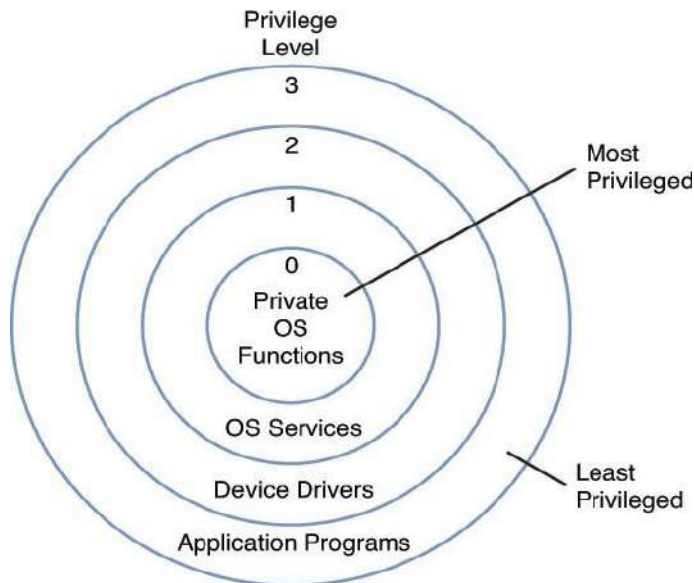
سیستم عامل نرم افزاری است که انسان را قادر می سازد با سخت افزاری که رایانه را تشکیل می دهد تعامل داشته باشد. بدون سیستم عامل، رایانه بی فایده خواهد بود. سیستم عاملها تعدادی از کارکردهای قابل توجه و جالب را به عنوان بخشی از واسطه بین انسان و سخت افزار انجام می دهند. در این بخش برخی از این فعالیتها را بررسی می کنیم.

یک نخ (Thread) کار جداگانه است که برای یک فرآیند خاص انجام می شود. فرآیند مجموعه ای از نخها که بخشی از همان کار بزرگتر برای یک برنامه خاص می باشد. دستورالعملهای یک اپلیکیشن تا زمانی که در حافظه بارگذاری (Load) نشوند، در نظر گرفته نمی شوند، در واقع جایی که ابتدا باید همه دستورالعملها برای پردازش توسط CPU کپی شود. یک فرآیند می تواند در حالت در حال اجرا، حالت آماده و یا حالت مسدود باشد. هنگامی که یک فرآیند مسدود می شود، به سادگی منتظر انتقال داده ها به آن است و معمولاً از طریق ورود داده های کاربر می باشد. به گروهی از فرآیندها که دسترسی به همان منابع مشترک دارند، یک دامنه حفاظت Protection Domain گفته می شود.

CPUها را می توان با توجه به نحوه انجام فرآیندها طبقه بندی کرد. معماری کامپیوتر فراعدهی Superscalar توسط یک پردازنده مشخص می شود که اجرای همزمان چندین دستورالعمل را در همان مرحله لوله کشی (Pipeline) امکان پذیر می کند. پردازنده ای که در آن یک دستورالعمل واحد بیش از یک عملیات همزمان را مشخص می کند، یک پردازنده با دستورالعمل بسیار طولانی Very Long Instruction Word (VLIW) نامیده می شود. یک پردازنده Pipeline مراحل دستورالعملهای مختلف را با هم به اشتراک می گذارد در حالی که یک پردازنده عددی (Scalar)

Processor) یک دستورالعمل را در یک زمان اجرا می‌کند، و در نتیجه باعث افزایش لوله کشی یا همان Pipeline می‌شود.

از دیدگاه امنیتی، فرایندها طبق ساختار کمترین امتیاز در یک ساختار حلقه قرار می‌گیرند، به این معنی که فقط آنها دسترسی به منابع و مؤلفه‌های لازم برای انجام کار را دارند. تصور مشترک این ساختار در شکل ۳-۳ نشان داده شده است.



شکل ۳-۳ ساختار حلقه

وقتی یک سیستم رایانه دستورالعمل‌های I/O را پردازش می‌کند، در حالت Supervisor کار می‌کند. خاتمه پردازش انتخابی و غیر مهم در هنگام بروز خرابی سخت افزاری یا نرم افزاری و تشخیص آن، شکست نرم (Fail Soft) نامیده می‌شود. در خرابی امن (Fail Safe)، وقتی یک خرابی رخ می‌دهد و سیستم تشخیص می‌دهد، سیستم به طور خودکار فرآیندها و مولفه‌های سیستم را در یک حالت امن قرار می‌دهد.

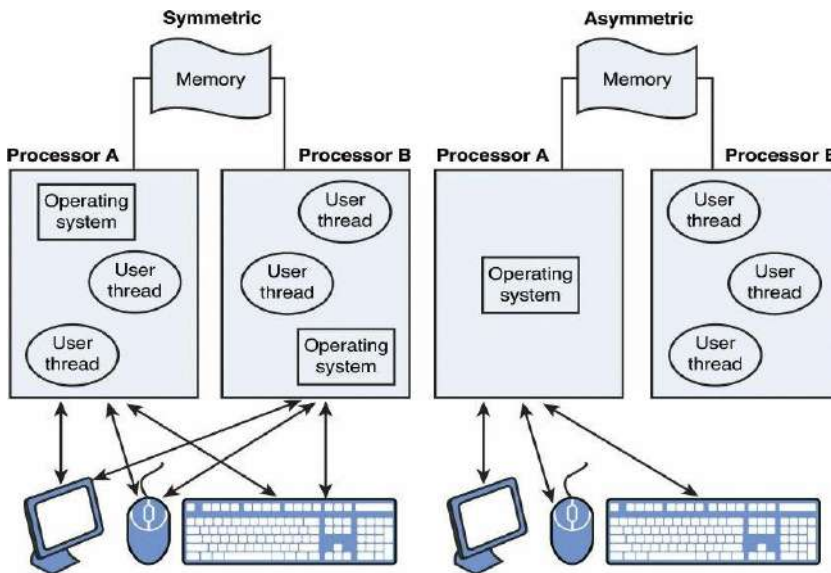
چند وظیفه‌ای Multitasking

چند وظیفه‌ای فرآیند انجام بیش از یک کار در یک زمان است. چند وظیفه‌ای به دو روش مختلف قابل انجام است. هنگامی که رایانه دارای یک پردازنده واحد است، در واقع چند کار را به طور

همزمان انجام نمی دهد. این چرخه پردازنده CPU خود را با سرعت بسیار بالایی بین کارها تقسیم می کند که به نظر می رسد همزمان چندین کار را انجام می دهد. اما، هنگامی که یک رایانه بیش از یک پردازنده داشته باشد یا دارای پردازنده ای با چند هسته (multiple cores) باشد، آنگاه قادر است همزمان دو کار را انجام دهد و می تواند این کار را به دو روش مختلف انجام دهد:

- حالت متقارن Symmetric mode: در این حالت پردازنده ها یا هسته ها به صورت round-robin کار می شوند، به صورت نخ به نخ.
- حالت نامتقارن Asymmetric mode: در این حالت یک پردازنده به یک فرآیند یا اپلیکیشن خاص اختصاص داده شده است. در صورت نیاز به کار برای آن فرآیند، همیشه توسط همان پردازنده انجام می شود.

شکل ۳-۴ رابطه این دو حالت را نشان می دهد.



شکل ۳-۴ انواع چند پردازشی

چند وظیفه ای انحصاری Multitasking Preemptive بدین معنی است که وظیفه سوئیچ ها را می توان مستقیماً از هدایت کننده های وقفه (Interrupt) شروع کرد. با همکاری چند وظیفه ای (غیر انحصاری)، وظیفه سوئیچ فقط وقتی انجام می شود که یک کار با هسته (Kernel) فراخوانی شود و به هسته فرصتی برای انجام وظیفه سوئیچ کردن بدهد.

مدیریت حافظه Memory Management

از آنجا که تمام اطلاعات قبل از پردازش به حافظه می‌روند، مدیریت امن حافظه بسیار مهم است. فضای حافظه عایق شده یا ایزوله شده از سایر فرایندهای در حال اجرا در یک سیستم چند پردازشی در یک دامنه حفاظت شده Protection Domain است.

مدل‌های ارزیابی امنیت سیستم System Security Evaluation Models

در تلاش برای ایجاد نظم در هرج و مرج امنیتی که هم شامل نرم افزارهای داخلی و هم نرم افزارهای تجاری (سیستم عامل، اپلیکیشن و غیره) می‌شود، چندین روش برای ارزیابی و رتبه بندی امنیت این محصولات ایجاد شده است. یک آزمون سطح اطمینان سعی در بررسی مؤلفه‌های امنیتی یک سیستم و تعیین سطح اطمینان دارد که سیستم می‌تواند سطح خاصی از امنیت را فراهم کند. در بخش‌های بعدی سازمان‌هایی که چنین سیستم‌های ارزیابی را ایجاد کرده اند مورد بحث قرار می‌گیرند.

TCSEC

ضوابط ارزیابی سیستم کامپیوتری مورد اعتماد Trusted Computer System Evaluation Criteria (TCSEC) توسط مرکز امنیت رایانه ملی (NCSC) Computer Security Center برای وزارت دفاع آمریکا برای ارزیابی محصولات تهیه شده است.

آنها مجموعه‌ای از کتاب‌ها را منتشر کرده اند که هم در سیستم‌های رایانه‌ای و هم شبکه‌هایی که در آن فعالیت می‌کنند متمرکز شده است. آنها محرمانه بودن را به جای یکپارچگی مورد توجه قرار می‌دهند. در سال ۲۰۰۵، TCSEC با معیارهای رایج جایگزین شد که بعداً در این فصل مورد بحث قرار می‌گیرد. با این حال، متخصصان امنیت به دلیل تأثیر آن بر روی اقدامات امنیتی امروزه و به دلیل برخی از اصطلاحات آن هنوز در حال استفاده می‌باشد و باید TCSEC را درک کنند.

با استفاده از TCSEC، عملکرد و اطمینان به طور جداگانه ارزیابی می‌شوند و پایه‌ای برای ارزیابی اثربخشی کنترل‌های امنیتی ساخته شده در محصولات سیستم پردازش خودکار داده‌ها هستند. به عنوان مثال، مفهوم حداقل امتیازات از TCSEC گرفته شده است. در این بخش، درباره کتاب‌ها و رتبه بندی‌هایی که از آنها صورت گرفته بحث شده است.

سری های رنگین کمان Rainbow Series

انتشار اصلی ایجاد شده توسط TCSEC، کتاب نارنجی بود (در قسمت بعدی مورد بحث قرار می گیرد)، اما با گذشت زمان، کتابهای دیگری نیز ایجاد شد که بر جنبه های اضافی امنیت سیستم های رایانه ای متمرکز است. به طور کل، هم اکنون این مجموعه بیش از ۲۰ کتاب به عنوان سری های رنگین کمان نامیده می شود که هر کتاب رنگ متفاوتی دارد. به عنوان مثال، کتاب سبز فقط بر مدیریت گذرواژه تمرکز دارد. مهمترین کتاب ها، کتاب نارنجی و کتاب قرمز می باشد.

کتاب نارنجی Orange Book

کتاب نارنجی مجموعه ای از معیارهای مبتنی بر مدل Bell-LaPadula است که برای ارزیابی و درجه بندی امنیت ارائه شده توسط یک محصول سیستم رایانه ای استفاده می شود. تحلیل کانال پنهان، مدیریت تاسیسات قابل اعتماد و بهبودی قابل اعتماد مفاهیمی هستند که در این کتاب مورد بحث قرار گرفته است.

اهداف این سیستم را می توان به دو دسته تقسیم کرد، الزامات تضمین عملیاتی و الزامات تضمین چرخه عمر که جزئیات مربوط به آنها در ادامه تعریف می شود.

الزامات تضمین عملیاتی که در کتاب نارنجی مشخص شده است به شرح زیر است:

- معماری سیستم System Architecture
- یکپارچگی سیستم System Integrity
- تجزیه و تحلیل کانال پنهان Covert Channel Analysis
- مدیریت تأمین اعتبار Trusted Facility Management
- بهبود قابل اطمینان Trusted Recovery

TCSEC از یک سیستم طبقه بندی استفاده می کند که یک حرف و شماره (letter, number) را برای توصیف اثربخشی امنیتی سیستم ها اختصاص می دهد. حرف به یک سطح یا بخش (division) ضمانت امنیتی اشاره دارد، که چهار مورد از آنها وجود دارد، و شماره به شیب های موجود در آن سطح یا کلاس تضمین امنیتی اشاره دارد. هر بخش و کلاس شامل تمام عناصر مورد نیاز زیر آن است.

به منظور حداقل امنیت بیشتر، چهار کلاس و بخش‌ها و الزامات تشکیل دهنده آنها به شرح زیر است:

✓ D - حداقل حفاظت Minimal Protection

برای سیستم‌هایی که مورد ارزیابی قرار گرفته اند ولی در شرایط لازم برای یک بخش بالاتر عمل نمی‌کنند، محفوظ است.

✓ C - محافظت از اختیار Discretionary Protection

▪ C1 محافظت از امنیت اختیاری Discretionary Security Protection

- نیاز به شناسایی و احراز هویت دارد.
- به جداسازی کاربران و داده‌ها نیاز دارد.
- از کنترل دسترسی اختیاری (DAC) Discretionary access control استفاده می‌کند که قادر است محدودیت‌های دسترسی را به صورت فردی یا گروهی اعمال کند.
- به اسناد سیستم و کتابچه راهنمای کاربر نیاز دارد.

▪ C2 حفاظت از دسترسی کنترل شده Controlled Access Protection

- از DAC استفاده می‌کند.
- پاسخگویی فردی از طریق مراحل ورود به سیستم را فراهم می‌کند.
- به مسیرهای ممیزی محافظت شده نیاز دارد.
- تئوری استفاده مجدد از شی را فراخوانی می‌کند.
- نیاز به ایزوله سازی منابع دارد.

✓ B - محافظت اجباری Mandatory Protection

▪ B1 دارای برچسب حفاظت از امنیت

- از بیانیه غیر رسمی سیاست امنیتی استفاده می‌کند.
- به برچسب‌های حساس یا طبقه بندی داده نیاز دارد.
- از MAC بر روی موضوعات و اشیاء انتخاب شده استفاده می‌کند.
- قابلیت صدور برچسب.
- نیاز به رفع یا کاهش نقص‌های کشف شده دارد.
- از مشخصات طراحی و تأیید استفاده می‌کند.

▪ B2 - حفاظت ساختاریافته Structured Protection

- به یک سیاست امنیتی کاملاً تعریف شده و رسماً مستند نیاز دارد.

- از DAC و MAC برای همه افراد و اشیاء استفاده می کند.
- تجزیه و تحلیل و جلوگیری از کانال های ذخیره پنهان برای رخداد و پهنای باند
- عناصر ساختار را به دسته های محافظتی و دسته های غیر محافظتی طبقه بندی می کند.
- آزمایش و بررسی جامع تر را از طریق طراحی و اجرا امکان پذیر می کند.
- مکانیسم های احراز هویت (Authentication) را تقویت می کند.
- مدیریت تاسیسات مورد اعتماد را با تفکیک ادمین و اپراتور فراهم می کند.
- کنترل های مدیریت پیکربندی سختگیرانه را اعمال می کند.
- B3 - دامنه های امنیتی Security Domains
 - الزامات نظارت مرجع را برآورده می کند.
 - کدهایی که برای اجرای سیاست های امنیتی ضروری نیستند را حذف می کند.
 - پیچیدگی را از طریق مهندسی سیستم به طور قابل توجهی به حداقل می رساند.
 - نقش مدیر امنیتی (Security Administrator) را تعریف می کند.
 - به ممیزی از وقایع مرتبط با امنیت احتیاج دارد.
 - به طور خودکار به تشخیص نفوذ قریب الوقوع، از جمله اطلاع رسانی پرسنل را ردیابی کرده، و پاسخ می دهد.
 - به روشهای بازیابی سیستم مورد اعتماد نیاز دارد.
 - کانال های زمان بندی پنهان برای وقوع و پهنای باند را تجزیه و تحلیل کرده و از آنها جلوگیری می کند.
 - نمونه ای از چنین سیستمی XTS-300، پیشرو XTS-400 است.

✓ A - حفاظت تأیید شده Verified Protection

- A1 - طراحی تأیید شده Verified Design
 - اطمینان بالاتری نسبت به B3 ارائه می دهد اما از نظر عملکردی با B3 یکسان است.
 - از تکنیک های رسمی طراحی و تأیید استفاده می کند، از جمله مشخصات رسمی سطح بالا.
 - نیاز دارد که از تکنیک های رسمی برای اثبات هم ارزی بین مشخصات رایانه مورد اعتماد (TCB) Trusted Computer Base و مدل سیاست امنیتی استفاده کند.
 - روشهای رسمی مدیریت و توزیع را ارائه می دهد.

- نمونه‌ای از چنین سیستمی پردازنده ارتباطات ایمن هانیول Honeywell's Secure Communications Processor (SCOMP)، پیشرو XTS400 است.

کتاب قرمز Red Book

تفسیر شبکه مورد اعتماد Trusted Network Interpretation (TNI) کلاس‌های ارزیابی TCSEC (DOD 5200.28-STD) به سیستم‌ها و مؤلفه‌های شبکه قابل اعتماد در کتاب قرمز گسترش می‌یابد. بنابراین در جاهایی که کتاب نارنجی روی امنیت یک سیستم واحد تمرکز دارد، کتاب قرمز به امنیت شبکه می‌پردازد.

ITSEC

TCSEC فقط محرمانه بودن را مورد توجه قرار داده و عملکرد و تضمین را به هم متصل می‌کند. برخلاف TCSEC، معیارهای ارزیابی امنیت فناوری اطلاعات (ITSEC) به یکپارچگی و در دسترس بودن و همچنین محرمانه بودن می‌پردازد. تفاوت دیگر این است که ITSEC عمدتاً مجموعه‌ای از دستورالعمل‌ها بود که در اروپا مورد استفاده قرار می‌گرفت، در حالی که TCSEC بیشتر در ایالات متحده تاکید می‌شود.

ITSEC از بسیاری جهات شبیه به TCSEC دارای سیستم رتبه بندی است. ITSEC دارای ۱۰ کلاس، F1 تا F10، برای ارزیابی الزامات عملکردی و ۷ کلاس TCSEC، E0 تا E6، برای ارزیابی الزامات تضمین است.

الزامات عملکردی امنیت شامل موارد زیر است:

- F00 شناسایی و احراز هویت Identification and authentication
- F01: ممیزی Audit
- F02: بهره‌برداری از منابع Resource utilization
- F03: مسیرها / کانالهای قابل اعتماد Trusted paths/channels
- F04: محافظت از داده‌های کاربر User data protection
- F05: مدیریت امنیت Security management
- F06: دسترسی به محصول Product access
- F07: ارتباطات Communications
- F08: حریم خصوصی Privacy

- F09: محافظت از عملکردهای امنیتی محصول Protection of the product's security functions
 - F10: پشتیبانی رمزنگاری Cryptographic support
- الزامات تضمین امنیت شامل موارد زیر است:
- E001: اسناد راهنما و کتابچه راهنمای کاربر Guidance documents and manuals
 - E01: مدیریت پیکربندی Configuration management
 - E02: ارزیابی آسیب پذیری Vulnerability assessment
 - E03: تحویل و بهره برداری Delivery and operation
 - E04: پشتیبانی چرخه عمر Life-cycle support
 - E05: تعمیر و نگهداری ضمانت Assurance maintenance
 - E06: توسعه Development
 - E07: آزمایش Testing
- سیستم های TCSEC و ITSEC می توانند به یکدیگر نگاشته شوند، اما ITSEC تعدادی از رتبه بندی را ارائه می دهد که هیچ مفهومی در رتبه بندی های TCSEC ندارند. جدول ۳-۳ نقشه برداری از دو سیستم را نشان می دهد.

ITSEC	TCSEC
E0	D
F1+E1	C1
F2+E2	C2
F3+E3	B1
F4+E4	B2
F5+E5	B3
F6+E6	A1
F6	Systems that provide high integrity
F7	Systems that provide high availability
F8	Systems that provide high data integrity during communication
F9	Systems that provide high confidentiality (using cryptography)
F10	Networks with high demands on confidentiality and integrity

جدول ۳-۳: نقشه برداری ITSEC و TCSEC

ITSEC به طور عمده با معیارهای مشترک جایگزین شده است، که در بخش بعدی مورد بحث قرار می‌گیرد.

معیارهای مشترک Common Criteria

در سال ۱۹۹۰، ISO نیاز به یک سیستم رتبه بندی استاندارد را که می‌تواند در سطح جهانی مورد استفاده قرار گیرد، شناسایی کرد. معیارهای مشترک (CC) نتیجه تلاش مشترک برای ایجاد این سیستم بود. این سیستم از سطوح تضمین ارزیابی (Evaluation Assurance levels (EAL برای رتبه بندی سیستم‌ها استفاده می‌کند و هر کدام سطح بالاتری از تست امنیتی و طراحی امنیتی را در یک سیستم نشان می‌دهند. رتبه بندی بالقوه نشان دهنده پتانسیل سیستم برای تأمین امنیت است. فرض بر این است که مشتری تمام راه‌های امنیتی موجود را بطور صحیح پی‌کربندی می‌کند، بنابراین لازم است که فروشنده همیشه مستندات مناسبی را ارائه دهد تا مشتری بتواند به طور کامل به رتبه بندی (Rating) خود دست یابد.

ISO/IEC 15408-1:2009 نسخه CC از ISO است.

CC بیانگر الزامات امنیتی IT در مورد یک محصول یا سیستم در دو دسته است: عملکرد و تضمین. این بدان معنی است که رتبه بندی باید آنچه را که سیستم انجام می‌دهد (عملکرد) و درجه یقین بودن رتبه دهنده‌ها مبنی بر ارائه قابلیت‌ها (تضمین) را دارد.

CC دارای هفت سطح تضمین است، که از EAL1 (پایین‌ترین)، جایی که تست عملکرد انجام می‌شود. از طریق EAL7 (بالاترین)، جایی که تست دقیق انجام شده و طراحی سیستم تأیید می‌شود. طراحان تضمین بکارگرفته شده در CC به شرح زیر است:

- EAL1: به صورت عملکردی تست شده است
- EAL2: از نظر ساختاری تست شده است
- EAL3: به صورت روشمند تست و چک شده است
- EAL4: به صورت طراحی، تست و بررسی شده است
- EAL5: به صورت نیمه رسمی طراحی و تست شده است
- EAL6: طراحی به طور نیمه رسمی تأیید و تست شده است
- EAL7: طراحی به طور رسمی تأیید و تست شده است

CC در طی فرآیند ارزیابی از مفهومی به نام پروفایل یا مشخصات حفاظتی (Protection Profil) استفاده می‌کند. مشخصات حفاظتی مجموعه‌ای از الزامات امنیتی یا اهداف امنیتی را به همراه

فرضیات عملکردی در مورد محیط توصیف می کند. بنابراین، اگر شخصی یک امنیت را شناسایی کرده باشد که در حال حاضر توسط هیچ محصولی مورد توجه قرار نگرفته است، می تواند پروفایل حفاظتی را که الزام و راه حل و کلیه مواردی را که می تواند در حین توسعه سیستم اشتباه باشد را بنویسد. این مشخصات می تواند برای هدایت توسعه محصول جدید استفاده شود. مشخصات حفاظتی شامل عناصر زیر است:

- عناصر توصیفی *Descriptive elements*: نام مشخصات (Profile) و شرح مشکل امنیتی است که باید حل شود.
- *Rationale* منطقی: توجیه مشخصات و توضیحات مفصل تر از مسئله دنیای واقعی که باید حل شود. محیط، فرضیات استفاده و تهدیدات همراه با راهنمایی سیاست امنیتی است که توسط محصولات و سیستم هایی که با این پروفایل سازگار هستند، پشتیبانی می شود.
- *Functional requirements* الزامات عملکردی: ایجاد مرز محافظت، به معنای تهدیدات یا سازش هایی که در این مرز وجود دارد که باید با آن مقابله کرد. محصول یا سیستم باید مرز را اجرا کند.
- *Development assurance requirements* الزامات تضمین توسعه: شناسایی الزامات خاص که محصول یا سیستم باید طی مراحل توسعه از طرح تا اجرا، آن را برآورده کند.
- الزامات ضمانت ارزیابی *Evaluation Assurance Requirements*: تعیین نوع و شدت ارزیابی.

نتیجه پیروی از این روند یک هدف امنیتی (Security Target) خواهد بود. این نتیجه توضیحات فروشنده درباره آنچه محصول از نقطه نظر امنیتی می باشد را در جدول آورده است. گروه بندی های واسطه ای از الزامات امنیتی که در طول مسیر برای رسیدن به هدف امنیتی ایجاد می شود، بسته ها (Packages) نامیده می شوند.

استانداردهای پیاده سازی امنیت Security Implementation Standards

شناختن استانداردهای پیاده سازی امنیت که توسط نهادهای بین المللی منتشر شده برای یک متخصص امنیتی بسیار ضروری است. علاوه بر این، متخصصان امنیت باید استانداردهای موجود در صنعت را که برای سازمانهایشان اعمال می شود، بررسی کنند. این استانداردها شامل ISO / IEC 27001، PCI-DSS و 27002 است.

ISO/IEC 27001

ISO/IEC 27001:2013 جدیدترین نسخه استاندارد ۲۷۰۰۱ است و یکی از رایج ترین استانداردهایی است که توسط آن، سازمان‌ها مجوز صدور گواهی برای امنیت اطلاعات را دریافت می‌کنند. این راهنمایی در مورد چگونگی اطمینان از سیستم مدیریت امنیت اطلاعات سازمان Information security management system (ISMS) که به درستی ساخته، اداره، نگهداری و پیشرفت می‌کند، که شامل اجزای زیر است:

- دامنه ISMS
 - سیاست امنیت اطلاعات
 - فرآیند ارزیابی ریسک و نتایج آن
 - فرایند رفتار ریسک و تصمیمات آن
 - اهداف امنیت اطلاعات
 - صلاحیت پرسنل امنیت اطلاعات
 - اسناد مربوط به ISMS که لازم است
 - برنامه ریزی عملیاتی و کنترل اسناد
 - نظارت و اندازه گیری شواهد امنیت اطلاعات
 - برنامه ممیزی داخلی ISMS و نتایج آن
 - بررسی شواهد توسط مدیریت ارشد ISMS
 - شواهد عدم تطابق و اقدامات اصلاحی شناسایی شده
- هنگامی که یک سازمان تصمیم به اخذ مجوز ISO/IEC 27001 می‌گیرد، باید یک مدیر پروژه انتخاب شود تا مطمئن شود که تمام اجزای آن به درستی تکمیل می‌شود.
- برای اجرای ISO/IEC 27001:2013، یک مدیر پروژه باید مراحل زیر را انجام دهد:
- پشتیبانی مدیریت را بدست آورد.
 - تعیین استفاده از مشاورین یا تکمیل اجرای داخلی، و در صورت وجود لیست، استاندارد ۲۷۰۰۱ را خریداری کرده، طرح پروژه را نوشته، ذینفعان را تعیین کرده و سازماندهی مجدد پروژه را انجام دهد.
 - الزامات را مشخص کند.
 - دامنه ISMS، سیاست امنیت اطلاعات و اهداف امنیت اطلاعات را تعریف کند.
 - کنترل اسناد، ممیزی داخلی و رویه‌های اقدامات اصلاحی را توسعه دهد.

- ارزیابی ریسک و درمان ریسک را انجام دهد.
- تهیه بیانیه برنامه کاربردی و برنامه درمان ریسک و پذیرش کلیه ریسک های باقیمانده.
- اجرای کنترل های تعریف شده در برنامه درمان ریسک و حفظ سوابق اجرایی.
- توسعه و اجرای برنامه های پرورش امنیت و آگاهی رسانی.
- پیاده سازی ISMS، حفظ سیاست ها و رویه ها و انجام اقدامات اصلاحی.
- حفظ و نظارت. ISMS
- انجام یک ممیزی داخلی و نوشتن گزارش ممیزی.
- بررسی مدیریت و حفظ سوابق بررسی شده مدیریت.
- یک نهاد صدور گواهینامه و مجوز کامل را انتخاب کند.
- برای بازدیدهای نظارتی سوابق را حفظ کند.

ISO/IEC 27002

ISO/IEC 27002:2013 جدیدترین نسخه استاندارد ۲۷۰۰۲ است و یک کد عملی برای مدیریت امنیت اطلاعات ارائه می دهد. شامل ۱۴ زمینه محتوا می باشد:

- ✓ سیاست امنیت اطلاعات Information security policy
- ✓ سازمان امنیت اطلاعات Organization of information security
- ✓ امنیت منابع انسانی Human resources security
- ✓ مدیریت دارایی Asset management
- ✓ کنترل دسترسی Access control
- ✓ رمزنگاری Cryptography
- ✓ امنیت فیزیکی و محیطی Physical and environmental security
- ✓ امنیت عملیات Operations security
- ✓ امنیت ارتباطات Communications security
- ✓ کسب، توسعه و نگهداری سیستم های اطلاعاتی، Information systems acquisition, development, and maintenance
- ✓ روابط تأمین کننده Supplier relationships
- ✓ مدیریت حادثه امنیت اطلاعات Information security incident management
- ✓ جنبه های امنیت اطلاعات در تداوم کسب و کار Information security aspects of business continuity

✓ انطباق Compliance

استاندارد امنیت داده‌های صنعت کارت پرداخت (PCI-DSS)

PCI-DSS v3.1، ساخته شده در آوریل ۲۰۱۵، جدیدترین نسخه استاندارد PCI-DSS از این نوشتار است، و امنیت داده‌های دارنده کارت را تشویق و تقویت می‌کند و اتخاذ گسترده‌ای از اقدامات مداوم امنیت داده‌ها در سطح جهان را تسهیل می‌کند. شکل ۳-۵ نمای کلی از سطح استاندارد PCI-DSS را نشان می‌دهد.

PCI Data Security Standard–High Level Overview

Build and Maintain a Secure Network and Systems	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters.
Protect Cardholder Data	3. Protect stored cardholder data. 4. Encrypt transmission of cardholder data across open, public networks.
Maintain a Vulnerability Management Program	5. Protect all systems against malware and regularly update anti-virus software or programs. 6. Develop and maintain secure systems and applications.
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know. 8. Identify and authenticate access to system components. 9. Restrict physical access to cardholder data.
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data. 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

شکل ۳-۵: بررسی سطح بالا از PCI-DSS

کنترل‌ها و اقدامات متقابل Controls and Countermeasures

بعد از اینکه سازمان یک الگوی ارزیابی امنیت سیستم و استاندارد پیاده سازی امنیت را اجرا کرد، سازمان باید براساس جدیدترین ارزیابی آسیب پذیری و ریسک انجام شده توسط متخصصان امنیت، از اجرای کنترل‌ها و اقدامات متقابل مناسب اطمینان حاصل کند. شناخت طبقه بندی‌ها و انواع مختلف کنترل دسترسی برای اطمینان از اجرای یک برنامه امنیتی جامع، بسیار ضروری است. امنیت اطلاعات همیشه باید موردی باشد که سازمان آن را ارزیابی و دنبال کند.

قابلیت های امنیت سیستم های اطلاعاتی Security Capabilities of Information Systems سازمان ها باید قابلیت های امنیت سیستم های اطلاعاتی را که پیاده سازی می کنند درک کنند. در این بخش در مورد حفاظت از حافظه، مجازی سازی، مازول پلتفرم مورد اعتماد، واسطها و تحمل خطا بحث می شود.

• محافظت از حافظه Memory Protection

در یک سیستم اطلاعاتی مهمترین منابع، حافظه و ذخیره سازی هستند. داده های آسیب دیده یا فاسد شده در حافظه می تواند باعث از کار افتادن سیستم شود. داده های موجود در حافظه قابلیت فاش شدن دارند در نتیجه باید محافظت شوند. حافظه فرآیندهای در حال اجرا و نخها را از داده تفکیک نمی کند. متخصصان امنیت باید از حالت های پردازنده، لایه بندی، جداسازی فرایند و مخفی کردن داده ها استفاده کنند تا بتوانند داده ها را جدا از هم نگه دارند.

اکثر پردازنده ها از دو حالت پردازنده پشتیبانی می کنند: حالت سرپرست (Supervisor Mode) یا حالت هسته (Kernel Mode) و حالت مشکل یا حالت کاربر (User Mode).

در حالت سرپرست، بالاترین سطح امتیاز در سیستم استفاده می شود تا پردازنده بتواند به تمام سخت افزار و داده های سیستم دسترسی پیدا کند. در حالت مشکل، پردازنده دسترسی به سخت افزار سیستم و داده ها را محدود می کند. فرآیندهای در حال اجرا در حالت سرپرست از فرآیندهایی هستند که از فرایند هایی که در حال اجرا نیستند جدا می شوند. فرآیندهای در حالت سرپرست باید فقط به کارکردهای اصلی سیستم عامل محدود شوند.

یک متخصص امنیت می تواند از لایه بندی Layering برای سازماندهی برنامه نویسی از توابع جداگانه ای که به صورت سلسله مراتبی با هم در تعامل هستند استفاده کند. در بیشتر موارد، هر لایه فقط به لایه های مستقیم در بالا و پایین خود دسترسی دارد.

محافظت از حلقه (Ring protection) رایج ترین اجرای لایه بندی است که حلقه داخلی (حلقه ۰) ممتازترین حلقه و حلقه بیرونی (حلقه ۳) کمترین امتیاز را دارد. هسته یا کرنل سیستم عامل معمولاً با حلقه ۰ اجرا می شود و اپلیکیشن های کاربر معمولاً با حلقه ۳ اجرا می شوند.

یک متخصص امنیت می تواند با تهیه فضاهای آدرس حافظه برای هر فرآیند، فرایندها را از هم جدا کند. سایر فرایندها قادر به دسترسی به فضای آدرس اختصاص داده شده یک فرآیند دیگر نیستند. تمایز نامگذاری و نقشه برداری مجازی به عنوان بخشی از جداسازی فرایند استفاده می شود.

پنهان کردن داده‌ها مانع از مشاهده داده‌ها در یک سطح امنیتی توسط فرآیندهای موجود در سایر سطوح امنیتی می‌شود.

• مجازی سازی Virtualization

امروزه سرورهای فیزیکی به طور فزاینده‌ای به عنوان سرورهای مجازی در همان جعبه فیزیکی (Physical Box) ادغام می‌شوند. شبکه‌های مجازی با استفاده از کلیدهای مجازی حتی در دستگاههای فیزیکی که میزبان این سرورهای مجازی هستند نیز وجود دارند. این سیستم‌های شبکه مجازی و ترافیک آنها را می‌توان به همان روشهای مشابه در یک شبکه فیزیکی با استفاده از زیر شبکه ها، VLANها و البته فایروال‌های مجازی تفکیک کرد. فایروال‌های مجازی نرم افزاری است که بطور خاص برای کار در محیط مجازی نوشته شده است. به طور فزاینده، فروشندگان مجازی سازی مانند VMware بخشی از کد خود را در اختیار فروشندگان امنیتی قرار می‌دهند تا بتوانند فایروال‌ها (و محصولات ضد ویروس) را ایجاد کرده که به طور کاملاً نزدیک با محصول یکپارچه شوند.

به خاطر داشته باشید که در هر محیط مجازی، هر سرور مجازی که در سرور فیزیکی میزبان است باید با مکانیسم‌های امنیتی خاص خود پیکربندی شود. این مکانیزم‌ها شامل نرم افزارهای آنتی ویروس آنتی بد افزار و کلیه آخرین بسته‌های سرویس و بروزرسانی‌های امنیتی برای کلیه نرم افزارهای میزبان شده در ماشین مجازی است. همچنین به خاطر داشته باشید که همه سرورهای مجازی منابع دستگاه فیزیکی را به اشتراک می‌گذارند.

• ماژول بسترهای نرم افزاری قابل اعتماد (Trusted Platform Module (TPM

یک تراشه (Chip) امنیتی نصب شده بر روی مادربردهای رایانه است که وظیفه مدیریت کلیدهای متقارن و نامتقارن، هش‌ها و گواهی‌های دیجیتال را بر عهده دارد. این تراشه خدمات را برای محافظت از گذرواژه‌ها، رمزگذاری درایوها و مدیریت حقوق دیجیتال فراهم می‌کند و دسترسی مهاجمین را به رایانه‌هایی که دارای تراشه TPM هستند، بسیار سخت تر می‌کند.

دو کاربرد خاص از TPM اتصال و مهر موم کردن (Binding , Sealing) است. اتصال در واقع هارد دیسک را از طریق رمزگذاری به یک رایانه خاص "اتصال" می‌دهد. از آنجا که کلید رمزگشایی در تراشه TPM ذخیره شده است، محتویات درایو هارد فقط هنگام اتصال به رایانه

اصلی در دسترس است. اما بخاطر داشته باشید که اگر تراشه TPM خراب شود و نسخه پشتیبان از کلید وجود نداشته باشد، تمام مطالب در معرض خطر قرار می گیرد.

از طرف دیگر مهرموم کردن (Sealing)، سیستم را با یک تنظیمات سخت افزاری و نرم افزاری خاص مهر و موم می کند. این عملکرد مانع از ایجاد هرگونه حمله در سیستم می شود. با این وجود، نصب سخت افزار یا سیستم عامل جدید نیز بسیار سخت تر می شود. سیستم تنها می تواند پس از تأیید TPM، یکپارچگی سیستم را با مقایسه مقدار هش محاسبه شده اصلی روی پیکربندی سیستم (System's Configuration) با مقدار هش پیکربندی آن در زمان بوت، تأیید کند.

TPM شامل حافظه استاتیک یا ایستا و حافظه پویا است که برای خاموش کردن اطلاعات مهم هنگام خاموش شدن رایانه استفاده می شود.

حافظه مورد استفاده در تراشه TPM به شرح زیر است:

✓ کلید تأیید (EK) Endorsement Key (EK): حافظه پایدار نصب شده توسط سازنده که حاوی یک جفت کلید عمومی یا خصوصی است.

✓ کلید ریشه ذخیره سازی (SRK) Storage Root Key (SRK): حافظه پایدار که کلیدهای ذخیره شده در TPM را ایمن می کند.

✓ کلید شناسایی هویت (AIK) Attestation Identity Key (AIK): حافظه پویا که یکپارچگی EK را تضمین می کند.

✓ هش های ثبت تنظیمات بستر یا پلتفرم (PCR) Platform Configuration Register (PCR) hashes: حافظه پویا که داده ها را برای عملکرد مهره موم شده ذخیره می کنند.

✓ کلیدهای ذخیره سازی: حافظه پویا که شامل کلیدهایی است که برای رمزگذاری حافظه رایانه استفاده می شود، از جمله درایوهای سخت، فلش های USB و غیره.

• واسطه ها Interfaces

واسط مکانیسمی است که کاربر برای دستیابی به یک سیستم، یک اپلیکیشن، یک دستگاه یا نهاد دیگر از آن استفاده می کند. بیشتر کاربران فرض می کنند واسط هایی که از آنها استفاده می شود امن هستند. سازمان ها وظیفه دارند تضمین کنند که واسط های امن در شبکه اجرا شده اند. اگر یک نهاد دارای چندین واسط کاربر مانند واسط کاربری گرافیکی، واسط خط فرمان و واسط دسترسی از راه دور باشد، تمام این واسط ها باید احراز هویت مطمئن شوند. درک این

مسئله که تفاوت بین واسطه‌های امن و ناامن، اطمینان و عدم اطمینان واسطه‌ها، جایگزینی واسطه‌های ناامن با واسطه‌های امن، وظیفه متخصص امنیت است.

• تحمل خطا Fault Tolerance

تحمل خطا به سیستم اجازه می‌دهد تا در صورت عدم موفقیت، مولفه‌های درون سیستم به درستی کار کند. به عنوان مثال، ارائه تحمل خطا برای سیستم هارد دیسک شامل استفاده از درایوهای تحمل خطا و آداپتورهای قابل تحمل در برابر خطا است. با این حال، هزینه هرگونه تحمل خطا باید در برابر هزینه دستگاه یا سخت افزار اضافی سنجیده شود. اگر قابلیت‌های امنیتی سیستم‌های اطلاعاتی قابل تحمل نباشد، در صورت عدم موفقیت مکانیسم‌های امنیتی، مهاجمان می‌توانند به سیستم دسترسی پیدا کنند. سازمانها باید هزینه استقرار یک سیستم تحمل خطا را در برابر هزینه هرگونه حمله به سیستم مورد حمله بسنجند. ممکن است تهیه یک مکانیسم امنیتی قابل تحمل در برابر خطا برای محافظت از داده‌های عمومی امری حیاتی نباشد، اما تهیه یک مکانیسم امنیتی قابل تحمل در برابر خطا برای محافظت از داده‌های محرمانه بسیار مهم است.

صدور گواهینامه و اعتبارسنجی Certification and Accreditation

اگرچه این اصطلاحات به عنوان مترادف در مکالمه تصادفی استفاده می‌شوند، اعتبارسنجی و صدور گواهینامه دو مفهوم متفاوت در زمینه سطوح تضمین و رتبه بندی‌ها هستند، اگرچه باهم بسیار ارتباط دارند. صدور گواهینامه مؤلفه‌های سیستم فنی را ارزیابی می‌کند، در حالی که اعتبارسنجی هنگامی اتفاق می‌افتد که کفایت امنیت کلی یک سیستم توسط مدیریت پذیرفته شود.

فرآیند صدور گواهینامه و اعتبارسنجی ملی تضمین اطلاعات The National Information Assurance Certification and Accreditation Process (NIACAP) مجموعه استانداردی از فعالیتها، وظایف عمومی و یک ساختار مدیریتی را برای صدور گواهینامه و اعتبارسنجی سیستمهایی فراهم می‌کند که تضمین اطلاعات و وضعیت امنیتی یک سیستم یا سایت را حفظ می‌کند.

مراحل اعتبارسنجی توسعه یافته توسط NIACAP دارای چهار مرحله است:

- فاز ۱: تعریف Definition

- فاز ۲: تأیید Verification
 - فاز ۳: اعتبار Validation
 - فاز ۴: اعتبارسنجی پس از اعتبار Post Accreditation
- NIACAP سه نوع اعتبارسنجی زیر را تعریف می‌کند:
- نوع اعتبارسنجی نوع اپلیکیشن یا سیستمی را که در تعدادی از مکانهای مختلف توزیع می‌شود ارزیابی می‌کند.
 - اعتبارسنجی سیستم، یک اپلیکیشن یا سیستم پشتیبانی را ارزیابی می‌کند.
 - اعتبارسنجی سایت اپلیکیشن یا سیستم را در یک مکان خاص خود ارزیابی می‌کند.

تعمیر و نگهداری معماری امنیتی Security Architecture Maintenance

متأسفانه پس از ارزیابی یک محصول، تأیید و اعتبارسنجی، داستان تمام نمی‌شود. این محصول بطور معمول با گذشت زمان تکامل می‌یابد و بروز رسانی‌ها پیچ‌هایی برای رسیدگی به مسائل امنیتی جدید بوجود می‌آورند یا عملکردهایی را اضافه می‌کنند و یا اشکالات را برطرف می‌کند. هنگامی که این تغییرات رخ می‌دهد، به عنوان نگهداری مداوم، باید معماری امنیتی حفظ شود. در حالت ایده آل، با توجه به این تغییرات، راه‌حل‌ها باید تحت ارزیابی‌های اضافی، صدور گواهینامه و اعتبارسنجی قرار گیرند، اما در بسیاری موارد فشارهای دنیای واقعی مانع از این مرحله زمانبر می‌شود. این مایه تأسف است، زیرا توسعه دهندگان موارد را برطرف می‌کنند، آنها اغلب از طرح اصلی امنیت دور می‌شوند و سعی می‌کنند در آخرین لحظه، آتش را خاموش کنند. اینجاست که مدل سازی بلوغ اهمیت پیدا می‌کند. بیشتر مدلهای بلوغ مبتنی بر CMMI مؤسسه مهندس نرم افزار است که در فصل ۱ مورد بحث قرار گرفت. این پنج سطح وجود دارد: اولیه، مدیریت شده، تعریف شده، به صورت کمی مدیریت شده و بهینه سازی شده.

ITGI برای رسیدن به سازمانها در برابر بهترین شیوه‌های صنعت و دستورالعمل‌های بین المللی، مدل بلوغ حاکمیت امنیت اطلاعات را تهیه کرد. این مدل شامل شش سطح رتبه بندی، از صفر به پنج است: عدم وجود، اولیه، قابل تکرار، تعریف شده، مدیریت شده و بهینه سازی شده. سطح عدم وجود با هیچ سطح CMMI مطابقت ندارد، اما تمام سطوح دیگر را انجام می‌دهند.

آسیب پذیری‌های معماری امنیتی، طرح‌ها و عناصر راه حل Vulnerabilities of Security Architectures, Designs, and Solution Elements

سازمان‌ها باید آسیب پذیری‌های معماری امنیتی، طرح‌ها و عناصر راه حل را ارزیابی و کاهش دهند. سیستم‌های ناامن در معرض بسیاری از آسیب پذیری‌ها و تهدیدات مشترک هستند. در این بخش به بررسی آسیب پذیری‌های سیستم‌های مبتنی بر مشتری، سیستم‌های مبتنی بر سرور، پایگاه داده‌ها، سیستم‌های توزیع شده، سیستم‌های داده موازی در مقیاس بزرگ، سیستم‌های توزیع شده، سیستم‌های رمزنگاری و سیستم‌های کنترل صنعتی می‌پردازیم.

مبتنی بر مشتری Client-Based

در اکثر شبکه‌ها، سیستم‌های مشتری بیشترین کاربرد را دارند زیرا آنها سیستم‌هایی هستند که کاربران برای دسترسی به منابع به آنها بیشتر اعتماد دارند. سیستم‌های مشتری از سیستم‌های دسکتاپ گرفته لپ تاپ تا دستگاه‌های تلفن همراه از انواع متفاوت هستند. در این بخش عمدتاً به آسیب پذیریهای دسکتاپ و لپ تاپ توجه می‌شود.

از آنجا که سیستم‌های مشتری بسیار پرکار هستند، به نظر می‌رسد که حملات جدید علیه این سیستم‌ها هر روز افزایش می‌یابد. متخصصان امنیت باید اطمینان حاصل کنند که می‌دانند سیستم‌های مشتری به شبکه وصل می‌شوند تا بتوانند مطمئن شوند که کنترل‌های مناسب برای محافظت از آنها انجام شده است.

آسیب پذیری‌های طرف مشتری معمولاً مرورگرهای وب، افزونه‌های مرورگر و ایمیل مشتری‌ها که هدف قرار می‌گیرند. اما آنها همچنین می‌توانند از طریق اپلیکیشن‌ها و سیستم عامل‌هایی که مستقر هستند انجام شود. سیستم‌های مشتری همچنین تمایل دارند که خدمات در معرض نمایش را مستقر کنند که نیازی به آنها نیست. اغلب سیستم‌های مشتری در معرض سرورهای خصمانه قرار می‌گیرند. واقعیت این است که اکثر کاربران عادی امنیت ندارند و غالباً ناخواسته باعث ایجاد مشکلات امنیتی در سیستم‌های مشتری می‌شوند.

معماری امنیتی برای سیستم‌های مشتری باید شامل سیاست‌ها و کنترل‌هایی باشد که مناطق زیر را در بر می‌گیرد:

- بکارگیری سیستم عامل‌های دارای مجوز و پشتیبانی شده. این سیستم عامل‌ها باید با همه پچ‌های فروشنده، بروزرسانی‌های امنیتی و بسته‌های خدمات به روز شوند.

- استقرار نرم افزار ضد بدافزار و آنتی ویروس در هر سیستم مشتری. بروزرسانی های این نرم افزار باید به صورت خودکار باشد تا در مقابل آسیب پذیری های اخیر پوشش داده شود.
 - استقرار فایروال و سیستم شناسایی نفوذی مبتنی بر میزبان روی سیستم های مشتری.
 - استفاده از رمزگذاری درایو برای محافظت از داده های موجود بر روی دیسک های سخت.
 - صدور حساب کاربری با حداقل مجوزهایی که کاربران برای انجام کارهای خود نیاز دارند. کاربرانی که به دسترسی ادمین نیاز دارند باید هم دارای حساب ادمین و هم یک حساب عادی باشند و فقط هنگام انجام وظایف ادمین باید از حساب ادمین استفاده کنند.
 - قبل از استقرار در سطح مشتری، تمام بروزرسانی ها و پچ ها، از جمله موارد مربوط به سیستم عامل ها و اپلیکیشن ها آزمایش شود.
- اپلت یک برنامه کوچک است که یک فعالیت خاص را انجام می دهد. این موتور درون یک ابزار کوچک (Widget) اختصاصی یا یک برنامه بزرگتر، اغلب به عنوان یک افزونه اجرا می شود. اپلت های جاوا و اپلت های ActiveX نمونه هایی از این مورد می باشند. اپلت های مخرب اغلب توسط مهاجمین مستقر می شوند و به نظر می رسد که از منابع قانونی تهیه شده باشند. سپس این اپلت ها می توانند برای به خطر انداختن سیستم مشتری مورد استفاده قرار گیرند. یک متخصص امنیت باید اطمینان حاصل کند که مشتریان فقط اپلت ها را از فروشندگان معتبر دانلود می کنند. علاوه بر این، یک متخصص امنیت باید تضمین کند که هر برنامه ای که شامل اپلت ها می باشد، با جدیدترین نسخه ها به روز شده است.
- یک سیستم مشتری شامل چندین نوع حافظه نهان (کش) محلی است. حافظه نهان (کش) DNS نتایج نمایش داده شدگان DNS را در اینترنت نگه داشته و حافظه پنهانی است که بیشتر مورد حمله قرار می گیرد. مهاجمان ممکن است برای دامنه های معتبر سعی در مسموم کردن حافظه نهان DNS با آدرس های IP غلط داشته باشند. آنها این کار را با ارسال پاسخ DNS مخرب به سیستم آسیب دیده انجام می دهند. مانند بسیاری از موارد دیگر، باید مطمئن شد که سیستم عامل و کلیه اپلیکیشن ها به روز هستند. علاوه بر این، کاربران باید آموزش ببینند که هرگز بر روی لینک های تایید نشده کلیک نکنند. باید توجه داشت همیشه آنها به سایت نشان داده شده در لینک قابل مشاهده اشاره نمی کنند.

مبتنی بر سرور Server-Based

در بسیاری موارد، یک حمله روی عملیات سیستم عامل سرور به جای اپلیکیشن‌های وب که در بالای آن قرار دارند تمرکز دارد. در این بخش، چگونگی اجرای این حملات را با تمرکز بیشتر بر موضوع دستکاری جریان داده بررسی می‌کنیم.

کنترل جریان داده Data Flow Control

حملات نرم افزاری غالباً جریان داده‌های یک برنامه آسیب پذیر را خراب می‌کنند. به عنوان مثال، مهاجمین سرریزهای بافر را اجرا کرده و آسیب پذیریهایی رشته‌ای را فرمت می‌کنند تا داده‌ها را در مکان‌های ناخواسته بنویسند. هدف نهایی خواندن داده‌ها از مکان‌های ممنوعه یا نوشتن داده در مکان‌های حافظه به منظور اجرای دستورات، خراب کردن سیستم یا ایجاد تغییرات مخرب در سیستم است. کاهش مناسب برای این نوع حملات، اعتبارسنجی ورودی مناسب و کنترل جریان داده‌ها است که در سیستم ایجاد می‌شوند.

با توجه به پایگاه داده‌ها به طور خاص، یک معماری Dataflow نمونه‌ای است که نشانه‌های (توکن) دستورالعمل را به واحدهای اجرایی تحویل می‌دهد و توکن‌های داده را به حافظه دارای آدرس محتوا (Content-Addressable Memory (CAM برمی‌گرداند. حافظه سخت افزاری، همانند RAM نیست. برخلاف معماری رایج، نشانه‌های داده یا توکن‌ها به طور دائم در حافظه ذخیره نمی‌شوند. در عوض، این پیام‌های گذرا هستند که فقط در هنگام انتقال به محل ذخیره دستورالعمل Instruction storage وجود دارند، که باعث می‌شود آنها کمتر به خطر بیفتند.

امنیت پایگاه داده Database Security

از بسیاری جهات، یک پایگاه داده، هدف اصلی برای مهاجم است و معمولاً جایی است که اطلاعات حساس در آن قرار دارد. هنگام بررسی امنیت پایگاه داده، باید اصطلاحات زیر را درک کنید: استنتاج، تجمع، آلودگی، انبار داده کاوی و تجزیه و تحلیل داده‌ها.

• استنتاج Inference

استنتاج زمانی اتفاق می‌افتد که هر شخصی به یک سطح اطلاعات دسترسی داشته باشد و به وی اجازه می‌دهد اطلاعات دیگری را در مورد سطح دیگری استنباط کند. تکنیک اصلی کاهش

استنتاج، ضد انعطاف پذیری است، که عبارت است از تهیه نسخه دقیق یک شی (Object) از یک شی دیگر با استفاده از مقادیر مختلف در شی جدید. این امر باعث می شود تا کاربران پایگاه داده سطح پایین از وجود داده های سطح بالاتر هراسی نداشته باشند.

• تجمع Aggregation

تجمع به عنوان جمع آوری یا گردآوری واحدهای اطلاعات در یک سطح حساس و داشتن نتیجه کلی حاصل از داده از سطح حساسیت بالاتری نسبت به اجزای جداگانه تعریف می شود. بنابراین ممکن است تجمیع را به عنوان روشی متفاوت برای دستیابی به همان هدف استنتاج، یعنی یادگیری اطلاعات در مورد داده ها در سطحی که فرد به آن دسترسی ندارد، تصور کنید.

• آلودگی Contamination

به هم آمیختگی یا مخلوط کردن داده های یک سطح حساس یا نیاز به دانستن سطح دیگر است. اجرای مناسب سطوح امنیتی بهترین دفاع در برابر این مشکلات است.

• انبار داده کاوی Data Mining Warehouse

انبار داده ها انبار اطلاعاتی از داده های ناهمگن است، و اجازه می دهد تا منابع چندگانه داده ها نه تنها در یک مکان ذخیره شوند بلکه به گونه ای سازماندهی شوند که افزونگی داده ها کاهش یابد (نرمال سازی داده ها)، و از ابزارهای پیچیده تر داده کاوی برای دستکاری داده ها برای کشف روابط استفاده می شود، که ممکن است قبلاً آشکار نبوده باشد. در کنار مزایایی که ارائه می دهند، همچنین چالش های امنیتی بیشتری را ارائه می دهند.

موارد زیر مراحل کنترلی است که باید در اپلیکیشن های ذخیره سازی داده ها انجام شود:

- جداول خلاصه برای استفاده منظم رصد شود.
- برنامه پاکسازی داده ها نظارت شود.
- داده های مشترک و وفق داده شده بین محیط عملیات و انبار داده جابجا شوند.

سیستم های توزیع شده Distributed Systems

برخی از مسائل امنیتی خاص هنگام کار در برخی از محیط های توزیع شده نیاز به بحث دارند. این بخش شامل سه مورد خاص است که امکان دارد دارای وابستگی های امنیتی باشد.

✓ رایانش ابری Cloud Computing

متمرکز کردن داده‌ها در یک محیط وب است که از هر مکانی و در هر زمان قابل دسترسی است. یک سازمان می‌تواند یک محیط ابری (ابر خصوصی) ایجاد کند یا می‌تواند به یک فروشنده برای ارائه این سرویس (ابر عمومی) پرداخت کند. در حالی که این ترتیب مزایای بسیاری را ارائه می‌دهد، با استفاده از یک ابر عمومی انواع دغدغه‌های امنیتی را معرفی می‌کند. چگونه می‌دانید داده‌های شما از سایر مشتریان جدا نگه داشته می‌شود؟ چگونه می‌دانید داده‌های شما بی خطر است؟ این امر باعث می‌شود بسیاری از امنیت برون سپاری داده هایشان راحت نباشند.

رایانش ابری این روزها شامل تغییرات و به اشکال مختلفی به وجود می‌آید. ایده اصلی رایانش ابری این است که منابع را در یک مرکز داده مبتنی بر وب در دسترس قرار دهیم تا از هر نقطه به منابع دسترسی پیدا کنیم. وقتی یک شرکت به شرکت دیگری برای میزبانی و مدیریت این محیط می‌پردازد، ما آن را راه حل ابر عمومی می‌نامیم. وقتی شرکت‌ها خودشان این محیط را میزبانی می‌کنند، ما آن را راه حل ابری خصوصی می‌نامیم.

وقتی تصمیم باید بین دو معماری اتخاذ شود، معامله ایجاد می‌شود. راه حل خصوصی بیشترین کنترل را در مورد ایمنی داده‌های شما فراهم می‌کند، اما همچنان کارکنان و دانش به استقرار، مدیریت و راه حل ایمن سازی نیاز دارند. یک ابر عمومی ایمنی داده‌های شما را در دست شخص ثالث قرار می‌دهد، اما آن شخص غالباً در زمینه محافظت از داده‌ها در این محیط و مدیریت محیط ابر، تواناتر و دانش بیشتری دارد.

ذخیره سازی ابری داده‌ها را روی یک سرور مرکزی قرار می‌دهد، اما تفاوت اصلی در این است که داده‌ها از هر کجا و در بسیاری موارد از انواع مختلف دستگاه قابل دسترسی هستند.

علاوه بر این، راه حل‌های ابری معمولاً تحمل خطا را ارائه می‌دهند.

باید با چهار راه حل ابری آشنا باشید:

○ *ابر خصوصی Private cloud*: این یک راه حل تحت مالکیت و مدیریت یک شرکت بوده و صرفاً برای استفاده شرکت است. این ابر بیشترین کنترل و امنیت را فراهم کرده و همچنین برای سخت افزار و تخصص نیاز به بزرگترین سرمایه گذاری دارد.

○ *ابر عمومی Public cloud*: راه حل ارائه شده توسط شخص ثالث است. این ابر جزئیات را برای شخص ثالث بارگذاری می‌کند اما از کنترل خارج می‌شود و می‌تواند مسائل امنیتی را معرفی کند. به طور معمول شما یک مستاجر هستید که با دیگران فضا را به

اشتراک می‌گذارید، و در بسیاری موارد نمی‌دانید که داده شما از نظر فیزیکی در کجا نگهداری می‌شود.

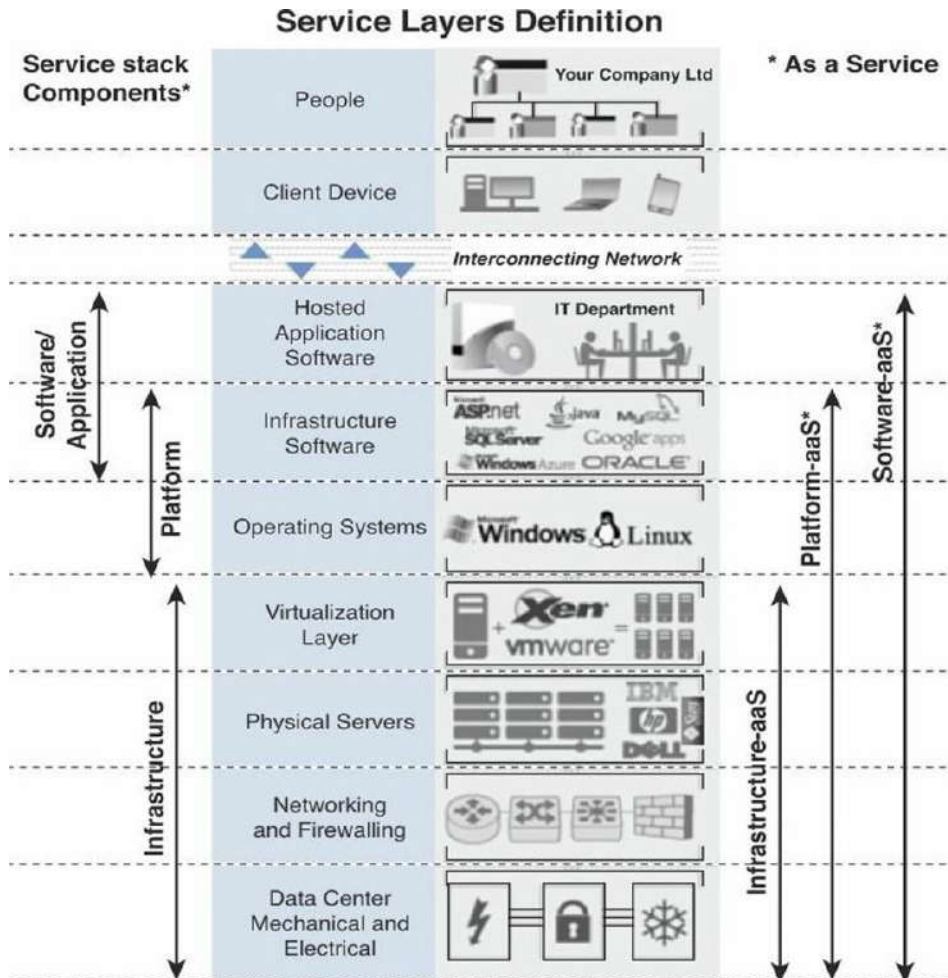
○ هیبریدی *Hybrid*: این راه حل ترکیبی از ابر خصوصی و عمومی است. به عنوان مثال، شاید شما فقط از تاسیسات ارائه دهنده استفاده می‌کنید اما هنوز هم داده‌ها را خودتان مدیریت می‌کنید.

○ جامعیت *Community*: یک راه حل است که توسط گروهی از سازمانها اداره می‌شود که ابر را برای یک هدف مشترک ایجاد می‌کنند، شاید برای رسیدگی به یک دغدغه مشترک از قبیل تطابق نظم است.

وقتی یک راه حل عمومی انتخاب می‌شود، می‌توانید سطوح مختلف خدمات را خریداری کنید. برخی از این سطوح عبارتند از:

- زیرساخت به عنوان یک سرویس *Infrastructure as a service (IaaS)*: فروشنده را که بستر سخت افزاری یا مرکز داده را در اختیار شما قرار می‌دهد و شرکت نصب و مدیریت سیستم عامل‌ها و سیستم‌های کاربردی خود را انجام می‌دهند. فروشنده به سادگی امکان دسترسی به مرکز داده را فراهم می‌کند و دسترسی را حفظ می‌کند.
- بسترهای نرم‌افزاری به عنوان یک سرویس *Platform as a service (PaaS)*: فروشنده را که بستر سخت افزار یا مرکز داده و نرم افزاری را که روی سیستم عامل اجرا می‌شود، درگیر می‌کند. و شامل سیستم عامل‌ها و نرم افزار زیرساختی است. باید توجه داشت که شرکت هنوز درگیر مدیریت سیستم است.
- نرم‌افزار به عنوان یک سرویس *Software as a service (SaaS)*: فروشنده را در ارائه راه حل کامل درگیر می‌کند. این درگیری شامل سیستم عامل، نرم افزار زیرساختی و اپلیکیشن است. به عنوان مثال ممکن است یک سیستم ایمیل برای شما فراهم شود، به موجب آن فروشنده می‌تواند همه چیز را برای شما میزبانی و مدیریت کند.

شکل ۳-۶ روابط این خدمات با یکدیگر را نشان می‌دهد.

**Notes:**

Brand names for illustrative/example purposes only, and examples are not exhaustive.

* Assumed to incorporate subordinate layers.

شکل ۳-۶: رایانش ابری

رایانش مشبک (Grid Comptting) فرآیند بهره برداری از توان CPU ماشین‌های فیزیکی متعدد برای انجام کار است. در برخی موارد، ممکن است سیستم‌های مجزا به مجاز به خروج و ورود مجدد به شبکه باشند. اگرچه مزیت قدرت پردازش اضافی فوق العاده است، اما باید امنیت داده‌هایی را که ممکن است در ماشین‌هایی که در شبکه وارد می‌شوند و از آنجا خارج می‌شوند، مورد توجه

قرار داد. بنابراین، رایانش مشبک هنگامی که محرمانه بودن داده ها یک مسئله کلیدی است، یک اجرای امن نیست.

رایانش همتا Peer-to-Peer Computing

هر راه حل مشتری یا سرور که در آن هر پلتفرم یا بستر ممکن است به عنوان مشتری یا سرور یا هر دو عمل کند، رایانش همتا نامیده می شود. نمونه بارز این مورد، پیام فوری Instant Messaging (IM) است. این پیاده سازیها موضوعات امنیتی را ارائه می دهند که خود را در یک سرویس مشتری / سرور استاندارد ارائه نمی دهند. در بسیاری از موارد، این سیستم ها خارج از کنترل عادی ادمین های شبکه هستند.

و می تواند مشکلاتی مانند موارد زیر را ایجاد کند:

- ویروس ها، کرم ها و اسب های تروجان را می توان از طریق نقطه ورودی به شبکه ارسال کرد.
- در بسیاری موارد، عدم احراز هویت قوی امکان جعل حساب را می دهد.
- حملات و حملات سرریز بافر با استفاده از بسته های ناقص گاهی می تواند موفقیت آمیز باشد.

اگر این سیستم ها باید در محیط قابل تحمل باشند، دستورالعمل های زیر باید رعایت شود:

- سیاست های امنیتی باید به استفاده صحیح از این برنامه ها پرداختند.
- کلیه سیستم ها باید دارای فایروال و محصولات آنتی ویروس باشند.
- فایروال ها برای مسدود کردن ترافیک IM ناخواسته پیکربندی شوند.
- در صورت امکان، فقط به محصولات که رمزگذاری می شوند، اجازه داده شود.

سیستم های داده موازی با مقیاس بزرگ Large-Scale Parallel Data Systems

بیشتر سیستم های داده موازی در مقیاس بزرگ برای رسیدگی به مشکلات علمی و صنعتی از قبیل کنترل ترافیک هوایی، دفاع موشکی بالستیک، تجزیه و تحلیل تصویر ماهواره ای، هدایت موشک و پیش بینی هوا طراحی شده اند. آنها به قدرت پردازش عظیم نیاز دارند. از آنجا که داده ها در این سیستم ها خیلی سریع مورد تجزیه و تحلیل قرار می گیرند، اغلب تشخیص و جلوگیری از حمله مداوم دشوار است. این نوع سیستم ها باید راهی برای تقسیم پرس و جوها در چندین گره Node موازی پیدا کنند تا پرس و جوها به صورت موازی پردازش شوند.

از آنجا که این سیستم‌های داده موازی غالباً دارای چندین سازمان هستند، متخصصان امنیت باید هر زمان که سازمانهایشان در سیستم‌های داده موازی در مقیاس بزرگ فعالیت می‌کنند، زمینه‌های اعتماد، حفظ حریم خصوصی و امنیت عمومی را در نظر بگیرند. موضوعات مرتبط با اعتماد مانند موارد زیر باید در شبکه‌های قابل اعتماد در نظر گرفته شود:

- تأیید کلید
- خدمات انکار سرویس (DoS) مبتنی بر اعتماد برای کاهش نشت اطلاعات
- موضوعات مربوط به حریم خصوصی که باید مورد توجه قرار گیرند شامل موارد زیر است:
 - احراز هویت از راه دور
 - کنترل دسترسی غیر متمرکز
 - پنهان کردن ترافیک
 - رمزنگاری مجموعه در مقیاس بزرگ
- سایر موارد امنیتی عمومی که باید مورد توجه قرار گیرد، شامل اعتبار کاربر متناقض و مجوزها و موضوعات اشتراک داده مربوط به استفاده از رمزنگاری (Cryptography) است.

سیستم‌های رمزنگاری Cryptographic Systems

با طراحی، سیستم‌های رمزنگاری وظیفه رمزگذاری داده‌ها را برای جلوگیری از افشای داده بر عهده دارند. متخصصان امنیت باید اطمینان دهند که در صورت امکان سازمان آنها از آخرین نسخه الگوریتم رمزنگاری استفاده می‌کند. هنگامی که سازش یک الگوریتم رمزنگاری شناخته شود، دیگر نباید از این الگوریتم استفاده شود.

سیستم‌های کنترل صنعتی Industrial Control Systems

سیستم‌های کنترل صنعتی (ICS) یک اصطلاح کلی است که شامل چندین نوع سیستم کنترل است که در تولید صنعتی مورد استفاده قرار می‌گیرند. گسترده ترین، کنترل نظارت و دستیابی به داده‌ها SCADA Supervisory control and data acquisition است.

SCADA سیستمی است که با سیگنال‌های رمزگذاری شده از طریق کانال‌های ارتباطی کار می‌کند تا امکان کنترل تجهیزات از راه دور را فراهم کند، و شامل اجزای زیر است:

- ✓ سنسورها (حسگرها) *Sensors*: سنسورها معمولاً دارای I/O دیجیتال یا آنالوگ هستند و به شکلی نیستند که بتواند به راحتی در مسافت‌های طولانی ارتباط برقرار کند.

✓ واحدهای ترمینال از راه دور (RTUs: Remote terminal units) ها به حسگرها متصل می شوند و داده های سنسور را به داده های دیجیتالی از جمله سخت افزار مسافت سنج تبدیل می کنند.

✓ کنترل کننده های منطقی قابل برنامه ریزی (Programmable logic controllers): PLC ها به سنسورها متصل می شوند و داده های سنسور را به داده های دیجیتالی تبدیل می کنند. آنها شامل سخت افزار مسافت سنج نمی شوند.

✓ سیستم مسافت سنجی (Telemetry system): سیستم هایی مانند RTU ها و PLC ها را به مراکز کنترل و شرکت متصل می کند.

✓ واسطه انسانی (Human interface): چنین واسطی داده ها را به اپراتور ارائه می دهد. ICS ها باید به طور ایمن از شبکه های دیگر به عنوان یک لایه امنیتی تفکیک می شوند. ویروس Stuxnet به SCADA که برای کنترل و نظارت بر فرایندهای صنعتی به کار برده شده است. اجزای SCADA اهداف ممتازی برای حملات سایبری محسوب می شوند. با استفاده از Cyber tools می توان یک فرایند صنعتی را تخریب کرد. این ایده برای حمله به نیروگاه هسته ای نطنز به منظور دخالت در برنامه هسته ای ایران بود.

با توجه به اهمیت سیستمها، دسترسی فیزیکی به سیستمهای مبتنی بر SCADA باید کاملاً کنترل شود. سیستم هایی که امنیت IT را برای کنترل های دسترسی فیزیکی مانند سیستم های خرابکاری و نظارت تصویری ادغام می کنند، باید مستقر شوند. علاوه بر این، راه حل باید با ابزارهای امنیتی موجود اطلاعات مانند مدیریت log و IDS / IPS یکپارچه شود. یک انتشار مفید توسط NIST، انتشارات ویژه 82-800، توصیه هایی را در مورد امنیت ICS ارائه می دهد. مشکلات مربوط به این سیستم های نوظهور شامل موارد زیر است:

- تغییرات لازم در سیستم ممکن است ضمانت را باطل کند.
- محصولات ممکن است پس از اتمام با امنیت به بازار عرضه شوند.
- بازده سرمایه گذاری ممکن است ده ها سال طول بکشد.
- در مورد این سیستم ها مقررات کافی وجود ندارد.

آسیب پذیری در سیستم های مبتنی بر وب Vulnerabilities in Web-Based Systems

با وجود همه تلاشها برای طراحی معماری وب امن، حملات به یک سیستم مبتنی بر وب هنوز هم رخ می دهد و هنوز هم موفقیت آمیز است. در این بخش برخی از انواع متداول حملات از

جمله قلاب‌های نگهدارنده، حملات زمان بررسی / زمان استفاده، حملات مبتنی بر وب و مسائل XML، SAML و OWASP را بررسی می‌کنیم.

قلاب‌های نگهدارنده Maintenance Hooks

از دیدگاه توسعه نرم افزار، قلاب نگهدارنده مجموعه‌ای از دستورالعمل هاست که درون آن کد ساخته شده است و به کسی که دانش "درب پشت Back door" را دارد اجازه می‌دهد تا از دستورالعمل‌های مربوط به اتصال برای مشاهده و ویرایش کد بدون استفاده از کنترل دسترسی عادی استفاده کند. در بسیاری موارد، قلاب‌های نگهدارنده درجایی قرار می‌گیرند تا بتوانند مشتری را آسانتر پشتیبانی کنند. در موارد دیگر، برای کمک به آزمایش و پیگیری فعالیت‌های محصول در آنجا قرار می‌گیرند و بعداً هرگز حذف نمی‌شوند.

توجه داشته باشید

یک حساب نگهدارنده اغلب با قلاب نگهدارنده اشتباه می‌شود. یک حساب کاربری نگهدارنده، یک حساب کاربری Back door است که توسط برنامه نویسان ایجاد شده است تا در یک برنامه خاص یا سیستم عامل خاص، مجوزهای کامل را به هر شخص بدهد. یک حساب کاربری تعمیر و نگهداری معمولاً می‌تواند به راحتی حذف یا غیرفعال شود، اما یک قلاب نگهدارنده واقعی اغلب یک قسمت پنهان از برنامه نویسی است و غیرفعال کردن آن بسیار ساده تر است. هر دوی اینها می‌توانند باعث ایجاد مشکلات امنیتی شوند زیرا بسیاری از مهاجمان ابتدا قلابهای نگهدارنده مستند و حسابهای نگهداری را امتحان می‌کنند. شما از تعداد رایانه هایی که بطور روزانه مورد حمله قرار می‌گیرند شگفت زده می‌شوید زیرا این دو موضوع امنیتی بدون فشار باقی مانده است.

صرف نظر از نحوه ورود قلاب‌های نگهدارنده، آنها می‌توانند در صورت شناخته شدن برای هک‌هایی که می‌توانند از آنها برای دسترسی به سیستم استفاده کنند، مسئله اصلی امنیتی را ارائه دهند. اقدامات متقابل از طرف مشتری برای کاهش خطر وجود دارد:

- با استفاده از یکی از این قلاب‌ها، از یک شناسه میزبان یا IDS میزبان برای ثبت هرگونه تلاش برای دسترسی به سیستم استفاده شود.
- تمام اطلاعات حساس موجود در سیستم رمزگذاری شود.
- ممیزی برای تکمیل IDS انجام شود.

بهترین راه حل برای فروشنده این است که تمام قلاب‌های نگهدارنده را قبل از شروع تولید محصول حذف کند. برای شناسایی و حذف این قلاب‌ها باید بررسی‌های مدون صورت گیرد.

حملات زمان بررسی / زمان استفاده Time-of-Check/Time-of-Use Attacks

حملات زمان بررسی / زمان استفاده، سعی می کنند از توالی رخدادهایی که با اتمام سیستم وظایف مشترک رخ می دهند، استفاده کنند، و همچنین بستگی به دانش وابستگی های موجود در هنگام وقوع یک سری از وقایع در سیستم های پردازش چندگانه دارد. با تلاش برای وارد کردن خود بین حوادث و ایجاد تغییرات، هکر می تواند کنترل نتیجه را بدست آورد. اصطلاحی که اغلب به عنوان مترادف برای حمله زمان بررسی / زمان استفاده بکار برده می شود، شرایط Race می باشد که در واقع یک حمله متفاوت می باشد. در این حمله، هکر خود را بین دستورالعمل ها قرار می دهد، تغییرات را معرفی می کند و ترتیب اجرای دستورالعمل ها را تغییر داده و نتیجه تغییر می کند.

اقدامات متقابل این حملات، ساختن مجموعه های مهم دستورالعمل اتمی است. این بدان معناست که آنها یا به صورت کلی اجرا می شوند یا با تغییراتی که ایجاد می کنند به عقب برمی گردند یا از آن جلوگیری می کنند. هنگام انجام این مجموعه دستورالعمل ها از آنها استفاده یا لمس خواهد شد و بهتر است که سیستم دسترسی به موارد خاص را مسدود کند.

حملات مبتنی بر وب Web-Based Attacks

حملات به زیرساخت های امنیت اطلاعات با گذشت زمان به طور پیوسته تکامل می یابد، و آخرین حملات از حملات مبتنی بر اپلیکیشن های وب پیچیده تر استفاده می کنند. دفاع از این حملات با رویکردهای سنتی با استفاده از فایروال های محیطی دشوارتر شده است. تمام حملات اپلیکیشن وب با انجام حداقل یک درخواست عادی یا یک درخواست اصلاح شده با هدف استفاده از اعتبار ورودی نامناسب و پارامترها یا دستورالعمل جعل عملکرد عمل می کنند. در این بخش، دو زبان نشانه گذاری وب با توجه به شایستگی امنیتی آنها مقایسه می شود و در ادامه نگاهی به سازمانی می اندازیم که آگاهانه از فناوری امنیتی پشتیبانی می کند.

XML

Expandible Markup Language (XML) امروزه پرکاربردترین زبان وب است که مورد انتقاد قرار گرفته است. روشی که در حال حاضر برای امضای داده ها برای تأیید صحت آن استفاده شده و برخی توصیف کرده اند که ناکافی می باشد و سایر انتقادات به طور کلی به معماری امنیت

XML هدایت شده است. در بخش بعدی، گسترش این زبان که سعی در رفع برخی از این دغدغه‌ها دارد، مورد بحث قرار می‌گیرد.

SAML

Security Marks Language Markup (SAML) یک فرمت داده استاندارد باز مبتنی بر XML برای تبادل داده‌های احراز هویت و مجوز بین طرفین، به ویژه، بین ارائه دهنده هویت و ارائه دهنده خدمات است. مسئله اصلی که روی آن تمرکز می‌کند، درمروگر وب مشکل اول ورود به سیستم single sign-on (SSO) است.

SSO توانایی احراز هویت یکباره برای دسترسی به چندین مجموعه داده است. SSO در سطح اینترنت معمولاً با کوکی‌ها انجام می‌شود، اما گسترش مفهوم فراتر از اینترنت، منجر به رویکردهای متناسب بسیاری شده است که سازگار نیستند. هدف SAML ایجاد استاندارد برای این فرآیند است.

OWASP

پروژه امنیت برنامه وب باز (OWASP) Open Web Application Security Project یک پروژه امنیتی برنامه منبع باز است که گروهی از دستورالعمل‌ها، روش‌های آزمایش و ابزارهایی را برای کمک به امنیت وب ایجاد می‌کند. آنها همچنین به دلیل حفظ ده رده لیست برتر از ریسک‌های امنیتی اپلیکیشن‌های وب شناخته شده‌اند.

آسیب پذیری در سیستم‌های سیار Vulnerabilities in Mobile Systems

امروزه تقریباً همه افراد دارای یک دستگاه تلفن همراه هستند. همانطور که با افزایش محبوبیت دستگاه‌های تلفن همراه، مسائل امنیتی مربوط به آن دستگاه‌ها افزایش یافته است. متخصصان امنیت به دلیل استفاده بیشتر از دستگاه‌های تلفن همراه در کنار این واقعیت که بسیاری از این دستگاه‌ها با استفاده از شبکه‌های عمومی با کمترین امنیت و یا عدم امنیت، با چالش‌های منحصر به فردی روبرو هستند.

آموزش کاربران در مورد ریسک‌های مربوط به دستگاه‌های تلفن همراه و اطمینان از اجرای اقدامات امنیتی مناسب می‌تواند به حفاظت در برابر تهدیدات مربوط به این دستگاه‌ها کمک کند. برخی از دستورالعمل‌هایی که باید برای کاربران دستگاه تلفن همراه ارائه شود شامل اجرای پین

قفل دستگاه، استفاده از رمزگذاری دستگاه، پیاده سازی خدمات موقعیت مکانی GPS و اجرای پاک کردن از راه دور است. همچنین، کاربران باید نسبت به دانلود برنامه های بدون اطمینان احتیاط کرده و از یک منبع معتبر دانلود کنند. در سال های اخیر، سیستم های مدیریت دستگاه های تلفن همراه (MDM) و سیستم های مدیریت برنامه تلفن همراه (MAM) در شرکت ها رایج شده اند. این سیستم ها برای اطمینان از اینکه سازمان می تواند تنظیمات دستگاه تلفن همراه، اپلیکیشن ها و سایر پارامترها را هنگام اتصال این دستگاهها به شرکت را کنترل کنند، پیاده سازی می شود.

تهدیداتی که با معرفی دستگاه های تلفن همراه شخصی (تلفن های هوشمند و تبلت ها) به شبکه یک سازمان ارائه می شود عبارتند از:

- مرورگر ناامن وب
- اتصال Wi-Fi ناامن
- دستگاه های از دست رفته یا سرقت شده که داده های شرکت را در اختیار دارند
- دانلود و نصب برنامه های فاسد
- پیچ های امنیتی مفقودی
- بروز رسانی مداوم دستگاه های شخصی
- استفاده از خدمات موقعیت مکانی

در حالی که رایج ترین انواع اطلاعات شرکت های ذخیره شده در دستگاه های شخصی، ایمیل های شرکت ها و اطلاعات تماس با شرکت هستند، توجه به این نکته نگران کننده است که تقریباً نیمی از این دستگاهها همچنین حاوی داده های مشتری، اعتبار ورود به شبکه و داده های شرکتی هستند که از طریق اپلیکیشن های کسب و کار قابل دسترسی هستند.

برای پرداختن به این مسائل و برآوردن تقاضای روزافزون و استفاده از دستگاه های شخصی، بسیاری از سازمان ها سیاست هایی را برای دستگاه شخصی خود (BYOD) ایجاد می کنند. در حمایت از ابتکار عمل Bring-your-own-device (BYOD)، یک متخصص امنیت باید در نظر داشته باشد که کاربران بی دقت تهدیدی بزرگتر از هکرها محسوب می شوند. کاربران نه تنها در حفظ و بروز رسانی های امنیتی و پیچ های دستگاهها کمتر تلاش می کنند، بلکه اغلب وسایل جدید را نیز خریداری می کنند. این عوامل، کنترل بر امنیت شبکه هایی که در آن امکان استفاده از این دستگاهها وجود دارد را دشوار می کند.

ابزارهای متمرکز مدیریت دستگاه تلفن همراه یک راه حل سریع در حال رشد است. برخی از این ابزارها از قابلیت‌های مدیریت سرور پیام رسانی بهره می‌برند و برخی دیگر ابزارهای شخص ثالث هستند که می‌توانند مارک‌های مختلف دستگاه را مدیریت کنند. مدیر سیستم‌ها توسط سیسکو نمونه‌ای است که با سرویس‌های ابری Cisco Meraki ادغام می‌شود. نمونه دیگر دستگاه‌های IOS Apple Configurator است. یکی از چالش‌های اجرای چنین سیستمی این است که همه دستگاه‌های شخصی ممکن است از رمزگذاری بومی و یا فرایند مدیریت پشتیبانی نکنند.

معمولاً ابزارهای مدیریت متمرکز دستگاه‌های تلفن همراه به صورت متفاوتی دستگاه‌های تلفن همراه شخصی و صادر شده توسط شرکت را اداره می‌کنند. برای دستگاه‌های صادر شده توسط سازمان، یک اپلیکیشن مشتری معمولاً پیکربندی و امنیت کل دستگاه را مدیریت می‌کند. اگر دستگاه وسیله شخصی است که از طریق ابتکار BYOD مجاز است، اپلیکیشن معمولاً پیکربندی و امنیت خود و داده‌های آن را کنترل می‌کند. اپلیکیشن و داده‌های آن از سایر اپلیکیشن‌ها و داده‌ها sandbox شده اند. نتیجه این که داده‌های سازمان و داده‌های کاربر در صورت دزدی دستگاه محافظت می‌شوند.

علیرغم استفاده از ابزار متمرکز مدیریت دستگاه تلفن همراه، سیاست BYOD باید موارد زیر را در سیاست امنیتی سازمان شامل شود:

- موارد استفاده مجاز از دستگاه‌های شخصی در شبکه شرکتها شناسایی شود.
- لیستی از اپلیکیشن‌های مجاز را در دستگاه‌ها ایجاد کرده و روشی برای جلوگیری از نصب اپلیکیشن‌هایی که در این لیست قرار ندارند تهیه شود (برای مثال، سیاست‌های محدودیت نرم افزار).

- اطمینان حاصل شود که سطح بالایی از مدیریت در سطح پشتیبانی قرار دارد.
- سیاست‌های جدید را به کاربران آموزش دهند.

در فرآیند استقرار و پشتیبانی از راه حل سیار، این دستورالعمل‌ها دنبال می‌شود:

- تضمین شود که راه حل انتخاب شده از راه دور کنترل‌های امنیتی را پشتیبانی می‌کند.
- تضمین شود که فروشنده منتخب در تبلیغات عمومی و تصحیح نقص‌های امنیتی سابقه خوبی دارد.

- استقرار ابزار MDM را در اولویت کاری خود قرار دهند.
- در صورت عدم وجود سیستم MDM، فرایندی طراحی شود تا اطمینان حاصل شود که تمام دستگاه‌ها در پیچ‌های امنیتی به روز نگه داشته می‌شوند.

- با تغییر فن آوری و رفتارها، این سیاست به روز شود.
 - از همه کارکنان بخواهید موافقت کنند که اجازه پاک کردن از راه دور دستگاه های مسروقه یا گمشده را از بین ببرند.
 - دستگاه های روت شده (Android) جیلبریک (iOS) از دسترسی به شبکه به شدت ممنوع شود.
 - در صورت امکان، محصولی انتخاب شود که به صورت زیر پشتیبانی می شود:
 - رمزگذاری درایو حالت جامد (SSD) و رم غیر فرار
 - برای دسترسی به دستگاه به پین نیاز دارد
 - قفل دستگاه هنگام تلاش برای تعداد مشخصی از پین های نادرست
- مانند بسیاری از موضوعات امنیتی دیگر که در این کتاب مورد بحث قرار می گیرد، آموزش کاربر مهم است. یک متخصص امنیت باید مطمئن شوند که کاربران اهمیت امنیت دستگاه تلفن همراه را درک می کنند.
- اگر یک سازمان راه حل MDM یا MAM را پیاده سازی نکند، سیاست امنیتی دستگاه همراه باید حداقل سیاست های زیر را شامل شود:
- نرم افزار ضد بدافزار یا آنتی ویروس در همه دستگاه های تلفن همراه پیاده سازی شود.
 - فقط از ارتباطات امن استفاده شود.
 - از احراز هویت قوی استفاده شود.
 - با هر بار استفاده از دستگاه پس از مدت زمانی از عدم فعالیت (حداکثر ۱۰ دقیقه عدم فعالیت) به یک پین یا مکانیزم ورود به سیستم مجدد نیاز داشته باشد. نرم افزار شخص ثالث محدود شود.
 - GPS و سایر خدمات موقعیت مکانی پیاده سازی شود.
 - ویژگی های قفل از راه دور و پاک کردن از راه دور فعال شود.
 - هرگز دستگاه بدون مراقبت رها نشود.
 - هر وسیله مفقوده یا سرقت شده فوراً گزارش شود.
 - همه گزینه ها، اپلیکیشن ها و سرویس های غیر ضروری، از جمله بلوتوث غیرفعال شود.
 - بطور منظم داده های پشتیبان تهیه شود.
 - همه بروزرسانی ها از منبع تولید کننده دستگاه نصب شود.

آسیب پذیری در دستگاه‌های تعبیه شده و سیستم‌های سایبر- فیزیکی

Vulnerabilities in Embedded Devices and Cyber-Physical Systems

یک سیستم تعبیه شده یک سیستم رایانه‌ای است که اغلب دارای محدودیت‌های محاسباتی (رایانشی) در زمان واقعی که عملکردی اختصاصی در یک سیستم بزرگتر دارد. این دستگاه به عنوان بخشی از دستگاه تعبیه شده است و اغلب شامل قطعات سخت افزاری و مکانیکی است. سیستم‌های تعبیه شده بسیاری از دستگاه‌های مورد استفاده امروز را کنترل می‌کنند و شامل سیستم‌های تعبیه شده در اتومبیل‌ها، سیستم‌های HVAC، هشدارهای امنیتی و حتی سیستم‌های روشنایی هستند. ارتباطات ماشین به ماشین M2M، اینترنت اشیاء IoT و سیستم‌های صنعتی از راه دور کنترل شده باعث افزایش تعداد دستگاه‌های متصل شده که همزمان این دستگاه‌ها را هدف قرار داده اند.

توجه داشته باشید

IoT اصطلاحی برای کلیه اشیاء یا «چیزهایی» است که اکنون با الکترونیک، نرم افزار و اتصال به شبکه تعبیه شده است. به لطف IoT، این اجسام از جمله خودرو، وسایل آشپزخانه و کنترل کننده‌های گرمایشی و تهویه مطبوع می‌توانند داده‌ها را جمع آوری و تبادل کنند. متأسفانه مهندسين اکثر این توانایی‌های اشیاء را فقط برای راحتی و بدون در نظر گرفتن تأثیرات امنیتی، در اختیار قرار می‌دهند. وقتی این اشیاء مستقر شدند، مصرف کنندگان به امنیت فکر نمی‌کنند. که نتیجه راحتی مصرف کننده و ریسک پذیری است. با تکامل IoT، متخصصان امنیت باید بطور فزاینده در تکامل IoT درگیر شوند تا تضمین شود که کنترل‌های امنیتی برای محافظت از این اشیاء و داده‌هایی که جمع آوری و انتقال می‌دهند طراحی شده اند.

از آنجا که سیستم‌های تعبیه شده معمولاً در دستگاه دیگری بدون ورودی Input از یک متخصص امنیت قرار می‌گیرند، امنیت در دستگاه نیز ساخته نمی‌شود. بنابراین، در حالی که امکان برقراری ارتباط دستگاه از طریق اینترنت با یک سیستم تشخیص، خدمات بسیار خوبی را به مصرف کننده ارائه می‌دهد، اغلب اوقات سازنده تصور نکرده است که هکر می‌تواند ارتباطات را معکوس کند و دستگاه را با سیستم تعبیه شده خودش در دست بگیرد. گزارش‌ها حاکی از آن است که افراد قادر به کنترل وسایل با استفاده از سیستم‌های تعبیه شده خود هستند. تولیدکنندگان پیچ‌هایی را منتشر کرده اند که به چنین مواردی می‌پردازند، اما همه مالکان وسایل تاکنون درخواست نکرده و یا حتی از پیچ‌های آنها اطلاع ندارند.

با افزایش محبوبیت M2M و IoT، متخصصان امنیت می توانند انتظار افزایش حوادثی از این دسته را داشته باشند. انتظار می رود یک متخصص امنیت از آسیب پذیری های این سیستم ها و چگونگی اعمال کنترل برای کاهش ریسک سازمان مطلع شود.

رمزنگاری Cryptography

در حالی که مهندسی امنیت شامل امنیت کلیه دستگاههایی است که یک سازمان پیاده سازی می کند، فقط امنیت دستگاه ها کافی نیست. سازمانها همچنین باید داده های موجود در دستگاه های خود را همانطور که از طریق شبکه منتقل می شوند، تضمین کنند. رمزنگاری شامل استفاده از الگوریتم ها برای محافظت از داده ها است. در این بخش مفاهیم رمزنگاری، چرخه عمر رمزنگاری، تاریخچه رمزنگاری، ویژگی های رمزنگاری و مدیریت کلید مورد بحث قرار می گیرد.

توجه داشته باشید

Cleartext یک داده قابل خواندن است که بصورت واضح و روشن در یکجا ذخیره شده است و

به بیان دیگر رمزنگاری نشده است

Plaintext در واقع ورودی یک الگوریتم رمزنگاری است، هر داده ای به یک الگوریتم رمزنگاری

وارد شود به عنوان Plaintext شناخته می شود

Ciphertext داده های غیرقابل خواندنی که از خروجی یک الگوریتم رمزنگاری خارج می شوند

Ciphertext هستند.

Plain Text واژه با فاصله نوشته شده است دقت کنید، به این معنی است که متن یا text هنوز

قالب بندی نشده است، یا برای مثال هنوز یک فایل متنی ساده است.

Clear Text واژه با فاصله نوشته شده است دقت کنید، وقتی متنی به سادگی قابل درک و

فهم باشد به آن Clear Text گفته می شود، مثلا جمله من ITPRO را دوست دارم یک جمله واضح و شفاف و قابل فهم است.

اگر داده cleartext باشد احتمالا Plain text هم می تواند باشد و به عنوان plaintext نیز می شود از آن استفاده کرد اما قطعا ciphertext نیست، اگر داده plaintext است باید plain text نیز باشد، امکان اینکه cleartext هم باشد وجود دارد و ممکن است در آینده تبدیل به ciphertext نیز بشود، داده که ciphertext است حتما باید plain text باشد و به عنوان plaintext هم می تواند استفاده شود ولی قطعا cleartext نیست.

مفاهیم رمزنگاری Cryptography Concepts

یک متخصص امنیت باید بسیاری از اصطلاحات و مفاهیم مربوط به رمزنگاری را درک کند. این اصطلاحات اغلب هنگام بحث در مورد رمزنگاری استفاده می‌شود:

- رمزگذاری *Encryption*: فرایند تبدیل داده‌ها از plaintext به ciphertext. همچنین به آن Enciphering نیز گفته می‌شود.
- رمزگشایی *Decryption*: فرایند تبدیل داده‌ها از ciphertext به plaintext همچنین به آن Deciphering نیز گفته می‌شود.
- کلید *Key*: پارامتری که تبدیل plaintext به ciphertext یا برعکس را کنترل می‌کند. تعیین داده‌های plaintext بدون کلید غیرممکن است. کلیدها می‌توانند هم عمومی و هم خصوصی باشند. از آن به عنوان رمزنگاری نیز یاد می‌شود.
- همگام *Synchronous*: وقتی بی درنگ رمزگذاری یا رمزگشایی رخ می‌دهد.
- ناهمگام *Asynchronous*: هنگامی که درخواست‌های رمزگذاری یا رمزگشایی در یک صف پردازش می‌شوند. در این روش از پردازنده‌های سخت افزاری و چندگانه در این فرآیند استفاده می‌شود.
- متقارن *Symmetric*: یک روش رمزگذاری که به موجب آن یک کلید خصوصی تنها داده‌ها را رمزگذاری و رمزگشایی می‌کند. همچنین به آن رمزگذاری کلید خصوصی یا مخفی نیز گفته می‌شود.
- نامتقارن *Asymmetric*: یک روش رمزگذاری است که به موجب آن یک جفت کلید، یک کلید خصوصی و یک کلید عمومی، رمزگذاری و رمزگشایی را انجام می‌دهد. یک کلید رمزگذاری را انجام می‌دهد، در حالی که کلید دیگر رمزگشایی را انجام می‌دهد. به آن رمزگذاری کلید عمومی نیز گفته می‌شود.
- امضای دیجیتال *Digital signature*: روشی برای تأیید هویت ارسال کننده و یکپارچگی پیام. این پیام به عنوان ورودی تابع هش عمل می‌کند، و کلید خصوصی ارسال کننده مقدار هش را رمزگذاری می‌کند. گیرنده می‌تواند محاسبه هش را بر روی پیام دریافتی انجام دهد تا اعتبار پیام را تعیین کند.
- Hash: یک عملکرد یک طرفه است که یک پیام را به یک مقدار هش کاهش می‌دهد. مقایسه ارزش هش فرستنده با مقدار هش گیرنده، یکپارچگی پیام را تعیین می‌کند.

اگر مقادیر هش حاصل متفاوت باشد، پیام به نوعی تغییر کرده است، مشروط بر اینکه هم فرستنده و هم گیرنده از تابع هش یکسان استفاده کنند.

- **گواهی دیجیتال** *Digital certificate*: یک سند الکترونیکی است که دارنده گواهی را مشخص می کند.
- **متن ساده** *Plaintext*: پیامی در قالب اصلی خود. همچنین به آن متن روشن نیز گفته می شود
- **متن رمزگذاری** *Cipher text*: یک فرم تغییر یافته از پیام است که بدون دانستن کلید و سیستم رمزگذاری استفاده شده قابل خواندن نیست. به آن cryptogram نیز گفته می شود.
- **سیستم رمزنگاری** *Cryptosystem*: کل فرایند رمزنگاری، از جمله الگوریتم، کلید و عملکردهای مدیریت کلید. امنیت سیستم رمزنگاری با اندازه فضای کلیدی و قدرت محاسباتی موجود اندازه گیری می شود.
- **تحلیل رمزنگاری** *Cryptanalysis*: علم رمزگشایی متن رمزگذاری بدون اطلاع قبلی از کلید یا رمزنگاری مورد استفاده. هدف از تحلیل رمزنگاری *Cryptanalysis*، جعل سیگنال ها یا پیام های رمزگذاری شده است که به عنوان سیگنال یا پیام معتبر پذیرفته شود.
- **کلید خوشه بندی** *Key clustering*: هنگامی رخ می دهد که کلیدهای رمزگذاری مختلف متن رمزگذاری شده را از همان پیام متن ساده تولید می کنند.
- **فضای کلیدی** *Key space*: تمام مقادیر کلیدی ممکن هنگام استفاده از یک الگوریتم خاص یا اندازه گیری امنیتی دیگر. یک کلید ۴۰ بیتی 2^{40} مقدار ممکن دارد، در حالی که یک کلید ۱۲۸ بیتی 2^{128} مقدار ممکن دارد
- **تصادم** *Collision*: رخدادی است که وقتی یک تابع hash مقدار هش یکسان را در پیامهای مختلف ایجاد می کند، رخ می دهد.
- **الگوریتم**: یک تابع ریاضی است که داده ها را رمزگذاری و رمزگشایی می کند. به آن رمز cipher نیز گفته می شود.
- **Cryptology**: علمی که ارتباطات و داده های رمزگذاری شده را مطالعه می کند.
- **Encoding**: فرایند تغییر داده ها به فرم دیگری با استفاده از کد.
- **Decoding**: فرایند تغییر یک پیام رمزگذاری شده به قالب (فرمت) اصلی آن.

- **جابجایی Transposition:** فرایند بهم آمیختن (Shuffling) یا تغییر شکل مجدد متن ساده برای مخفی کردن پیام اصلی. همچنین به آن جایگشت (Permutation) نیز گفته می‌شود. به عنوان مثال، AEEGMSS یک نسخه جابه جا شده از MESSAGE است.
- **جایگزینی Substitution:** فرایند تبادل یک بایت در یک پیام برای دیگری. به عنوان مثال، ABCCDEB یک نسخه جایگزینی MESSAGE است.
- **سردرگمی Confusion:** فرایند تغییر یک مقدار کلیدی در هر دوره رمزگذاری است. Confusion اغلب با جانشینی انجام می‌شود. Confusion ارتباط آماری بین متن ساده (plaintext) و متن رمزگذاری شده (Cipher text) را پنهان می‌کند. کلود شانون برای اولین بار در مورد Confusion بحث کرد.
- **انتشار Diffusion:** فرایند تغییر مکان متن ساده در متن رمزنگاری. انتشار اغلب با استفاده از جابجایی انجام می‌شود. کلود شانون اولین بار انتشار را معرفی کرد.
- **اثر بهمن Avalanche effect:** شرایطی که هرگونه تغییر در کلید یا متن ساده، هر چقدر جزئی باشد، متن را به طور قابل توجهی تغییر می‌دهد. هورست فیستل برای اولین بار اثر Avalanche را معرفی کرد.
- **ضریب کار Work factor:** مقدار زمان و منابعی که برای شکستن رمزگذاری لازم است.
- **درب تله Trapdoor:** مکانیسم مخفی است که امکان اجرای تابع معکوس را در یک تابع یک طرفه فراهم می‌کند.
- **تابع یک طرفه One-way function:** یک تابع ریاضی است که می‌تواند از یک جهت آسان تر از جهت دیگر انجام شود.

چرخه عمر رمزنگاری Cryptographic Life Cycle

متخصصان امنیت هنگام در نظر گرفتن اجرای رمزنگاری یا تکنیک‌های رمزگذاری در سازمان، باید نیازهای سازمان را به طور کامل تجزیه و تحلیل کنند. هر تکنیک نقاط قوت و وضعی دارد. علاوه بر این، هر یک اهداف خاصی دارند. تجزیه و تحلیل نیازهای سازمانی را تضمین می‌کند که بهترین الگوریتم برای اجرا را شناسایی کنیم.

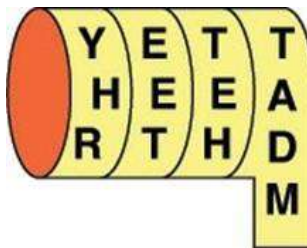
سازمان‌های حرفه‌ای الگوریتم‌ها را مدیریت می‌کنند تا از حمایت لازم مورد نیاز خود مطمئن شوند. ضروری است که متخصصان امنیت، الگوریتم‌هایی را که پیاده سازی می‌کنند، تحقیق کنند و هرگونه اطلاعاتی را از سازمان حاکم در مورد بروزرسانی، بازنشستگی یا جایگزینی برای

الگوریتم های اجرا شده درک کنند. چرخه عمر هر الگوریتم رمزنگاری شامل اجرا، نگهداری و بازنشستگی یا جایگزینی است. هر متخصص امنیت که نتواند اطلاعات به روز در مورد الگوریتم های اجرا شده را بدست آورد، می تواند به اعتبار سازمان و اعتبار شخصی خود در نتیجه سهل انگاری آسیب وارد کند.

تاریخچه رمزنگاری

رمزنگاری ریشه در تمدن های باستان دارد. اگرچه راه حل های اولیه رمزنگاری از نظر ماهیت ساده گرایانه بودند، اما آنها قادر بودند وسیله ای برای پنهان کردن پیام ها از دشمنان به رهبران ارائه دهند.

در اشکال آغازین، اکثر روش های رمزنگاری نوعی رمز جایگزینی را اجرا می کردند که در آن هر کاراکتر در الفبا با کاراکتر دیگری جایگزین می شد. یک رمز جایگزینی تک الفبایی تنها از یک الفبا استفاده می کند، و یک رمزگذاری جایگزینی چند الفبایی از الفبای متعدد استفاده می کند. مانند سایر روش های رمزنگاری، رمزهای جایگزینی اولیه با روش های پیچیده تر جایگزین شدند. اسپارتهای رمزهای scytale را ایجاد کردند که از یک ورق پاپیروس پیچیده شده در اطراف میله چوبی استفاده می شد. همانطور که در شکل ۳-۷ نشان داده شده است، باید پیام رمزگذاری شده در اطراف یک میله با اندازه درست پیچیده شود تا رمزگشایی شود.



شکل ۳-۷: رمزنگاری Scytale

سایر پیشرفت های قابل توجه در تاریخ رمزنگاری شامل موارد زیر است:

- ✓ رمزگذاری سزار
- ✓ رمزگذاری Vigenere
- ✓ اصل کرکوف
- ✓ جنگ جهانی دوم انیگما

✓ لوسیفر توسط IBM

• جولیوس سزار و رمز سزار

جولیوس سزار یک رمزگذاری تک الفبایی ایجاد کرد که حروف الفبا را در سه مکان تغییر می‌دهد. این تکنیک بسیار ساده است و تغییرات آن بسیار آسان، زیرا می‌توان کلید (تعداد مکانهایی که الفبای تغییر یافته است) را تغییر داد. از آنجا که بسیار ساده بود، به راحتی می‌توانست مهندس معکوس شود و منجر به توسعه رمزهای چندقطبی شود.

نمونه‌ای از پیام رمزگذاری شده با سزار در شکل ۳-۸ نشان داده شده است. در این مثال حروف الفبا در یک جابجایی سه حرفی اعمال می‌شود، به این معنی که حروف توسط سه حرف تغییر داده می‌شوند. همانطور که مشاهده می‌شود، ابتدا الفبای انگلیسی استاندارد ذکر شده است و در زیر آن، حروف جایگزینی بیان شده است.

Standard Alphabet

ABCDEFGHIJKLMNOPQRSTUVWXYZ

DEFGHIJKLMNOPQRSTUVWXYZABC

Caesar Cipher

Plaintext – PEARSON EDUCATION

Ciphertext – SHDUVRQ HGXFDWLRQ

شکل ۳-۸: رمز سزار

• رمزگذاری Vigenere

در قرن شانزدهم، بلیز د ویگنر از فرانسه یکی از اولین رمزهای جایگزین چند الفبایی را توسعه داد که امروزه با نام رمزگذاری Vigenere شناخته می‌شود. اگرچه بر اساس رمز سزار است، اما رمزگذاری Vigenere به طور چشمگیری پیچیده تر است زیرا از ۲۷ الفبای تغییر یافته استفاده می‌کند، به جدول Vigenere در شکل ۳-۹ مراجعه شود. برای رمزگذاری یک پیام، باید کلید امنیتی را دانسته و از آن در رابطه با پیام ساده برای تعیین متن رمزگذاری شده استفاده کنید.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	S	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

شکل ۳-۹: جدول ویگنر

به عنوان نمونه پیامی که روی آن رمزگذاری Vigenere اعمال شده است، اجازه دهید از کلید امنیتی PEARSON و پیام متن ساده (plaintext) MEETING IN CONFERENCE ROOM استفاده شود. حرف اول در متن ساده M است، و حرف اول در کلید P است. باید حرف M را در اولین سطر ستون‌ها پیدا کنیم. آن ستون را به پایین دنبال می‌کنیم تا اینکه با ردیفی که با حرف P شروع می‌شود تلاقی کند و در نتیجه حرف B حاصل شود. حرف دوم پیام متن E است، و حرف دوم در کلید E است. با استفاده از همین روش، حرف I را بدست می‌آوریم. حروف را به همین ترتیب ادامه می‌دهیم تا زمانی که حرف‌های کلیدی را تمام کنیم، سپس با شروع کلید، که منجر به حرف دوم I در پیام ساده می‌شود که با حرف P کلید کار می‌کند. بنابراین با استفاده از این تکنیک برای کل پیام، پیام متن ساده (plaintext) MEETING IN CONFERENCE ROOM به پیام رمزگذاری شده BIEKABT XR CFFTRGINTW تبدیل می‌شود.

• اصل کرکهوف

در قرن نوزدهم، آگوست کرکهوف شش اصل طراحی را برای استفاده نظامی از رمزها ایجاد کرد. شش اصل به شرح زیر است:

- این سیستم باید عملی باشد، و از لحاظ ریاضی، غیرقابل کشف شدن باشد.
 - این امر نباید مخفی باشد و بتواند بدون نگرانی به دست دشمن بیفتد.
 - کلید آن باید بدون کمک یادداشت‌های کتبی قابل انتقال و قابل حفظ باشد و به خواسته مکاتبه کنندگان قابل تغییر یا اصلاح باشد.
 - باید برای مکاتبات تلگرافی قابل اجرا باشد.
 - باید قابل حمل باشد و استفاده و کارکرد آن نباید به جمع چندین نفر احتیاج داشته باشد.
 - سرانجام، با توجه به شرایطی که دستور کار آن را می‌دهد، سیستم باید به راحتی مورد استفاده قرار گیرد، و نیازی به فشار روانی و آگاهی از یک سری از قوانین زیاد نیست.
- در اصل کرکهوف، به خاطر داشته باشید که کلید مخفی و الگوریتم شناخته شده است.

• جنگ جهانی دوم انیگما

در طول جنگ جهانی دوم، بسیاری از قدرت‌های اصلی نظامی ماشین‌های رمزگذاری را توسعه دادند. مشهورترین ماشین‌های مورد استفاده در طول جنگ دستگاه Enigma بود که توسط آلمان توسعه یافت. دستگاه Enigma از روتور و یک برد پلاگین تشکیل شده بود.

برای تبدیل پیام متن ساده plaintext به متن رمزگذاری شده ciphertext، اپراتور دستگاه ابتدا تنظیمات اولیه خود را پیکربندی می‌کند. سپس اپراتور هر حرف پیام متن ساده plaintext اصلی را به طور هم زمان در دستگاه تایپ می‌کند. دستگاه برای هر حرف وارد شده حرف دیگری را نمایش می‌دهد. بعد از اینکه اپراتور نامه متن رمزگذاری شده ciphertext را نوشت، اپراتور روتورها (یک قطعه متحرک) را به سمت تنظیمات جدید سوق می‌دهد. بنابراین با هر حرف وارد شده، اپراتور مجبور بود تنظیم دستگاه را تغییر دهد. نکته اصلی این فرایند تنظیم اولیه دستگاه و سری‌های افزایشی بود که برای جلو بردن روتور مورد استفاده قرار می‌گرفت، که هر دو مورد برای دریافت صحیح متن رمزگذاری شده به متن ساده، توسط گیرنده می‌بایست شناخته می‌شدند.

به همان اندازه که سیستم پیچیده بود، گروهی از رمزنگاران لهستانی توانستند کد را بشکنند، از این رو اعتبار این کار باعث کوتاه شدن جنگ جهانی دوم حداقل به مدت دو سال گردید.

لوسیفر توسط IBM

پروژه لوسیفر که توسط IBM تهیه شده است، معادلات پیچیده ریاضی را توسعه داده است. این معادلات بعداً توسط آژانس امنیت ملی ایالات متحده در توسعه دیجیتال ایالات متحده مورد استفاده قرار گرفت. استاندارد رمزگذاری (DES)، که امروزه هنوز به نوعی استفاده می شود. لوسیفر از رمزنگاری فستل، رمزگذاری شده تکراری استفاده کرد که متن ساده plaintext را با شکستن بلوک به دو نیمه رمزگذاری می کند. سپس رمزنگار با استفاده از زیرکلید، دور تغییر شکل را در یکی از نیمه ها اعمال می کند. خروجی این تبدیل XORed با نیمه دیگر بلوک است. سرانجام، برای تکمیل دور، دو نیمه تعویض می شود.

ویژگی های سیستم رمزنگاری Cryptosystem Features

سیستم رمزنگاری شامل نرم افزار، پروتکل، الگوریتم و کلید است. قدرت هر سیستم رمزنگاری از الگوریتم و طول و پنهان بودن کلید حاصل می شود. به عنوان مثال، یکی از روش های ساختن کلید سیستم رمزنگاری مقاوم تر در برابر حملات جامع، افزایش طول کلید است. اگر سیستم رمزنگاری از کلید ضعیفی استفاده کند، حملات را برضد الگوریتم تسهیل می کند. در حالی که یک سیستم رمزنگاری از سه اصل اصلی مثلث CIA پشتیبانی می کند، سیستم های رمزنگاری به طور مستقیم احراز هویت، محرمانه بودن، یکپارگی، مجوز و عدم رد اعتبار را ارائه می دهند. اصطلاح در دسترس بودن مثلث CIA توسط سیستم های رمزنگاری پشتیبانی می شود، بدین معنی که اجرای رمزنگاری کمک می کند تا از داده موجود در سازمان اطمینان حاصل شود. با این حال، رمزنگاری مستقیماً در دسترس بودن داده ها را تضمین نمی کند اگرچه می تواند برای محافظت از داده ها استفاده شود.

احراز هویت Authentication

سیستم های رمزنگاری با شناسایی هویت و اعتبار فرستنده، تأیید اعتبار را ارائه می دهند. امضاهای دیجیتال هویت فرستنده را تأیید می کنند. محافظت از کلید اطمینان می دهد که فقط کاربران معتبر می توانند پیام را به درستی رمزنگاری و رمزگشایی کنند.

محرمانه بودن Confidentiality

سیستم‌های رمزنگاری محرمانه با تغییر داده‌های اصلی به گونه‌ای است که تضمین می‌کند که داده‌ها به جز توسط گیرنده معتبر خوانده نمی‌شوند. بدون کلید مناسب، کاربران غیرمجاز قادر به خواندن پیام نیستند.

یکپارچگی Integrity

سیستم‌های رمزنگاری با اجازه دادن به گیرندگان معتبر، تأیید می‌کند که داده‌ها تغییر نکرده اند و یکپارچگی را فراهم می‌کنند. توابع هش از تغییر داده‌ها جلوگیری نمی‌کند اما وسیله‌ای برای تعیین اینکه آیا تغییر داده‌ها رخ داده است فراهم می‌کند.

مجوز Authorization

پس از آنکه کاربر هویت خود را از طریق احراز هویت اثبات کرد، سیستم‌های رمزنگاری با ارائه کلید به یک کاربر معتبر، مجوز ارائه می‌دهد. کلید داده شده به کاربر این امکان را برای کاربر فراهم می‌کند تا به یک منبع دسترسی پیدا کند.

عدم تکذیب Non-repudiation

عدم تکذیب در سیستم‌های رمزنگاری شده اثبات منشأ داده‌ها را فراهم می‌کند و باعث جلوگیری فرستنده از تکذیب ارسال پیام و همینطور پشتیبانی از یکپارچگی داده‌ها می‌شود. رمزنگاری کلید عمومی و امضاهای دیجیتال امکان عدم تکذیب را فراهم می‌کند.

مدیریت کلید Key Management

مدیریت کلید در رمزنگاری برای اطمینان از اینکه رمزنگاری محرمانه، یکپارچگی و محرمانه بودن را تأمین می‌کند، ضروری است. اگر یک کلید به خطر بیفتد، می‌تواند در کل سازمان عواقب جدی داشته باشد.

مدیریت کلید شامل کل فرآیند اطمینان از محافظت از کلیدها در حین ایجاد، توزیع، انتقال و ذخیره سازی می‌باشد. به عنوان بخشی از این فرآیند، کلیدها نیز باید به درستی از بین بروند. وقتی تعداد زیادی از شبکه‌هایی را که کلید بر روی آنها منتقل شده است و انواع مختلف

سیستمهایی که یک کلید در آن ذخیره شده است، در نظر می گیرید، بسیار زیاد این مسئله آشکار می شود.

به عنوان مهمترین جنبه رمزنگاری، مهم است که متخصصان امنیت اصول اصلی مدیریت را درک کنند.

کلیدها باید همیشه به صورت متن رمزگذاری شده ciphertext روی دستگاه غیر رمزنگاری ذخیره شوند. توزیع، ذخیره سازی و نگهداری کلید باید با ادغام فرآیندها در برنامه به صورت خودکار باشد.

از آنجا که کلیدها از بین می روند، باید نسخه های پشتیبان تهیه شده و در یک مکان امن ذخیره شوند. یک فرد مشخص شده باید کپی های پشتیبان را همراه با افراد دیگری که به عنوان پشتیبان اضطراری معرفی شده اند، نظارت کنند. فرایند بازیابی کلید همچنین باید به بیش از یک اپراتور نیاز داشته باشد تا تضمین شود که فقط درخواست های معتبر بازیابی کلید کامل هستند. در بعضی موارد، کلیدها حتی به قسمتهایی شکسته می شوند و به نمایندگان قابل اعتماد سپرده می شوند، که هنگام مجاز بودن انجام این کار، بخش اصلی کلید یک اجازه مرکزی را ارائه می دهد. اگرچه روشهای دیگر توزیع قسمتهای یک کلید مورد استفاده قرار می گیرد، همه راه حل ها شامل استفاده از نمایندگان معتمد است که به آنها قسمتی از کلید و یک اجازه مرکزی که مونتاژ کلید از آن قسمت ها، واگذار شده است. همچنین، پرسنل بازیابی کلید باید در کل سازمان باشند و فقط عضو بخش IT نباشند.

سازمانها همچنین باید تعداد کلیدهای مورد استفاده را محدود کنند. هرچه تعداد کلیدهای بیشتری در اختیار داشته باشید، باید بیشتر نگران کلیدها باشید و از محافظت آنها مطمئن شوید. اگرچه یک دلیل معتبر برای صدور کلید هرگز نباید نادیده گرفته شود، محدود کردن تعداد کلیدهای صادر شده و بکاربرده شده باعث کاهش خسارت احتمالی می شود.

هنگام طراحی فرایند مدیریت کلید، باید نحوه انجام موارد زیر در نظر گرفته شود:

- ✓ کلیدها با خیال راحت ذخیره و انتقال داده شود.
- ✓ از کلیدهای تصادفی استفاده شود.
- ✓ برای اطمینان از محافظت، کلیدهایی با طول کافی صادر شود.
- ✓ اگر دیگر نیازی به استفاده از کلیدها نیست، به درستی آنها از بین بروند.
- ✓ برای اطمینان از بازیابی آنها، از کلیدها نسخه پشتیبان تهیه شود.

انواع رمزنگاری

الگوریتم‌های مورد استفاده در سیستم‌های رایانه‌ای هنگام تبدیل متن ساده plaintext به متن رمزگذاری ciphertext، فرمول‌های پیچیده ریاضی را پیاده‌سازی می‌کنند. دو مؤلفه اصلی برای هر سیستم رمزگذاری کلید و الگوریتم هستند. در برخی از سیستم‌های رمزگذاری، دو طرف ارتباط دهنده از همان کلید استفاده می‌کنند. در سایر سیستم‌های رمزگذاری، دو طرف ارتباط دهنده از کلیدهای مختلفی در این فرآیند استفاده می‌کنند، اما کلیدها به هم مرتبط هستند. در این بخش موارد زیر مورد بحث قرار می‌گیرد:

- ✓ اجرای رمزهای کلید و رمزهای پنهان Running key and concealment ciphers
- ✓ رمزهای جایگزینی (جانشینی) Substitution ciphers
- ✓ رمزهای انتقال Transposition ciphers
- ✓ الگوریتم‌های متقارن Symmetric algorithms
- ✓ الگوریتم‌های نامتقارن Asymmetric algorithms
- ✓ رمزگذارهای هیبریدی Hybrid ciphers

• رمز کلید در حال اجرا و رمزهای پنهان Running key and concealment ciphers

روشهای کلاسیک تولید رمز محسوب می‌شوند. رمز کلید در حال اجرا از یک مؤلفه فیزیکی، معمولاً یک کتاب (book)، برای کاراکترهای چندرسانه‌ای استفاده می‌کند. یک بلوک نشانگر باید در جایی در متن قرار بگیرد تا گیرنده بداند که مبدأ از کجا شروع شده است. بنابراین، دو طرف باید با هم توافق کنند که از کدام کتاب (book) استفاده کنند و بلوک نشانگر در پیام رمز درج شود. به رمزهای در حال اجرا نیز رمزهای کلید و رمز کلیدهای در حال اجرا گفته می‌شود. رمز پنهان Concealment cipher، که همچنین به آن رمز تهی null cipher نیز گفته می‌شود، هنگامی رخ می‌دهد که متن ساده plaintext در جای نوشتاری دیگر مشاهده شود. دو طرف باید در مورد مقدار کلید توافق کنند، که مشخص می‌کند حرف‌ها بخشی از پیام واقعی هستند. به عنوان مثال، هر حرف سوم یا اولین حرف هر کلمه بخشی از پیام واقعی است. رمز پنهان متعلق به قلمرو استگنوگرافی (پنهانکاری) است.

• رمزهای جایگزینی (جانشینی) Substitution Ciphers

رمزهای جایگزینی از کلید برای جایگزینی کاراکترها یا بلوک های کاراکتر با کاراکترهای مختلف یا بلوک های کاراکتر استفاده می کند. رمزهای سزار و رمزگذاری وینگر دو نوع از اولین رمزهای جایگزینی هستند.

نمونه دیگر رمزهای جایگزینی رمزگذاری جایگزینی مازول ۲۶ است. با استفاده از این رمز، ۲۶ حرف الفبای شماره گذاری شده اند و از صفر شروع شود. فرستنده پیام اصلی را می گیرد و تعداد هر حرف را در پیام اصلی تعیین می کند. سپس مقادیر حروف کلید به مقادیر حروف اصلی اضافه می شوند. سپس نتیجه مقدار به متن برگردانده می شود.

شکل ۳-۱۰ نمونه ای از رمزگذاری رمز مازول ۲۶ را نشان می دهد. با این مثال، پیام اصلی PEARSON است، و کلید اصلی KEY است. پیام رمزنگاری شده ZIYBSMX است.

Original Message	Original Value	Key	Key Value	Result	Mod 26	Cipher Message
P	15	K	10	25	25	Z
E	4	E	4	8	8	I
A	0	Y	24	24	24	Y
R	17	K	10	27	1	B
S	18	E	4	18	18	S
O	14	Y	24	38	12	M
N	13	K	10	23	23	X

Modulo 26 Letter Chart

a 0	h 7	o 14	v 21
b 1	i 8	p 15	w 22
c 2	j 9	q 16	x 23
d 3	k 10	r 17	y 24
e 4	l 11	s 18	z 25
f 5	m 12	t 19	
g 6	n 13	u 20	

شکل ۳-۱۰: مازول ۲۶ نمونه رمز جایگزینی

• رمزهای انتقال Transposition Ciphers

رمزهای انتقالی حروف پیام اصلی را به ترتیب متفاوت می کند. کلید موقعیت هایی را که حروف به آنها منتقل می شوند تعیین می کند.

شکل ۳-۱۱ نمونه ای از رمز انتقال ساده را نشان می دهد. با این مثال، پیام اصلی PEARSON EDUCATION است و کلید آن 2314 4231 است. پیام رمزگذاری شده REAP ONSE AUCD IOTN است. بنابراین شما چهار حرف اول پیام ساده PEAR را می گیرید و از چهار شماره اول (4231) به عنوان کلید انتقال استفاده می کنید. در متن جدید، نامه ها REAP می شوند. سپس چهار حرف بعدی از متن ساده SONE را می گیرید و از چهار شماره بعدی (2314) به عنوان کلید برای انتقال استفاده می کنید. در متن جدید، حروف ONSE خواهند بود. سپس چهار حرف بعدی

از پیام اصلی را می‌گیرید و چهار شماره اول کلید را اعمال می‌کنید زیرا شماره دیگری در کلید ندارید. این الگو را تا زمان کامل شدن ادامه دهید.

Original message: PEARSON EDUCATION
 Broken into groups: PEAR SONE DUCA TION
 Key: 4231 2314 4231 2314
 Ciphertext message: REAP ONSE AUCD IOTN

شکل ۳-۱۱: مثال انتقالی

• الگوریتم‌های متقارن Symmetric Algorithms

الگوریتم‌های متقارن از یک کلید خصوصی یا مخفی استفاده می‌کنند که باید بین دو طرف پنهان بماند. هر دو طرف نیاز به یک کلید خصوصی جداگانه دارند. بنابراین، یک کاربر منفرد نیاز به یک کلید مخفی برای هر کاربر دارد که با او ارتباط برقرار کند.

مثالی را در نظر بگیرید که ۱۰ کاربر منحصر به فرد در آن وجود دارد. هر کاربر برای برقراری ارتباط با سایر کاربران به یک کلید خصوصی جداگانه نیاز دارد. برای محاسبه تعداد کلیدهای مورد نیاز در این مثال، از فرمول زیر استفاده می‌کنید: $\# \text{ of users} \times (\# \text{ of users} - 1) / 2$

با استفاده از مثال می‌توانید $10 \times (10 - 1) / 2$ یا ۴۵ کلید مورد نیاز را محاسبه کنید.

با الگوریتم‌های متقارن، کلید رمزگذاری باید ایمن بماند. برای بدست آوردن کلید مخفی، کاربران باید یک روش خارج از باند را برای برقراری ارتباط کلید مخفی، از جمله پیک یا تماس مستقیم بین کاربران پیدا کنند.

نوع خاصی از کلید متقارن به نام کلید جلسه، پیام‌ها را بین دو کاربر در طی یک جلسه ارتباط رمزگذاری می‌کند.

الگوریتم‌های متقارن را می‌توان به صورت رمزنگاری تک کلید، کلید مخفی، کلید خصوصی یا کلید مشترک به کار برد.

سیستم‌های متقارن محرمانه بودن را تأمین می‌کنند اما احراز هویت یا عدم تکذیب آن را انجام نمی‌دهند. اگر هر دو کاربر از یک کلید مشابه استفاده کنند، تعیین منبع آن پیام غیرممکن است.

الگوریتم‌های متقارن شامل DES، AES، IDEA، Skipjack، Blowfish، wofish، RC4/RC5/6RC، CAST

است. تمام این الگوریتم‌ها بعداً در این فصل مورد بحث قرار می‌گیرند.

در جدول ۳-۴ نقاط قوت و ضعف الگوریتم‌های متقارن آورده شده است.

Strengths	Weaknesses
1,000 to 10,000 times faster than asymmetric algorithms	Number of unique keys needed can cause key management issues
Hard to break	Secure key distribution critical
Cheaper to implement than asymmetric	Key compromise occurs if one party is compromised, thereby allowing impersonation

جدول ۳-۴: نقاط قوت و ضعف الگوریتم متقارن

دو نوع گسترده الگوریتم متقارن رمزهای مبتنی بر جریان و رمزهای بلوک هستند. بردارهای اولیه IVs بخش مهمی از رمزهای بلوک هستند.

• رمزهای مبتنی بر جریان Stream-based Ciphers

رمزهای مبتنی بر جریان، رمزگذاری را بطور بیتی انجام می دهند و از ژنراتورهای اصلی استفاده می کنند. ژنراتورهای جریان اصلی جریان کمی را ایجاد می کنند که XORed با بیت های متن ساده است. نتیجه این عمل XOR متن رمزگذاری شده است.

رمزهای مبتنی بر جریان همگام تنها به کلید بستگی دارد، و رمزنگاری جریان ناهمگام به کلید و متن ساده بستگی دارد. کلید اطمینان می دهد که جریان بیتی که XORed به متن ساده می باشد تصادفی است.

نمونه ای از رمزهای مبتنی بر جریان RC4 است که بعداً در این فصل مورد بحث قرار می گیرد. مزایای رمزهای مبتنی بر جریان شامل موارد زیر است:

- ✓ معمولاً انتشار خطا کمتر است زیرا رمزگذاری در هر بیت رخ می دهد.
- ✓ معمولاً بیشتر در پیاده سازی سخت افزار استفاده می شود.
- ✓ از همان کلید برای رمزگذاری و رمزگشایی استفاده می شود.
- ✓ به طور معمول برای پیاده سازی از رمزهای بلوک ارزانتر است.
- ✓ فقط در سردرگمی Confusion استفاده شود.

رمزهای بلوک Block Ciphers

رمزهای بلوک رمزگذاری را با شکستن پیام به واحدهایی با طول ثابت انجام می دهند. یک پیام از ۱۰۲۴ بیت می تواند به ۱۶ بلوک ۶۴ بیتی تقسیم شود. هر یک از این ۱۶ بلوک توسط

فرمول‌های الگوریتم پردازش می‌شود و در نتیجه یک بلوک تک رمزگذاری شده Ciphertext انجام می‌شود.

نمونه هایی از رمزهای بلوک شامل IDEA ، Blowfish ، 5RC ، 6RC است که بعداً در این فصل مورد بحث قرار می‌گیرد.

مزایای رمزهای بلوک شامل موارد زیر است:

- اجرا آسانتر از پیاده سازی رمز مبتنی بر جریان است.
- عموماً نسبت به مسائل امنیتی حساسیت کمتری دارند.
- معمولاً بیشتر در اجرای نرم افزار استفاده می‌شود.

رمزگذارهای بلوک هم اغتشاش و هم انتشار ایجاد می‌کنند. رمزگذارهای بلوک اغلب از حالت‌های مختلف استفاده می‌کنند ECB ، CBC ، CFB ، CTR این حالت‌ها بعداً در این فصل با جزئیات مورد بحث قرار خواهد گرفت.

بردارهای اولیه (IV) Initialization Vectors

حالت‌های ذکر شده قبلی از IV ها استفاده می‌کنند تا مطمئن شوند که الگوهای در حین رمزگذاری تولید نمی‌شوند. این IV ها با استفاده از مقادیر تصادفی با الگوریتم ها، این سرویس را ارائه می‌دهند. بدون استفاده از IV ، یک عبارت تکراری در یک پیام ساده می‌تواند به متن رمزگذاری شده ciphertext منجر شود. مهاجمان احتمالاً می‌توانند از این الگوها برای شکستن رمزگذاری استفاده کنند.

الگوریتم‌های نامتقارن Asymmetric Algorithms

الگوریتم‌های نامتقارن هم از یک کلید عمومی و هم یک کلید خصوصی یا مخفی استفاده می‌کنند. کلید عمومی توسط همه طرفین شناخته شده است و کلید خصوصی فقط توسط صاحب آن شناخته شده می‌باشد. یکی از این کلیدها پیام را رمزگذاری می‌کند و دیگری پیام را رمزگشایی می‌کند.

در رمزنگاری نامتقارن، تعیین کلید خصوصی کاربر حتی اگر کلید عمومی شناخته شده باشد، تقریباً غیرممکن است، اگرچه هر دو کلید از لحاظ ریاضی مرتبط هستند. ولی اگر کلید خصوصی کاربر کشف شود، سیستم به خطر می‌افتد.

از الگوریتم‌های نامتقارن می‌توان به رمزنگاری دو کلید یا کلید عمومی اشاره کرد.

سیستم های نامتقارن محرمانه، یکپارچگی، تأیید اعتبار(احراز هویت) و عدم تکذیب را فراهم می کنند. از آنجا که هر دو کاربر دارای یک کلید منحصر به فرد هستند که بخشی از فرآیند است، تعیین مبدا پیام امکان پذیر است.

اگر محرمانه بودن دغدغه اصلی یک سازمان است، باید یک پیام با کلید عمومی گیرنده رمزگذاری شود که به آن به عنوان فرمت پیام امن گفته می شود. اگر احراز هویت اصلی ترین دغدغه برای یک سازمان باشد، باید یک پیام با کلید خصوصی فرستنده رمزگذاری شود که به آن فرمت پیام باز گفته می شود. هنگام استفاده از فرمت پیام باز، این پیام توسط هر کسی که کلید عمومی را دارد می تواند رمزگشایی شود.

الگوریتم های نامتقارن شامل Diffie-Hellman، RSA، El Gamal، ECC، Knapsack، DSA، Zero اثبات دانش صفر Zero Knowledge Proof است. در جدول ۳-۵ نقاط قوت و ضعف الگوریتم های نامتقارن آورده شده است.

Strengths	Weaknesses
Key distribution is easier and more manageable than with symmetric algorithms.	More expensive to implement than symmetric algorithms.
Key management is easier because the same public key is used by all parties.	1,000 to 10,000 times slower than symmetric algorithms.

جدول ۳-۵: نقاط قوت و ضعف الگوریتم نامتقارن

• رمزهای هیبریدی Hybrid Ciphers

از آنجا که هر دو الگوریتم متقارن و نامتقارن دارای ضعف هایی هستند، راه حلهایی ایجاد شده است که از هر دو نوع الگوریتم در رمز هیبریدی استفاده می کند. رمزگذار با استفاده از هر دو نوع الگوریتم، محرمانه بودن، تأیید اعتبار(احراز هویت) و عدم تکذیب را فراهم می کند. مراحل رمز هیبریدی به شرح زیر است:

- ۱- الگوریتم متقارن کلیدهای مورد استفاده برای رمزگذاری را فراهم می کند.
- ۲- سپس کلیدهای متقارن به الگوریتم نامتقارن منتقل می شوند، که کلیدهای متقارن را رمزگذاری می کند و به طور خودکار آنها را توزیع می کند.
- ۳- سپس پیام با کلید متقارن رمزگذاری می شود.
- ۴- هم پیام و هم کلید به گیرنده ارسال می شود.

۵- گیرنده کلید متقارن را رمزگشایی می‌کند و از کلید متقارن برای رمزگشایی پیام استفاده می‌کند.

اگر طرفین کلید پنهان مشترک نداشته باشند، باید مقادیر زیادی از داده‌های حساس منتقل شوند، سازمان باید از رمز هیبریدی استفاده کند.

رمزهای جایگزینی Substitution Ciphers

همانطور که قبلاً نیز اشاره شد، رمز جایگزینی از کلید برای جایگزینی کاراکترها یا بلوک‌های کاراکتر با کاراکترهای مختلف یا بلوک کاراکتر استفاده می‌کند. رمزهای تک الفبایی و چند الفبایی مثل رمزهای سزار و رمز ویگنر و رمز کلیدهای در حال اجرا می‌باشند. رمزهای جایگزینی که در این بخش توضیح داده می‌شود شامل موارد زیر است:

- پدهای یک زمانه
- استگانوگرافی

پدهای یک زمانه One-Time Pads

پد یک زمانه، که توسط Gilbert Vernam اختراع شده است، امن ترین طرح رمزگذاری است که می‌تواند مورد استفاده قرار گیرد. در صورت استفاده صحیح، یک مهاجم نمی‌تواند یک پد یک زمانه را بشکند. پد یک زمانه مانند یک رمز در حال اجرا کار می‌کند به این دلیل که مقدار کلید به مقدار حروف اضافه می‌شود. اما، پد یک زمانه از یک کلید استفاده می‌کند که طول آن برابر با طول پیام ساده است، در حالی که رمز در حال اجرا از یک کلید کوچکتر استفاده می‌کند که بارها و بارها روی پیام متنی اعمال می‌شود.

شکل ۳-۱۲ نمونه‌ای از رمز پد یک زمانه را نشان می‌دهد. با این مثال پیام اصلی PEARSON است و کلید آن JOHNSON است. پیام رمزگذاری شده YSHEKCA است.

Original Message	Original Value	Key	Key Value	Result	Mod 26	Cipher Message
P	15	J	9	24	24	Y
E	4	O	14	18	18	S
A	0	H	7	7	7	H
R	17	N	13	30	4	E
S	18	S	18	36	10	K
O	14	O	14	28	2	G
N	13	N	13	26	0	A

Modulo 26 Letter Chart

a 0	h 7	o 14	v 21
b 1	i 8	p 15	w 22
c 2	j 9	q 16	x 23
d 3	k 10	r 17	y 24
e 4	l 11	s 18	z 25
f 5	m 12	t 19	
g 6	n 13	u 20	

شکل ۳-۱۲: به عنوان مثال پد یک بار

برای اطمینان از ایمن بودن پد یک زمانه، شرایط زیر باید وجود داشته باشد:

- ✓ فقط باید یک بار استفاده شود.
- ✓ باید به اندازه (یا بلند تر) از پیام باشد.
- ✓ باید از مقادیر تصادفی تشکیل شده باشد.
- ✓ باید با اطمینان توزیع شود.
- ✓ باید در مبدا و مقصد آن محافظت شود.

اگرچه نمونه اولیه از یک پد یک زمانه در یک طرح مازول ۲۶ استفاده می شود، اما می توان از پدهای یک زمانه نیز در سطح بیت استفاده کرد. هنگامی که از سطح بیت استفاده می شود، پیام به باینری تبدیل می شود و یک عملیات XOR همزمان دو بیت رخ می دهد. بیت های پیام اصلی برای بدست آوردن پیام رمزگذاری شده با مقادیر اصلی ترکیب می شوند. وقتی مقادیر ترکیب می شود، اگر هر دو مقدار یکسان باشند نتیجه ۰ است و اگر هر دو مقدار متفاوت باشند، نتیجه ۱ است. نمونه ای از عمل XOR به شرح زیر است:

Original message	0 1 1 0 1 1 0 0
Key	1 1 0 1 1 1 0 0
Cipher message	1 0 1 1 0 0 0 0

پنهان سازی Steganography

زمانی رخ می دهد که یک پیام درون یک شیء دیگر، مانند تصویر یا سند پنهان می شود. در استگانوگرافی بسیار مهم است که فقط کسانی که منتظر پیام هستند بدانند که پیام وجود دارد. یک رمز پنهان Concealment cipher، که قبلاً در مورد آن بحث شد، یکی از روش های استگانوگرافی است. روش دیگر استگانوگرافی، سایه گذاری دیجیتالی (Watermarking) است. سایه گذاری دیجیتالی یک آرم یا علامت تجاری است که در اسناد، تصاویر یا اشیاء دیگر تعبیه می شود. سایه گذاری دیجیتالی باعث می شود که استفاده مردم از مواد به روش غیر مجاز جلوگیری شود.

در این بخش برخی از رایج ترین الگوریتم های متقارن را مورد بحث قرار می دهیم. برخی از این موارد ممکن است دیگر مورد استفاده قرار نگیرند زیرا گزینه های امن تری بوجود آمده است. متخصصان امنیت باید با الگوریتم های متقارن زیر آشنا باشند:

- DES/3DES
- AES
- IDEA
- Skipjack
- Blowfish
- Twofish
- RC۴/RC۵/RC ۶
- CAST

✓ استاندارد رمزگذاری دیجیتالی (DES) و Triple DES (3DES)

استاندارد رمزگذاری دیجیتالی (DES) یک سیستم رمزگذاری متقارن است که توسط آژانس امنیت ملی (NSA) ایجاد شده ولی بر اساس الگوریتم ۱۲۸ بیتی لوسیفیر توسط IBM ساخته شده است. در ابتدا، این الگوریتم به عنوان الگوریتم رمزگذاری داده (DEA) نامگذاری شد و از مخفف DES برای ارجاع به استاندارد استفاده شد. اما در دنیای امروز، DES اصطلاح رایج تر برای هر دو می‌باشد.

DES از یک کلید ۶۴ بیتی استفاده می‌کند که ۸ بیت از آن بیت توازن می‌باشد. بنابراین، طول کلیدی موثر برای DES، ۵۶ بیت است. DES پیام را به بلوک‌های ۶۴ بیتی تقسیم می‌کند. شانزده دور جابجایی و جایگزینی در هر بلوک انجام می‌شود، و در نتیجه یک بلوک رمزگذاری شده ۶۴ بیتی ایجاد می‌شود.

DES بیشتر توسط DES۳ و AES جایگزین شده است، که هر دو مورد بعداً در این فصل مورد بحث قرار می‌گیرند.

DES-X نوعی از DES است که علاوه بر کلید DES، ۵۶ بیتی، از چندین کلید ۶۴ بیتی استفاده می‌کند. اولین کلید ۶۴ بیتی XORed به متن ساده plaintext است که سپس با DES رمزگذاری می‌شود. کلید ۶۴ بیتی دوم XORed به نتیجه رمزگذاری است.

Double-DES، نسخه DES که از طول کلید ۱۱۲ بیتی استفاده می‌کند که دیگر مورد استفاده قرار نمی‌گیرد. پس از انتشار، یک حمله امنیتی رخ داد که باعث کاهش امنیت Double-DES به همان سطح DES شد.

حالت‌های DES

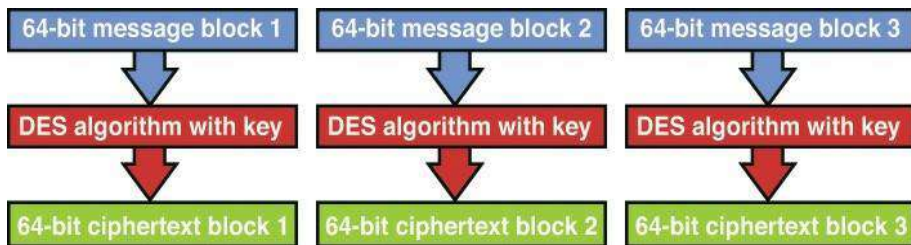
DES در پنج حالت زیر ارائه می‌شود:

- کتاب کد الکترونیکی (Electronic Code Book (ECB)
- زنجیره بلوک رمزگذاری (Cipher Block Chaining (CBC)
- بازخورد رمزگذاری (Cipher Feedback (CFB)
- بازخورد خروجی (Output Feedback (OFB)
- حالت پیشخوان (Counter Mode (CTR)

در ECB، بلوک های ۶۴ بیتی داده ها توسط الگوریتم با استفاده از کلید پردازش می شوند. متن رمزگذاری شده (Ciphertext) را می توان برای اطمینان از این که نتیجه یک بلوک ۶۴ بیتی شود، قرار داد. اگر یک خطای رمزگذاری رخ دهد، فقط یک بخش از پیام تحت تأثیر قرار می گیرد. عملیات ECB به صورت موازی اجرا می شود، و همچنین یک روش سریع است.

اگرچه ECB ساده ترین و سریعترین حالت برای استفاده است، اما دارای مشکلات امنیتی است زیرا هر بلوک ۶۴ بیتی با همان کلید رمزگذاری می شود. اگر یک مهاجم کلید را کشف کند، می تواند تمام بلوک های داده را بخواند. اگر یک مهاجم هر دو نسخه از بلوک ۶۴ بیتی (متن ساده plaintext و متن رمزگذاری شده ciphertext) را کشف کند، می تواند کلید را تعیین کند. به همین دلایل، نباید هنگام رمزگذاری حجم زیادی از داده ها را در حالت استفاده قرار داد زیرا الگوها آشکار می شوند.

اگر یک سازمان نیاز به رمزگذاری برای پایگاه داده های خود داشته باشد، ECB یک انتخاب خوب است زیرا ECB با رمزگذاری پیام های کوتاه به خوبی کار می کند. شکل ۳-۱۳ فرایند رمزگذاری ECB را نشان می دهد.

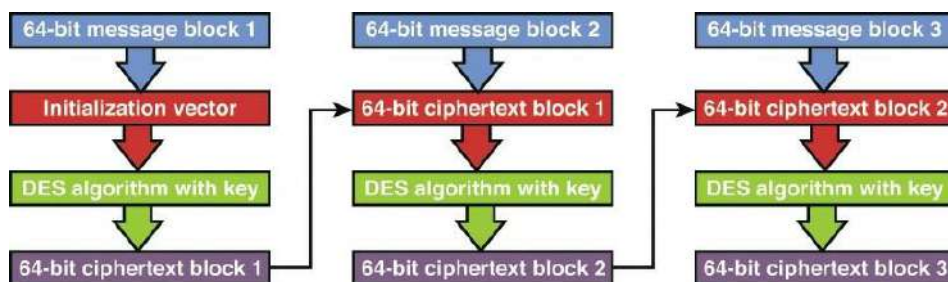


شکل ۳-۱۳: DES حالت ECB

در CBC، هر بلوک ۶۴ بیتی با هم زنجیر شده است زیرا هر بلوک متن رمزگذاری شده ۶۴ بیتی حاصل به بلوک بعدی اعمال می شود. بنابراین پیام بلوک متن ساده ۱ توسط الگوریتم با استفاده از بردارهای اولیه IV پردازش می شود. پیام بلوک متن رمزگذاری شده حاصل XOR با پیام بلوک

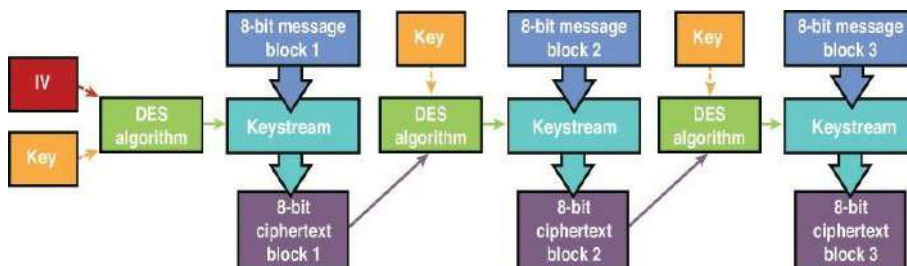
متن ساده ۲ است، که منجر به پیام متن رمزگذاری ۲ می‌شود. این روند تا زمان کامل شدن پیام ادامه می‌یابد.

برخلاف ECB، CBC، فایل‌های بزرگ را بدون داشتن هیچ الگویی در متن رمز ciphertext رمزگذاری می‌شوند. اگر از یک IV منحصر به فرد با هر رمزگذاری پیام استفاده شود، متن رمزگذاری نتیجه هر بار متفاوتی خواهد داشت حتی در مواردی که از همان پیام متن ساده (plaintext) استفاده می‌شود. شکل ۳-۱۴ روند رمزگذاری CBC را نشان می‌دهد.



شکل ۳-۱۴: CBC حالت DEC

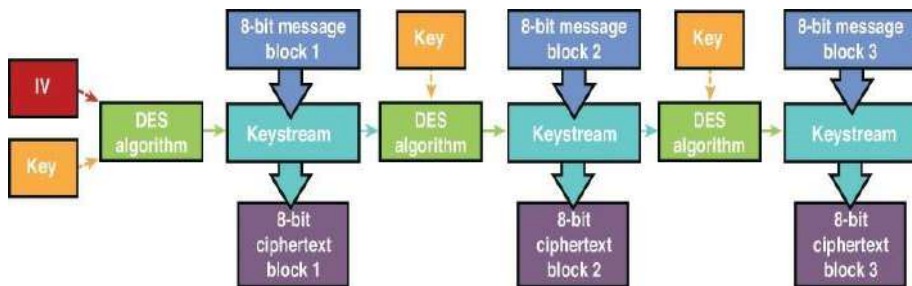
در حالی که CBC و ECB به بلوک‌های ۶۴ بیتی نیاز دارند، CFB با بلوک‌های ۸ بیتی (یا کوچکتر) کار می‌کند و از ترکیبی از رمز مبتنی بر جریان و رمزگذاری بلوک استفاده می‌کند. مانند CBC، اولین بلوک ۸ بیتی پیام متنی ساده توسط الگوریتمی با استفاده از کلید اصلی XORed، که نتیجه یک IV و کلید است. پیام متن رمزگذاری شده منتخب به بلوک پیام متن ساده بعدی اعمال می‌شود. شکل ۳-۱۵ روند رمزگذاری CFB را نشان می‌دهد.



شکل ۳-۱۵: DES حالت CFB

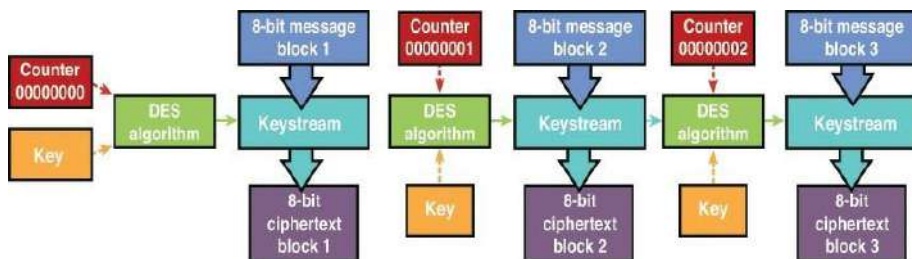
اندازه بلوک متن رمزگذاری شده باید برابر اندازه بلوک متن ساده باشد. روشی که CFB استفاده می‌کند می‌تواند در صورت بروز هرگونه نتیجه متن رمزگذاری شده دارای مشکلاتی باشد زیرا

این خطاها روی هرگونه رمزگذاری بلوک آینده تأثیر می‌گذارد. به همین دلیل، نباید از CFB برای رمزگذاری داده‌هایی که تحت تأثیر این مشکل قرار دارند، بخصوص سیگنال‌های ویدیویی یا صوتی استفاده شود. این مشکل منجر به نیاز به حالت DES OFB شد. مشابه CFB، OFB با بلوک‌های ۸ بیتی (یا کوچکتر) کار می‌کند و از ترکیبی از رمزگذاری مبتنی بر جریان و رمزگذاری بلوک استفاده می‌کند. با این حال، OFB از کلید اصلی قبلی با کلید برای ایجاد جریان اصلی بعدی استفاده می‌کند. شکل ۳-۱۶ روند رمزگذاری OFB را نشان می‌دهد.



شکل ۳-۱۶: DES حالت OFB

با OFB، اندازه مقدار کلید جریان باید به اندازه بلوک متن ساده باشد. از آنجا که روش OFB پیاده‌سازی شده است، OFB نسبت به خطایی که CFB دارد کمتر مستعد است. حالت CTR شبیه حالت OFB است. تفاوت اصلی این است که در حالت CTR از پیشخوان (شمارنده) IV در حال افزایش استفاده می‌کند تا اطمینان حاصل شود که هر بلوک با یک کلید جریان منحصر به فرد رمزگذاری شده است. همچنین، متن رمز ciphertext به فرآیند رمزگذاری متصل نمی‌شود. از آنجا که این زنجیر سازی رخ نمی‌دهد، عملکرد CTR بسیار بهتر از حالت‌های دیگر است. شکل ۳-۱۷ فرایند رمزگذاری CTR را نشان می‌دهد.



شکل ۳-۱۷: DES حالت CTR

سه گانه DES, DES 3 و حالتها

به دلیل نیاز به تعویض سریع DES، DES سه گانه، 3DES و حالتها، نسخه DES که امنیت را با استفاده از سه کلید ۵۶ بیتی افزایش می‌دهد، ساخته شد. اگرچه 3DES در برابر حملات مقاوم است، اما تا سه برابر کندتر از DES است. 3DES به عنوان یک جایگزین موقت DES کار می‌کرد. با این حال، NIST در واقع استاندارد رمزگذاری پیشرفته (AES) را به عنوان جایگزینی برای DES معرفی کرد، با اینکه 3DES هنوز در حال استفاده می‌باشد.

3DES در چهار حالت زیر ارائه می‌شود:

- 3DES-EEE3: هر بلوک از داده‌ها سه بار رمزگذاری می‌شوند، هر بار با یک کلید متفاوت.
- 3DES-EDE3: هر بلوک از داده‌ها با کلید اول رمزگذاری می‌شوند، با کلید دوم رمزگشایی می‌شوند و با کلید سوم رمزگذاری می‌شوند.
- 3DES-EEE2: هر بلوک از داده‌ها با کلید اول رمزگذاری می‌شود، با کلید دوم رمزگذاری می‌شود و در آخر دوباره با کلید اول رمزگذاری می‌شود.
- 3DES-EDE2: هر بلوک از داده‌ها با کلید اول رمزگذاری می‌شوند، با کلید دوم رمزگشایی می‌شود و در آخر دوباره با کلید اول رمزگذاری می‌شود.

✓ استاندارد رمزگذاری پیشرفته (Advanced Encryption Standard (AES)

AES الگوریتم جایگزینی برای DES است. هنگامی که NIST تصمیم گرفت استاندارد جدیدی را بخاطر اینکه DES شکست خورده بود، NIST پنج گزینه صنعتی را ارائه کرد:

- IBM's MARS
- RSA Laboratories' RC6
- Anderson, Biham, and Knudsen's Serpent
- Counterpane Systems' Twofish
- Daemen and Rijmen's Rijndael

از بین این گزینه‌ها، NIST، Rijndael را انتخاب کرد. بنابراین اگرچه AES استاندارد محسوب می‌شود، الگوریتمی که در استاندارد AES استفاده می‌شود، الگوریتم Rijndael است. اصطلاحات AES و Rijndael اغلب بصورت متقابل استفاده می‌شوند.

سه اندازه بلوک که در الگوریتم Rijndael استفاده می‌شود که شامل ۱۲۸، ۱۹۲، ۲۵۶ بیتی است. یک کلید ۱۲۸ بیتی با اندازه بلوک ۱۲۸ بیتی، ۱۰ دور تحول (تغییرات) را پشت سر می‌گذارد.

یک کلید ۱۹۲ بیتی با اندازه بلوک ۱۹۲ بیتی، ۱۲ دور تحول را پشت سر می گذارد. سرانجام، یک کلید ۲۵۶ بیتی با اندازه بلوک ۲۵۶ بیتی ۱۴ دور تحول را پشت سر می گذارد. Rijndael از تحولات متشکل از سه لایه استفاده می کند: لایه غیر خطی، لایه اضافه کلید و لایه حداکثر خطی. طراحی Rijndael بسیار ساده است و کد آن بهم فشرده و متراکم است که امکان استفاده از آن را در انواع مختلف سیستم عامل فراهم می کند. این الگوریتم مورد نیاز برای داده های حساس غیر طبقه بندی شده دولت ایالات متحده می باشد.

IDEA ✓

الگوریتم رمزگذاری داده های بین المللی (International Data Encryption Algorithm (IDEA یک رمزگذاری بلوک است که از بلوک های ۶۴ بیتی استفاده می کند. هر بلوک ۶۴ بیتی به ۱۶ بلوک کوچکتر تقسیم می شود. IDEA از یک کلید ۱۲۸ بیتی استفاده می کند و هشت دور تحول را روی هر یک از ۱۶ بلوک کوچکتر انجام می دهد.

شکستن IDEA سریعتر و سخت تر از DES است. با این حال، IDEA به اندازه DES یا AES کاربرد زیادی ندارد، زیرا ثبت اختراع (PATENT) بود، و مجوزهای لیسانس مربوطه را باید به مالک IDEA که یک شرکت سوئیسی به نام Ascom بود پرداخت می شد، با این حال، حق ثبت اختراع در سال ۲۰۱۲ منقضی شد. IDEA در PGP استفاده می شود.

Skipjack ✓

یک الگوریتم متقارن با رمزگذاری بلوک (Block Cipher) است که توسط NSA ایالات متحده ساخته شده است. از یک کلید ۸۰ بیتی برای رمزگذاری بلوک های ۶۴ بیتی استفاده می کند. این الگوریتمی است که در تراشه Clipper استفاده می شود و جزئیات الگوریتم طبقه بندی می شوند.

Blowfish ✓

یک رمزگذاری بلوک است که از بلوک های داده ۶۴ بیتی با استفاده از کلیدهای رمزگذاری ۳۲- تا ۴۴۸ بیتی استفاده می کند. Blowfish، ۱۶ دور تحول (تغییر شکل) را انجام می دهد. در ابتدا با هدف سرویس به عنوان جایگزینی برای DES توسعه یافته است، Blowfish یکی از محدود الگوریتم هایی است که ثبت اختراع نشده است.

Twofish ✓

نسخه‌ای از Blowfish است که از بلوک‌های داده ۱۲۸ بیتی با استفاده از کلیدهای ۱۲۸ و ۱۹۲ و ۲۵۶ بیتی استفاده می‌کند. از ۱۶ دور تحول استفاده می‌کند. Twofish مانند Blowfish نیز ثبت اختراع نشده است.

RC4/RC5/RC6 ✓

در مجموع شش الگوریتم RC توسط ران ریوست ساخته شده است. RC1 هرگز منتشر نشد، RC2 یک رمزگذاری بلوک ۶۴ بیتی بود و RC3 قبل از انتشار شکست خورد. بنابراین اصلی ترین پیاده سازی‌های RC که یک متخصص امنیت باید درک کند RC4، RC5، RC6 است. RC4 که به آن ARC4 نیز می‌گویند، یکی از رایج ترین رمزگذارهای جریان است، و در SSL و WEP استفاده می‌شود. RC4 از اندازه کلید متغیر ۴۰ تا ۲۰۴۸ بیت و تا ۲۵۶ دور تحول استفاده می‌کند.

RC5 یک رمزگذاری بلوک است که از اندازه کلید تا ۲۰۴۸ بیت و تا ۲۵۵ دور تحول استفاده می‌کند. اندازه بلوک پشتیبانی شده ۳۲ یا ۶۴ یا ۱۲۸ بیت است. از آنجا که از همه متغیرهای ممکن در RC5، صنعت اغلب از یک $w / r / b$ استفاده می‌کند، در جایی که w اندازه بلوک باشد، r تعداد دور و b تعداد بایت‌های ۸ بیتی در کلید است. به عنوان مثال، RC5-64 / 16/16 یک کلمه ۶۴ بیتی (یا بلوک‌های داده ۱۲۸ بیتی)، ۱۶ دور تحول و یک کلید ۱۶ بایت (۱۲۸ بیتی) را مشخص می‌کند. RC6 رمزگذاری بلوک مبتنی بر RC5 است و از همان اندازه کلید، دور و اندازه بلوک استفاده می‌کند. RC6 در ابتدا به عنوان یک راه حل AES توسعه داده شد، اما در رقابت با Rijndael شکست خورد. RC6 سریعتر از RC5 است.

CAST ✓

CAST که توسط Carlisle Adams و Stafford Tavares اختراع شده است، دو نسخه دارد: CAST-128 و CAST-256.

CAST-128 یک رمزگذاری بلوک است که از یک کلید ۴۰ تا ۱۲۸ بیتی استفاده می‌کند که ۱۲ یا ۱۶ دور تحول را در بلوک‌های ۶۴ بیتی انجام می‌دهد. CAST-256 یک رمزگذاری بلوک است که از یک کلید ۱۲۸، ۱۶۰، ۱۹۲، ۲۲۴ یا ۲۵۶ بیتی استفاده می‌کند که ۴۸ دور تحول را در بلوک‌های ۱۲۸ بیتی انجام می‌دهد.

در جدول ۳-۶ حقایق اصلی در مورد هر الگوریتم متقارن آورده شده است.

Algorithm Name	Block or Stream Cipher?	Key Size	Number of Rounds	Block Size
DES	Block	64 bits (effective length 56 bits)	16	64 bits
3DES	Block	56, 112, or 168 bits	48	64 bits
AES	Block	128, 192, or 256 bits	10, 12, or 14 (depending on block/ key size)	128, 192, or 256 bits
IDEA	Block	128 bits	8	64 bits
Skipjack	Block	80 bits	32	64 bits
Blowfish	Block	32-448 bits	16	64 bits
Twofish	Block	128, 192, or 256 bits	16	128 bits
RC4	Stream	40-2,048 bits	Up to 256	N/A
RC5	Block	Up to 2,048	Up to 255	32, 64, or 128 bits
RC6	Block	Up to 2,048	Up to 255	32, 64, or 128 bits

جدول ۳-۶: حقایق اصلی الگوریتم های متقارن

الگوریتم های نامتقارن Asymmetric Algorithms

الگوریتم های نامتقارن در ابتدای این فصل توضیح داده شد. در این بخش برخی از رایج ترین الگوریتم های نامتقارن را مورد بحث قرار می دهیم. برخی از این موارد ممکن است دیگر مورد استفاده قرار نگیرند زیرا گزینه های مطمئن تری ایجاد شده است. متخصصان امنیت باید با الگوریتم های متقارن زیر آشنا باشند:

- Diffie-Hellman
- RSA
- El Gamal
- ECC
- کوله پشتی Knapsack
- اثبات دانش صفر Zero Knowledge Proof

Diffie-Hellman ✓

یک الگوریتم توافق کلید نامتقارن است که توسط ویتفیلد دیفی و مارتین هلمن ایجاد شده است. دیفی هلمن مسئول فرایند توافق کلید است. فرایند توافق کلید مراحل زیر را شامل می‌شود:

۱- جان و سالی باید از طریق کانال رمزگذاری شده ارتباط برقرار کنند و تصمیم بگیرند که از دیفی هلمن استفاده کنند.

۲- جان یک کلید خصوصی و عمومی تولید می‌کند.

۳- جان و سالی کلیدهای عمومی خود را با یکدیگر به اشتراک می‌گذارند.

۴- یک اپلیکیشن در رایانه جان، کلید خصوصی جان و کلید عمومی سالی و الگوریتم Diffie-Hellman را به کار می‌گیرد و همینطور یک اپلیکیشن در رایانه سالی، کلید خصوصی سالی و کلید عمومی جان را می‌گیرد و الگوریتم Diffie-Hellman را اعمال می‌کند.

۵- از طریق این اپلیکیشن، همان ارزش مشترک برای جان و سالی ایجاد می‌شود که با استفاده از الگوریتم توافق کلید نامتقارن، همان کلید متقارن یکسان را در هر سیستم ایجاد می‌کند.

از طریق این فرآیند، Diffie-Hellman توزیع کلید امن را فراهم می‌کند، اما نه به صورت محرمانه بودن، تایید اعتبار یا عدم تکذیب. کلید این الگوریتم توزیع با لگاریتم‌های گسسته است. Diffie-Hellman مستعد اثر حملات Man-in-the-Middle است مگر اینکه سازمانی در ابتدای فرآیند Diffie-Hellman امضاهای دیجیتالی یا گواهینامه‌های دیجیتال را برای احراز هویت انجام دهد.

RSA ✓

رایج ترین الگوریتم نامتقارن است و توسط Ron Rivest, Adi Shamir, Leonard Adleman اختراع شده است. RSA می‌تواند تبادل کلید، رمزگذاری و امضاهای دیجیتالی را فراهم کند. قدرت الگوریتم RSA یافتن عوامل یا فاکتورهای اصلی از اعداد بسیار بزرگ است. RSA از یک کلید ۱۰۲۴ تا ۴۰۹۶ بیتی استفاده می‌کند و یک دور تحول را انجام می‌دهد.

RSA-768 و RSA-704 فاکتورگیری شده اند. اگر فاکتورگیری تعداد اصلی که توسط یک پیاده سازی RSA استفاده می‌شود رخ دهد، اجرای آن به صورت شکستی در نظر گرفته می‌شود و نباید از آن استفاده شود. RSA-2048 بزرگترین شماره RSA است. به طوریکه جایزه نقدی

۲۰۰۰۰۰ دلار آمریکا برای فاکتورگیری مؤثر موفقیت آمیز پیشنهاد شده است. RSA-4096 تاکنون شکست نخورده است.

به عنوان یک پروتکل تبادل کلیدی، RSA یک کلید متقارن DES یا AES را برای توزیع امن رمزگذاری می کند. RSA از تابع یک طرفه برای ارائه رمزگذاری / رمزگشایی و تأیید امضای دیجیتال / تولید، استفاده می کند. کلید عمومی با تابع یک طرفه برای انجام رمزگذاری و تأیید امضای دیجیتال فعالیت می کند. کلید خصوصی با تابع یک طرفه برای انجام رمزگشایی و تولید امضا کار می کند.

در RSA، تابع یک طرفه Trapdoor است. کلید خصوصی تابع یک طرفه را می شناسد. کلید خصوصی قادر به تعیین شماره های اولیه اصلی است. سرانجام، کلید خصوصی می داند چگونه از تابع یک طرفه برای رمزگشایی پیام رمزگذاری شده استفاده کند.

مهاجمان می توانند برای حمله به RSA از Number Field Sieve (NFS)، یک الگوریتم فاکتورگیری استفاده کنند.

El Gamal ✓

یک الگوریتم کلید نامتقارن مبتنی بر الگوریتم Diffie-Hellman است. مانند Diffie-Hellman با لگاریتم های گسسته سروکار دارد. در حالی که Diffie-Hellman فقط می تواند برای توافقی های کلید مورد استفاده قرار گیرد، El Gamal می تواند تبادل کلید، رمزگذاری و امضای دیجیتال را فراهم کند.

با استفاده از El Gamal، از هر اندازه کلید می توان استفاده کرد. با این حال، اندازه بزرگتر کلید بر عملکرد آن تأثیر منفی می گذارد. از آنجا El Gamal کمترین سرعت الگوریتم نامتقارن را دارد، استفاده از اندازه کلید ۱۰۲۴ بیت یا کمتر عاقلانه است.

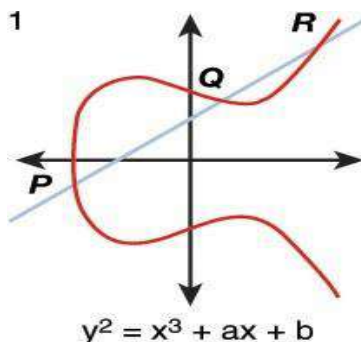
ECC ✓

منحنی بیضوی سیستم رمزنگاری Cryptosystem Elliptic Curve (ECC) توزیع کلیدی امن، رمزگذاری و امضای دیجیتال را فراهم می کند. اندازه منحنی بیضوی دشواری این مساله را مشخص می کند.

اگرچه ECC می تواند از یک کلید به هر اندازه استفاده کند، اما می تواند از کلید بسیار کوچکتری نسبت به RSA یا هر الگوریتم نامتقارن دیگر استفاده کند و هنوز هم امنیت حائز اهمیتی را ارائه می دهد. بنابراین، منافع اصلی وعده داده شده توسط ECC، اندازه کلید کوچکتر می باشد و باعث

کاهش نیازهای ذخیره سازی و انتقال می‌شود. ECC با توجه به اندازه کارآمدتر بوده و امنیت بهتری نسبت به کلیدهای RSA دارد.

شکل ۳-۱۸ نمونه‌ای از منحنی بیضوی را با معادله منحنی بیضوی نشان می‌دهد.



شکل ۳-۱۸: معادله منحنی بیضوی

Knapsack ✓

مجموعه‌ای از الگوریتم‌های نامتقارن است که امضای رمزگذاری و دیجیتالی را ارائه می‌دهد. این گروه الگوریتم‌ها به دلیل مشکلات امنیتی دیگر مورد استفاده قرار نمی‌گیرد.

Zero Knowledge Proof اثبات دانش صفر ✓

اثبات دانش صفر روشی است که برای اطمینان از این که حداقل اطلاعات مورد نیاز بدون ارائه همه جزئیات، استفاده می‌شود. نمونه‌ای از این تکنیک هنگامی رخ می‌دهد که یک کاربر داده‌ها را با کلید خصوصی خود رمزگذاری کند و گیرنده با کلید عمومی مبدأ رمزگشایی کند. مبدأ کلید خصوصی خود را به گیرنده نداده است، اما مبدأ ثابت می‌کند که کلید خصوصی خود را فقط دریافت کننده پیام می‌تواند بخواند.

Public Key Infrastructure زیرساخت کلید عمومی

زیرساخت کلید عمومی (PKI) شامل سیستم‌ها، نرم افزارها و پروتکل‌های ارتباطی است که توزیع، مدیریت و کنترل رمزنگاری کلید عمومی را شامل می‌شود. یک PKI گواهی‌های دیجیتال را منتشر می‌کند. از آنجا که یک PKI اعتماد به یک محیط را ایجاد می‌کند، یک PKI می‌تواند تأیید کند که یک کلید عمومی به یک موجودیت (Entity) گره خورده است و تأیید کرده است

که یک کلید عمومی معتبر است. کلیدهای عمومی از طریق گواهینامه‌های دیجیتال منتشر می‌شوند.

استاندارد X.509 چارچوبی است که احراز هویت بین شبکه‌ها و اینترنت را ممکن می‌سازد PKI. شامل زمان سنجی و ابطال مجوز برای اطمینان از مدیریت درست گواهینامه‌ها است، PKI محرمانه، یکپارچگی پیام، احراز هویت و عدم تکذیب را فراهم می‌کند. ساختار PKI شامل CA، گواهینامه‌ها، مراجع ثبت نام، لیست‌های ابطال مجوز، صدور گواهینامه متقابل و پروتکل آنلاین وضعیت صدور گواهی (OCSP) است. در این بخش، ما در مورد این مؤلفه‌های PKI و همچنین چند مفهوم دیگر PKI بحث می‌کنیم. مرجع صدور گواهینامه و مرجع ثبت

Certification Authority (CA) and Registration Authority (RA)

هر مشارکت کننده‌ای که درخواست گواهینامه می‌کند باید ابتدا از طریق مرجع ثبت نام (RA)، هویت درخواست کننده را تأیید و درخواست کننده را ثبت می‌کند. پس از تأیید هویت، RA درخواست را به CA ارسال می‌کند.

مرجع صدور گواهینامه (CA) مؤسسه‌ای است که گواهینامه‌های دیجیتالی را ایجاد و امضا می‌کند، گواهینامه‌ها را حفظ کرده و در صورت لزوم آنها را ابطال می‌کند. هر موجودیت که می‌خواهد در PKI شرکت کند باید با CA تماس بگیرد و یک گواهی دیجیتالی را درخواست کند. این امر با امضای هر گواهی نامه دیجیتالی، قدرت نهایی برای صحت هر شرکت کننده در PKI است. گواهینامه هویت شرکت کننده را با کلید عمومی پیوند می‌زند.

انواع مختلف CA وجود دارد. سازمان هایی وجود دارند که PKI را به عنوان خدمات قابل پرداخت به شرکت هایی که به آنها نیاز دارند ارائه می‌دهند. نمونه‌ای از آن Symantec است. بعضی از سازمانها CA های خصوصی خود را به گونه‌های اجرا می‌کنند که سازمان بتواند تمامی جوانب روند PKI را کنترل کند. اگر یک سازمان به اندازه کافی بزرگ باشد، ممکن است نیاز به ساختاری از CA ها داشته باشد که ریشه CA بالاترین سطح در سلسله مراتب باشد.

از آنجا که بیش از یک موجودیت اغلب در فرآیند صدور گواهینامه PKI درگیر است، اعتبارسنجی مسیر صدور گواهینامه به شرکت کنندگان امکان می‌دهد تا مشروعیت گواهینامه‌ها را در مسیر صدور گواهینامه بررسی کنند.

OCSP

پروتکل اینترنتی است که وضعیت ابطال یک گواهی دیجیتالی X.509 را بدست می‌آورد. OCSP جایگزینی برای لیست ابطال مجوزهای استاندارد (Certificate revocation list (CRL است که توسط بسیاری از PKI ها استفاده می‌شود. OCSP به طور خودکار گواهینامه‌ها را تأیید می‌کند و گزارش‌های موجود با دسترسی به CRL در CA را از وضعیت گواهی دیجیتال بازمی‌گرداند.

گواهینامه‌ها Certificates

یک گواهی نامه دیجیتالی برای اثبات هویت خود به یک موجودیت، معمولاً به کاربر، اعتبار می‌دهد و آن هویت را با یک کلید عمومی مرتبط می‌کند. حداقل، یک گواهینامه دیجیتال باید شماره سریال، صادر کننده، موضوع (مالک) و کلید عمومی را ارائه دهد. یک گواهی X.509 مطابق با استاندارد X.509 است. یک گواهی X.509 شامل قسمت‌های زیر است:

- ✓ نسخه Version
- ✓ شماره سریال Serial Number
- ✓ شناسه الگوریتم Algorithm ID
- ✓ صادر کننده Issuer
- ✓ اعتبار Validity
- ✓ موضوع Subject
- ✓ موضوع کلید اطلاعات عمومی Subject Public Key Info
 - الگوریتم کلید عمومی Public Key Algorithm
 - موضوع کلید عمومی Subject Public Key
- ✓ شناسه منحصر به فرد صادر کننده (اختیاری) Issuer Unique Identifier (optional)
- ✓ شناسه منحصر به فرد موضوع (اختیاری) Subject Unique Identifier (optional)
- ✓ برنامه‌های افزودنی (اختیاری) Extensions (optional)

Symantec ابتدا کلاسهای مجوز دیجیتال زیر را معرفی کرد:

کلاس ۱: برای افرادی که ایمیل در نظر گرفته شده است. این گواهینامه‌ها توسط مرورگرهای وب ذخیره می‌شوند.

کلاس ۲: برای سازمان هایی که باید اثبات هویت ارائه دهند.
 کلاس ۳: برای سرورها و امضای نرم افزاری که در آن تأیید مستقل و بررسی هویت و قدرت توسط صدور CA انجام می شود.

لیست ابطال مجوزها (Certificate Revocation List (CRL

CRL لیستی از گواهینامه های دیجیتالی است که یک CA آن را باطل کرده است. برای اطلاع از اینکه آیا مجوز دیجیتالی ابطال شده است، مرورگر باید CRL را بررسی کند یا CA باید مقادیر CRL را به مشتری منتقل کند. این مسئله می تواند بسیار دلهره آور باشد وقتی که در نظر بگیرید که CRL شامل هر گواهینامه ای است که قبلاً ابطال شده است. یکی از ایده هایی که باید در نظر داشته باشید دوره تایید تقاضای ابطال است. این دوره حداکثر زمان بین زمان دریافت درخواست ابطال توسط CA و زمان وقوع ابطال در واقعیت است. یک دوره ابطال کوتاهتر امنیت بهتری را ارائه می دهد اما اغلب منجر به هزینه پیاده سازی بالاتری می شود.

مراحل انجام درخواست گواهینامه دیجیتالی به شرح زیر است:

- ۱- یک کاربر درخواست گواهی نامه دیجیتالی می کند، و RA این درخواست را دریافت می کند.
 - ۲- RA درخواست شناسایی اطلاعات از درخواست کننده را می دهد.
 - ۳- پس از دریافت اطلاعات مورد نیاز، RA درخواست گواهی نامه را به CA ارسال می کند.
 - ۴- CA یک گواهی نامه دیجیتالی برای درخواست کننده ایجاد می کند. کلید عمومی و اطلاعات هویت درخواست کننده به عنوان بخشی از گواهینامه درج می شود.
 - ۵- کاربر گواهی نامه را دریافت می کند.
- بعد از اینکه کاربر دارای گواهینامه شد، وی آماده ارتباط با دیگر اشخاص قابل اعتماد است. روند برقراری ارتباط بین موجودیت (Entity) به شرح زیر است:
- ۱- کاربر ۱ کلید عمومی کاربر ۲ را از مخزن (Repository) گواهی نامه درخواست می کند.
 - ۲- مخزن، گواهی نامه دیجیتالی کاربر ۲ را به کاربر ۱ ارسال می کند.
 - ۳- کاربر ۱ گواهی نامه را تأیید می کند و کلید عمومی کاربر ۲ را استخراج می کند.
 - ۴- کاربر ۱ کلید جلسه را با کلید عمومی کاربر ۲ رمزگذاری می کند و کلید جلسه رمزگذاری شده و گواهی نامه کاربر ۱ را به کاربر ۲ ارسال می کند.

۵- کاربر ۲ گواهی نامه کاربر ۱ را دریافت می‌کند و گواهی نامه را با یک CA قابل اعتماد تأیید می‌کند.

پس از انجام این فرآیند تبادل و تأیید مجوز، هر دو نهاد با استفاده از رمزگذاری قادر به برقراری ارتباط هستند.

گواهینامه متقابل Cross-Certification

صدور گواهینامه متقابل روابط اعتماد بین CA را برقرار می‌کند تا CAهای شرکت کننده بتوانند به گواهینامه‌های دیجیتال و کلیدهایی عمومی سایر شرکت کنندگان اعتماد کنند. این امکان را به کاربران می‌دهد تا گواهی نامه‌های یکدیگر را هنگامی که آنها واقعاً تحت سلسله مراتب صدور گواهینامه مختلف تأیید شده اند، تأیید کنند. در صورت وجود یک رابطه اعتماد متقابل یک CA برای یک سازمان می‌تواند گواهی نامه‌های دیجیتالی را از CA سازمان دیگر تأیید کند.

شیوه‌های عملیات مدیریت کلید Key Management Practices

بحث در مورد رمزنگاری بدون پوشش شیوه‌های مدیریت کلید، ناقص خواهد بود. NIST SP 800-57 شامل توصیه‌هایی برای مدیریت کلید در سه بخش می‌باشد: قسمت اول: این پیش نویس نشریات توصیه‌های کلی برای مدیریت کلیدی را در بر می‌گیرد. قسمت دوم: این نشریات بهترین شیوه‌های مدیریت کلید یک سازمان را در بر می‌گیرد. قسمت سوم: این نشریه راهنمایی مدیریت کلیدی خاص برنامه را در بر می‌گیرد. متخصصان امنیت حداقل باید اصول اصلی مدیریت را در قسمت اول، SP 80057 درک کنند. اگر متخصصان امنیت در سازمانهایی شرکت می‌کنند که خدمات مدیریت کلید را به سازمانهای دیگر ارائه می‌دهند، درک قسمت دوم یک ضرورت است. قسمت سوم وقتی سازمان برنامه‌هایی را که از کلید استفاده می‌کنند اجرا می‌شود لازم است.

چندین نوع کلید مختلف تعریف شده است. این کلیدها طبق طبقه بندی آنها به عنوان کلیدهای عمومی، خصوصی یا متقارن و همچنین با توجه به کاربرد آنها مشخص می‌شوند. برای کلیدهای توافق کلید عمومی و خصوصی، وضعیت به عنوان کلیدهای ایستا یا زودگذر نیز مشخص شده است:

- **کلید امضای خصوصی Private signature key:** این کلیدهای خصوصی جفت‌های نامتقارن (عمومی) هستند که توسط الگوریتم‌های کلید عمومی برای تولید امضاهای

دیجیتالی با پیامدهای احتمالی بلند مدت استفاده می شوند. در صورت بکاربردن صحیح، از کلیدهای امضای خصوصی می توان برای احراز هویت منبع، تأیید یکپارچگی هویت و پشتیبانی از عدم تکذیب، اسناد یا داده های ذخیره شده استفاده کرد.

- **کلید تأیید امضای عمومی Public signature-verification key:** این کلید عمومی یک جفت کلید نامتقارن (عمومی) است که توسط یک الگوریتم کلید عمومی برای تأیید امضاهای دیجیتالی که برای تأمین اعتبار منبع، تأمین اعتبار یکپارچگی و پشتیبانی از عدم رد پیام، پیام ها، اسناد یا داده های ذخیره شده استفاده می کند.
- **کلید احراز هویت متقارن Symmetric authentication key:** این کلید با الگوریتم های کلید متقارن به منظور احراز هویت منبع و اطمینان از صحت جلسات ارتباطی، پیام ها، اسناد یا داده های ذخیره شده استفاده می شود (یعنی تأیید یکپارچگی).
- **کلید احراز هویت خصوصی Private authentication key:** این کلید خصوصی یک جفت کلید نامتقارن (عمومی) است که با استفاده از یک الگوریتم کلید عمومی برای اطمینان از هویت موجودیت اصلی (یعنی منبع) هنگام ایجاد یک جلسه ارتباطی معتبر استفاده می شود.
- **کلید احراز هویت عمومی Public authentication key:** این کلید عمومی یک جفت کلید نامتقارن (عمومی) است که از یک الگوریتم کلید عمومی استفاده می شود تا اطمینان حاصل شود که هویت یک موجودیت اصلی (یعنی منبع) هنگام ایجاد یک جلسه ارتباطی معتبر ارائه شده است.
- **کلید رمزگذاری داده متقارن Symmetric data-encryption key:** این کلید از الگوریتم های کلید متقارن برای اعمال محافظت از محرمانه بودن اطلاعات (یعنی رمزگذاری اطلاعات) استفاده می کند. همین کلید نیز برای از بین بردن محافظت از محرمانه بودن (یعنی رمزگشایی اطلاعات) استفاده می کند.
- **کلید بسته بندی کلید متقارن (به آنها کلیدهای کلید رمزگذاری نیز می گویند) Symmetric key-wrapping key:** این کلید برای رمزگذاری سایر کلیدها با استفاده از الگوریتم های کلید متقارن انجام می شود. از کلید بسته بندی کلید برای رمزگذاری یک کلید و برای معکوس کردن عملیات رمزگذاری استفاده می شود (یعنی رمزگشایی).

کلید رمزگذاری شده)، ممکن است از این کلید بستگی به الگوریتمی که از آن استفاده می‌شود برای محافظت از یکپارچگی استفاده شود.

- **کلیدهای تولید شماره تصادفی متقارن Symmetric random number generation keys:** این کلید برای تولید اعداد تصادفی یا بیت‌های تصادفی استفاده می‌شود.
- **کلید اصلی متقارن Symmetric master key:** این کلید برای استخراج سایر کلیدهای متقارن (به عنوان مثال، کلیدهای رمزگذاری داده، کلیدهای بسته بندی کلید یا کلیدهای احراز هویت منبع) استفاده می‌شود.
- **کلید اصلی همچنین به عنوان کلید مشتق Key-Derivation:** شناخته می‌شود.
- **کلید انتقال کلید خصوصی Private key-transport key:** کلیدهای خصوصی جفتهای کلید نامتقارن (عمومی) هستند که برای رمزگشایی کلیدهایی که با کلید عمومی مربوطه با استفاده از یک الگوریتم کلید عمومی، رمزگذاری می‌شوند. از کلیدهای انتقال کلید معمولاً برای ایجاد کلیدها (به عنوان مثال، کلیدهای بسته بندی کلید، کلیدهای رمزگذاری داده یا کلیدها MAC)، به صورت اختیاری، سایر موارد کلید سازی (به عنوان مثال، بردارهای اولیه IV) استفاده می‌شوند.
- **کلید انتقال عمومی Public key-transport key:** این کلیدهای عمومی جفتهای کلید نامتقارن (عمومی) هستند که برای رمزگذاری کلیدها با استفاده از الگوریتم کلید عمومی استفاده می‌شوند. این کلیدها برای ایجاد کلیدها (به عنوان مثال، کلیدهای بسته بندی کلید، کلیدهای رمزگذاری داده یا کلیدهای MAC)، به صورت اختیاری، سایر موارد کلید سازی (به عنوان مثال، بردارهای اولیه IV) استفاده می‌شوند. ممکن است فرم رمزگذاری شده کلید رمزگذاری شده برای رمزگشایی بعدی با استفاده از کلید انتقال کلید خصوصی ذخیره شود.
- **کلید توافق کلید متقارن Symmetric key-agreement key:** این کلید برای ایجاد کلیدها (به عنوان مثال، کلیدهای بسته بندی کلید، کلیدهای رمزگذاری داده یا کلیدهای MAC)، به صورت اختیاری، سایر موارد کلید سازی (به عنوان مثال، بردارهای اولیه)، با استفاده از یک کلید توافق متقارن، انجام می‌شود.

- **کلید توافق کلید ایستای خصوصی Private static key-agreement key :** این کلیدهای خصوصی بلند مدت جفتهای کلید نامتقارن (عمومی) هستند که برای ایجاد کلیدها استفاده می‌شوند (به عنوان مثال، کلیدهای بسته بندی کلید، کلیدهای رمزگذاری داده یا کلیدهای MAC)، به صورت اختیاری، دیگر موارد کلید سازی (به عنوان مثال، بردارهای اولیه).
- **کلید توافق کلید ایستای عمومی Public static key-agreement key :** کلیدهای عمومی بلند مدت جفتهای نامتقارن (عمومی) هستند که برای ایجاد کلیدها استفاده می‌شوند (به عنوان مثال، کلیدهای بسته بندی کلید، کلیدهای رمزگذاری داده یا کلیدهای MAC)، به صورت اختیاری، دیگر موارد کلید سازی (به عنوان مثال، بردارهای اولیه).
- **کلید خصوصی کلید توافق زودگذر خصوصی Private ephemeral key-agreement key :** کلیدهای خصوصی کوتاه مدت جفتهای کلید نامتقارن (عمومی) هستند که فقط یک بار برای ایجاد یک یا چند کلید استفاده می‌شوند (به عنوان مثال، کلیدهای بسته بندی کلید، کلیدهای رمزگذاری داده یا کلیدهای MAC)، به صورت اختیاری، سایر مواد کلیدسازی (مانند بردارهای اولیه).
- **کلید توافق زودگذر عمومی Public ephemeral key-agreement key :** این کلیدهای عمومی کوتاه مدت جفتهای کلید نامتقارن هستند که در تراکنش ایجاد کلید واحد برای ایجاد یک یا چند کلید استفاده می‌شوند (به عنوان مثال، کلیدهای بسته بندی کلید، کلیدهای رمزگذاری داده یا کلیدهای MAC)، به صورت اختیاری، سایر موارد کلید (به عنوان مثال، بردارهای مقداردهی اولیه).
- **کلید مجوز متقارن Symmetric authorization key :** این نوع کلید برای ارائه امتیازات به یک واحد با استفاده از روش رمزنگاری متقارن استفاده می‌کند. کلید مجوز توسط سازمان مسئول نظارت و اعطای امتیازات دسترسی برای اشخاص مجاز و همچنین موجودیت مورد نظر برای دسترسی به منابع، شناخته شده است.
- **کلید مجوز خصوصی Private authorization key :** این کلید خصوصی یک جفت کلید نامتقارن (عمومی) است که برای ارائه امتیازات به یک موجودیت استفاده می‌شود.

- **کلید مجوز عمومی Public authorization key**: این کلید عمومی یک جفت کلید نامتقارن (عمومی) است که برای تأیید امتیازات برای یک موجودیت که کلید مجوز خصوصی مرتبط را می‌شناسد استفاده می‌شود.
- به طور کلی، یک کلید واحد، تنها برای یک هدف استفاده می‌شود (مثلاً رمزگذاری، یکپارچگی، احراز هویت، بسته بندی کلید، تولید بیت تصادفی یا امضاهای دیجیتالی). دوره رمزنگاری cryptoperiod زمانی است که در طی آن یک کلید خاص برای استفاده توسط اشخاص قانونی مجاز می‌باشد یا مدت زمانی که کلیدهای مربوط در یک سیستم معین قابل اجرا هستند. از جمله عوامل مؤثر بر طول یک رمزنگاری عبارتند از:
 - ✓ قدرت رمزنگاری (به عنوان مثال، الگوریتم، طول کلید، اندازه بلوک و حالت عملیات)
 - ✓ تجسم مکانیزمها (به عنوان مثال، اجرای [FIPS140] سطح ۴ یا اجرای نرم افزار در رایانه شخصی)
 - ✓ محیط عملیاتی (به عنوان مثال، یک مرکز دسترسی محدود، محیط اداری باز یا ترمینال در دسترس عموم)
 - ✓ حجم جریان اطلاعات یا تعداد تراکنش ها
 - ✓ عمر امنیتی داده ها
 - ✓ عملکرد امنیتی (به عنوان مثال، رمزگذاری داده ها، امضای دیجیتال، مشتق کلید یا محافظت از کلید)
 - ✓ روش اتصال مجدد کلید (به عنوان مثال، ورود به صفحه کلید، کلید زدن مجدد با استفاده از یک دستگاه بارگذاری کلید key loading که در آن انسانها دسترسی مستقیم به اطلاعات کلیدی یا کلید مجدد از راه دور (Remote Re-keying) در یک PKI ندارند).
 - ✓ فرایندهای بروزرسانی کلید یا مشتق کلید
 - ✓ تعداد گره‌های موجود در شبکه که دارای یک کلید مشترک هستند
 - ✓ تعداد نسخه‌های یک کلید و توزیع آن نسخه ها
 - ✓ گردش مالی پرسنل (به عنوان مثال، کاربر سیستم CA)
 - ✓ تهدید اطلاعات از طرف رقبا (مثلاً اطلاعاتی که از آنها محافظت می‌شود و تواناییهای فنی درک شده و منابع مالی آنها برای حمله) تهدید اطلاعات از فن آوری‌های جدید و

مخرب (به عنوان مثال، رایانه های کوانتومی) الزامات محافظت از کلیدهای رمزنگاری شده در جدول ۳-۷ نشان داده شده است.

ستون عمودی سرویس امنیتی لیست خدمات امنیت توسط کلید را ارائه می دهد. ستون حمایت امنیتی (Security Protection) نوع حفاظت مورد نیاز برای کلید را فهرست می کند.

Key Type	Security Service	Security Protection	Period of Protection
Private signature key	Source authentication	Integrity	From generation until the end of the cryptoperiod
	Integrity authentication	Confidentiality	
	Support nonrepudiation		
Public signature verification key	Source authentication	Integrity	From generation until no protected data needs to be verified
	Integrity authentication		
	Support nonrepudiation		
Symmetric authentication key	Source authentication	Integrity	From generation until no protected data needs to be verified
	Integrity authentication	Confidentiality	
Private authentication key	Source authentication	Integrity	From generation until the end of the cryptoperiod
	Integrity authentication	Confidentiality	
Public authentication key	Source authentication	Integrity	From generation until no protected data needs to be authenticated
	Integrity authentication		
Symmetric data encryption/decryption key	Confidentiality	Integrity Confidentiality	From generation until the end of the lifetime of the data or the end of the cryptoperiod, whichever comes later

Symmetric key-wrapping key	Support	Integrity Confidentiality	From generation until the end of the cryptoperiod or until no wrapped keys require protection, whichever is later
Symmetric RGB key	Support	Integrity Confidentiality	From generation until replaced
Symmetric master key	Support	Integrity Confidentiality	From generation until the end of the cryptoperiod or the end of the lifetime of the derived keys, whichever is later
Private key-transport key	Support	Integrity Confidentiality	From generation until the end of the period of protection for all transported keys
Public key-transport key	Support	Integrity	From generation until the end of the cryptoperiod
Symmetric key-agreement key	Support	Integrity Confidentiality	From generation until the end of the cryptoperiod or until no longer needed to determine a key, whichever is later
Private static key-agreement key	Support	Integrity Confidentiality	From generation until the end of the cryptoperiod or until no longer needed to determine a key, whichever is later
Public static key-agreement key	Support	Integrity	From generation until the end of the cryptoperiod or until no longer needed to determine a key, whichever is later
Private ephemeral key-agreement key	Support	Integrity Confidentiality	From generation until the end of the key-agreement process; after the end of the process, the key is destroyed
Public ephemeral key-agreement key	Support	Integrity	From generation until the key-agreement process is complete
Symmetric authorization keys	Authorization	Integrity Confidentiality	From generation until the end of the cryptoperiod of the key
Private authorization key	Authorization	Integrity Confidentiality	From generation until the end of the cryptoperiod of the key
Public authorization key	Authorization	Integrity	From generation until the end of the cryptoperiod of the key

جدول ۳-۷: الزامات محافظت در مورد کلیدهای رمزنگاری

باتوجه به وضعیت آن در چرخه عمر کلید، یک کلید متفاوت استفاده می شود. حالت های کلید از نقطه نظر سیستم، بر خلاف نقطه نظر یک ماژول رمزنگاری منفرد تعریف می شوند. حالت هایی که ممکن است یک کلید عملیاتی یا پشتیبان گیری فرض شود به شرح زیر است:

- **حالت قبل از فعال سازی Pre-activation state:** کلید تولید شده است اما برای استفاده مجاز نیست. در این حالت، ممکن است از کلید فقط برای انجام اثبات تملک یا تأیید کلید استفاده شود.
- **حالت فعال Active state:** این کلید ممکن است برای محافظت از رمزنگاری اطلاعات (به عنوان مثال رمزگذاری متن ساده plaintext یا تولید یک امضای دیجیتال)، برای پردازش رمزنگاری اطلاعات از قبل محافظت شده (به عنوان مثال رمزگشایی متن رمزگذاری شده ciphertext یا تأیید یک امضای دیجیتال) یا هر دو، مورد استفاده قرار گیرد. هنگامی که یک کلید فعال است، بسته به نوع آن، فقط برای محافظت یا فقط پردازش، یا محافظت و پردازش نیز ممکن است تعیین شود.
- **حالت معلق Suspended state:** استفاده از یک جفت کلید یا یک کلید، امکان دارد به دلایل مختلف به حالت معلق درآید. در مورد جفت های کلید نامتقارن، کلیدهای عمومی و خصوصی هم زمان به حالت معلق در می آیند. یکی از دلایل معلق ممکن است یک سازش مهم احتمالی باشد تا زمان بررسی وضعیت را بدهد. دلیل دیگر ممکن است این باشد که موجودیت یک جفت کلید امضای دیجیتالی در دسترس نیست (مثلاً در مرخصی بلند مدت یا غیبت است)، امضاهایی که گفته شده در زمان تعلیق امضا شده اند، نامعتبر است. یک کلید یا جفت کلید معلق ممکن است بعداً به حالت فعال برگردد یا غیرفعال یا از بین برود، یا ممکن است به حالت سازش (مصالحه) منتقل شود.
- **حالت غیرفعال Deactivated state:** از کلیدهای موجود در حالت غیرفعال برای اعمال حفاظت از رمزنگاری استفاده نمی شود، اما در بعضی موارد ممکن است از آنها برای پردازش اطلاعات محافظت شده با رمزنگاری استفاده شود. اگر یک کلید ابطال شده باشد (به دلایل دیگری غیر از مصالحه یا سازش)، ممکن است این کلید همچنان برای پردازش استفاده شود. توجه داشته باشید که کلیدهای بازیابی شده از آرشیو می توانند در حالت غیرفعال تلقی شوند، مگر اینکه به حالت سازش (مصالحه) منتقل شود.

- **حالت مصالحه یا سازش Compromised state:** به طور کلی، کلیدها وقتی توسط یک موجودیت غیرمجاز آزاد یا تعیین می‌شوند به خطر می‌افتند. برای به کار بردن حفاظت رمزنگاری در اطلاعات، از کلید سازش نباید استفاده شود. با این وجود، در برخی موارد، یک کلید سازش (مصالحه) یا یک کلید عمومی مربوط به یک کلید خصوصی به سازش یک جفت کلید می‌باشد که ممکن است برای پردازش اطلاعات محافظت شده رمزنگاری شده استفاده شود. به عنوان مثال، ممکن است یک امضا تأیید شود تا یکپارچگی داده‌های امضا شده را تأیید کند اگر امضای آن از زمانی قبل از وقوع سازش از نظر فیزیکی محافظت شده باشد. این پردازش فقط در شرایط بسیار کنترل شده انجام می‌شود، در حالی که کاربران اطلاعات کاملاً از عواقب احتمالی آگاه هستند.
- **حالت تخریب Destroyed state:** کلید همانطور که در مرحله تخریب مشخص شده که نابود می‌شود. حتی اگر در این حالت کلید دیگر وجود نداشته باشد، ممکن است ابر داده‌ها Metadata کلیدی خاص (به عنوان مثال، تاریخ انتقال کلید اصلی، نام اصلی، نوع، رمزنگاری) حفظ شود.

چرخه عمر مدیریت کلید رمزنگاری را می‌توان به چهار مرحله زیر تقسیم کرد:

۱- **فاز قبل از عمل Pre-operational phase:** موارد کلید سازی برای عملیات رمزنگاری عادی هنوز در دسترس نیست. ممکن است کلید هنوز تولید نشده یا در حالت قبل از فعال سازی قرار داشته باشد. سیستم یا ویژگی‌های سازمانی نیز در این فاز ایجاد می‌شود. در طی این مرحله، عملکرد زیر رخ می‌دهد:

الف. ثبت نام کاربر User registration

ب. ساخت اولیه سیستم System initialization

ج. ساخت اولیه کاربر User initialization

د. نصب کلیدهای مواد Keying-material installation

ه. استقرار کلیدی Key establishment

ز. ثبت کلید Key registration

۲- **فاز عملیاتی Operational phase:** موارد کلید سازی در دسترس بوده و در حالت عادی استفاده می‌شود. کلیدها در حالت فعال، معلق یا غیرفعال قرار دارند. کلیدهای موجود در حالت فعال فقط به عنوان محافظت یا فقط پردازش یا محافظت و پردازش تعیین می‌شوند. کلیدهای

موجود در حالت معلق یا غیرفعال فقط برای پردازش قابل استفاده هستند. در طی این مرحله، عملکرد زیر رخ می دهد:

الف. یک ذخیره سازی عملیاتی عادی Normal operational storage

ب. استمرار عملیات Continuity of operations

ج. تغییر کلید Key change

د. استخراج کلید Key derivation

۳- فاز بعد از عملیات Post-operational phase: موارد کلید سازی دیگر در حالت عادی استفاده نمی شود، اما دسترسی به موارد کلید سازی امکان پذیر است و فقط در شرایط خاص می توان برای پردازش استفاده کرد. کلیدها در حالت غیرفعال یا سازش هستند. کلیدها در مرحله بعد از فعالیت ممکن است هنگامی که پردازش داده ها صورت نمی گیرد در آرشیو باشند. در طی این مرحله عملکرد زیر رخ می دهد:

الف. یک ذخیره سازی بایگانی و بازیابی کلید Archive storage and key recovery

ب. ثبت نام مجدد موجودیت Entity de-registration

پ. ثبت نام مجدد کلید Key de-registration

ت. تخریب کلید Key destruction

س. ابطال کلید Key revocation

۴- فاز تخریب Destroyed phase: کلیدها دیگر در دسترس نیستند. سوابق وجود آنها ممکن است حذف شده باشند یا حذف شده نباشد. کلیدها در حالت های تخریب شده قرار دارند. اگرچه این کلیدها از بین می روند، کلید ابر داده ها Meta Data (به عنوان مثال، نام کلید، نوع، رمزنگاری، دوره استفاده) ممکن است حفظ شود.

سیستم هایی که اطلاعات ارزشمند را پردازش می کنند، به منظور محافظت از اطلاعات در برابر افشا و اصلاح غیرمجاز، نیاز به کنترل دارند. سیستم های رمزنگاری که حاوی کلیدها و سایر اطلاعات رمزنگاری هستند بسیار مهم هستند. متخصصان امنیت باید برای اطمینان از اینکه محافظت از موارد مهم، پاسخگویی، ممیزی و بقا را فراهم می کند، تلاش کنند.

مسئولیت پذیری (Accountability) شامل شناسایی اشخاصی است که در کل چرخه های زندگی خود به کلیدهای رمزنگاری دسترسی یا کنترل دارند. مسئولیت پذیری می تواند ابزاری مؤثر برای جلوگیری از سازش های (مصالحه) کلیدی و کاهش تأثیر سازش در هنگام شناسایی باشد. اگرچه

ترجیح داده می‌شود هیچ انسانی قادر به مشاهده کلیدها نباشد، اما سیستم مدیریت کلید باید کلیه افرادی که قادر به مشاهده کلیدهای رمزنگاری متن ساده plaintext هستند را به خود اختصاص دهد. علاوه بر این، سیستم‌های مدیریت کلید پیچیده تر ممکن است تمام افراد مجاز به دسترسی یا کنترل کلیدهای رمزنگاری، چه به صورت متن ساده plaintext و چه متن رمزگذاری شده ciphertext، را به خود اختصاص دهند.

دو نوع ممیزی باید روی سیستم‌های مدیریت کلید انجام شود:

امنیت Security: طرح (Plan) امنیتی و رویه‌هایی که برای پشتیبانی از این طرح تدوین شده است باید بطور دوره‌ای مورد بازرسی قرار گیرد تا تضمین شود که آنها همچنان از سیاست‌های مدیریت کلید پشتیبانی می‌کنند.

محافظ Protective: سازوکارهای حفاظتی بکار رفته باید با توجه به سطح امنیتی که در حال حاضر ارائه می‌دهند، مورد ارزیابی مجدد قرار گیرند و انتظار می‌رود در آینده آنها را تأمین کنند. همچنین باید ارزیابی شوند تا مشخص شود آیا سازوکارها به درستی و به طور مؤثر از سیاست‌های مناسب پشتیبانی می‌کنند. تحولات و حملات جدید فن آوری باید به عنوان بخشی از ممیزی محافظ در نظر گرفته شود.

بقای مدیریت کلید مستلزم پشتیبان‌گیری یا آرشیو‌کپی از کلیه کلیدهای استفاده شده است. برای اطمینان از گم شدن کلیدها، باید مراحل پشتیبان‌گیری و بازیابی کلید برقرار شود. افزونگی سیستم و برنامه ریزی‌های احتمالی نیز باید به درستی ارزیابی شوند تا تضمین شود که تمام سیستم‌های درگیر در مدیریت کلید دارای تحمل خطا هستند.

امضاهای دیجیتال Digital Signatures

امضای دیجیتالی یک مقدار هش رمزگذاری شده با کلید خصوصی فرستنده است. امضای دیجیتالی احراز هویت، عدم تکذیب و یکپارچه بودن را فراهم می‌آورد. امضای کورکورانه Blind Signature نوعی امضای دیجیتالی است که در آن محتوای پیام قبل از امضای آن پوشش داده می‌شود.

رمزنگاری کلید عمومی، که در قسمت بعدی مورد بحث قرار می‌گیرد، برای ایجاد امضاهای دیجیتالی استفاده می‌شود. کاربران کلیدهای عمومی خود را با یک CA ثبت می‌کنند که گواهی حاوی کلید عمومی کاربر و امضای دیجیتال CA را توزیع می‌کند. امضای دیجیتال توسط کلید

عمومی و دوره اعتبار کاربر در کنار صدور گواهی و شناسه الگوریتم امضای دیجیتال محاسبه می شود.

استاندارد امضای دیجیتال Digital Signature Standard (DSS) یک استاندارد امنیتی دیجیتال فدرال است که بر الگوریتم امنیت دیجیتال (DSA) حاکم است، DSA 160 پیام را تولید می کند. دولت فدرال ایالات متحده برای امضاهای دیجیتالی نیاز به استفاده از RSA، DSA که در ابتدا در این بخش مورد بحث قرار گرفت و یا Elliptic Curve DSA (ECDSA) و SHA دارد. DSA از RSA کندتر می باشد و فقط امضاهای دیجیتالی را ارائه می دهد. RSA امضاهای دیجیتالی، رمزگذاری و توزیع کلید متقارن امن را فراهم می کند.

هنگام بررسی رمزنگاری، موارد زیر را به خاطر داشته باشید:

- رمزگذاری محرمانه است.
- هشینگ یکپارچگی را فراهم می کند.
- امضاهای دیجیتال احراز هویت، عدم تکذیب و یکپارچگی را ارائه می دهند.

مدیریت حقوق دیجیتال (Digital Rights Management (DRM

برای مهندسی امنیت، متخصصان امنیت باید مطمئن شوند که سازمانها از سیاستها و رویه های DRM برای محافظت از مالکیت معنوی از جمله موسیقی، فیلم، کتابهای الکترونیکی و نرم افزار استفاده می کنند. اجرای DRM امروزه شامل موارد زیر است:

✓ فهرست Directories

- پروتکل دسترسی به فهرست سبک Lightweight Directory Access Protocol (LDAP)

- فهرست فعال Active Directory (AD)

- سفارشی Custom

✓ مجوزها:

- باز کردن Open

- چاپ کردن Print

- اصلاح کردن Modify

- کلیپ برد Clipboard

✓ کنترل های اضافی Additional controls

- انقضا (ابطال مطلق، نسبی، فوری) Expiration
- نسخه کنترل Version control
- تغییر سیاست در اسناد موجود Change policy on existing documents
- سایه‌گذاری دیجیتالی Watermarking
- آنلاین / آفلاین Online/offline
- ممیزی Auditing
- ✓ فرآیندهای موقت و ساختار یافته Ad hoc and structured processes
- کاربر آغازین بر روی دسکتاپ User initiated on desktop
- نقشه برداری سیستم Mapped to system
- ساخته شده در روند جریان کار Built into workflow process

یکپارچگی پیام Message Integrity

یکپارچگی یکی از سه اصول اساسی امنیت است. یکپارچگی پیام تضمین می‌کند که یک پیام با استفاده از بیت‌های برابر یا یکسان Parity bits، بررسی‌های افزونگی چرخشی (CRC) یا Checksumها تغییر نکرده است.

روش بیت یکسان bit parity مقدار کمی به داده اضافه می‌کند. این بیت یکسان به سادگی نشان می‌دهد که آیا تعداد ۱ بیت، زوج یا فرد است. بیت یکسان ۱ است اگر تعداد ۱ بیتها فرد باشد، و بیت یکسان ۰ می‌باشد اگر تعداد ۱ بیتها زوج می‌باشد. قبل از انتقال داده‌ها، بیت یکسان تنظیم شده است. با ورود داده‌ها، میزان بیت یکسان در برابر سایر داده‌ها بررسی می‌شود. اگر بیت یکسان با داده‌های ارسالی مطابقت ندارد، خطایی به مبدأ ارسال می‌شود.

روش CRC از تقسیم چند جمله‌ای برای تعیین مقدار CRC برای یک فایل استفاده می‌کند. مقدار CRC معمولاً طول آن ۱۶ یا ۳۲ بیت است. از آنجا که CRC بسیار دقیق است، اگر یک بیت نادرست باشد، مقدار CRC مطابقت نخواهد داشت.

روش checksum بایت داده‌های ارسال شده را اضافه می‌کند و سپس با استفاده از همان روش، شماره را منتقل می‌کند. منبع مقادیر بایتها را اضافه می‌کند و داده‌ها و checksum آن را ارسال می‌کند. در پایان دریافت اطلاعات، بایتها را به همان روشی که منبع انجام داده است اضافه کرده و checksum صورت می‌گیرد. سپس گیرنده checksum خود را با بررسی کردن منبع مقایسه می‌کند. اگر مقادیر منطبق باشند، یکپارچگی پیام دست نخورده است. اگر مقادیر مطابقت

نداشته باشند، داده ها باید دوباره ارسال شده یا جایگزین شوند. به checksumها همچنین مجموعه هش نیز گفته می شوند زیرا به طور معمول از توابع هش برای محاسبه استفاده می کنند. یکپارچگی پیام توسط توابع هش و کد تصدیق پیام ارائه شده است.

هش کردن Hashing

. در این بخش، در مورد برخی از معروف ترین توابع هش بحث می کنیم. برخی از این موارد ممکن است دیگر مورد استفاده قرار نگیرند زیرا گزینه های مطمئن تری در دسترس هستند. متخصصان امنیت باید با توابع هش زیر آشنایی داشته باشند:

- هش یک طرفه One-way hash
- MD2 / MD4 / MD5 / MD6
- SHA / SHA-2 / SHA-3
- HAVAL
- RIPEMD-160
- TIGER

• هش یک طرفه One-way hash

یک تابع هش یک پیام با طول متغیر می گیرد و یک مقدار هش با طول ثابت ایجاد می کند. مقادیر Hash، که به آن خلاصه پیام نیز گفته می شود، با استفاده از پیام اصلی محاسبه می شود. اگر گیرنده مقدار هش را محاسبه کند، پیام اصلی دست نخورده می باشد. اگر گیرنده یک مقدار هش را با هم محاسبه کند، پیام اصلی تغییر می کند.

با استفاده از یک تابع H، باید معادله زیر درست باشد تا اطمینان حاصل شود که پیام اصلی M1

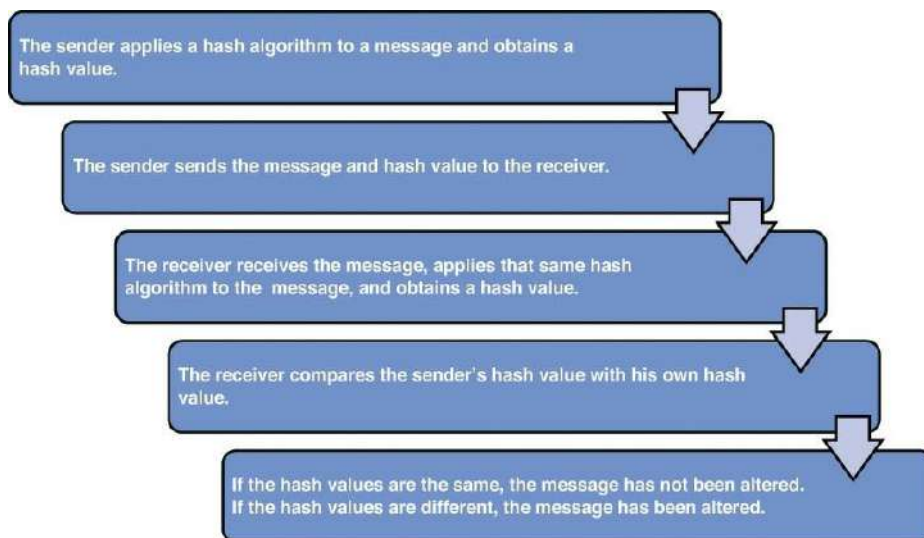
تغییر نکرده است یا با پیام جدید جایگزین نشده است، $M2: H(M1) \neq H(M2)$

برای اینکه یک هش یک طرفه موثر باشد، ایجاد دو پیام متفاوت با همان مقدار هش از نظر ریاضی غیرممکن می باشد. با توجه به مقدار هش، کشف پیام اصلی که مقدار هش از آن بدست آمده از نظر ریاضی غیرممکن می باشد. الگوریتم هش یک طرفه در صورت محافظت در برابر ایجاد همان مقدار هش از پیام های مختلف، بدون تصادم (Collision Free) است.

برخلاف الگوریتم های متقارن و نامتقارن، الگوریتم هشینگ به طور عمومی شناخته شده است. توابع هش همیشه در یک جهت انجام می شوند و استفاده از آن به صورت معکوس ضروری نیست.

با این حال، توابع هش یک طرفه محدودیت هایی دارند. اگر یک مهاجم پیامی را که حاوی مقدار هش است، متوقف کند، مهاجم می تواند پیام اصلی را ایجاد کند تا یک پیام نامعتبر دوم با یک مقدار هش جدید ایجاد کند. اگر مهاجم سپس دومین پیام نامعتبر را برای گیرنده مورد نظر ارسال کند، گیرنده در نظر گرفته شده هیچ راهی برای اطلاع از دریافت پیام نادرست نخواهد داشت. هنگامی که گیرنده محاسبه مقدار هش را انجام می دهد، پیام نامعتبر، به صورت معتبر به نظر می رسد زیرا پیام نامعتبر با مقدار هش جدید مهاجم نه مقدار هش پیام اصلی ضمیمه شده است. برای جلوگیری از بروز این امر، فرستنده باید از کد تأیید اعتبار پیام (احراز هویت) MAC استفاده کند.

رمزگذاری تابع هش با یک الگوریتم کلید متقارن، MAC دارای کلید را ایجاد می کند. کلید متقارن پیام اصلی را رمزگذاری نمی کند، فقط برای محافظت از مقدار هش استفاده می شود. مراحل اساسی یک تابع هش در شکل ۳-۱۹ نشان داده شده است.



شکل ۳-۱۹: فرآیند تابع هش

• MD2 / MD4 / MD5 / MD6

الگوریتم تولیدشده پیام MD2 مقدار هش ۱۲۸ بیتی تولید می کند و ۱۸ دور محاسبات را انجام می دهد. اگرچه MD2 هنوز در حال استفاده است، اما بسیار کندتر از MD4، MD5، MD6 است.

الگوریتم MD4 همچنین یک مقدار هش ۱۲۸ بیتی تولید می‌کند. با این حال، تنها سه دور محاسبات (رایانش) را انجام می‌دهد. اگرچه MD4 سریعتر از MD2 است، اما استفاده از آن به میزان قابل توجهی کاهش یافته است زیرا حملات علیه آن بسیار موفقیت آمیز بوده است. مانند سایر الگوریتم‌های MD، الگوریتم MD5 یک مقدار هش ۱۲۸ بیتی تولید می‌کند و چهار دور محاسبات را انجام می‌دهد. در ابتدا به دلیل مشکلات MD4 ایجاد شده و از MD4 پیچیده تر است. با این حال، MD5 بدون تصادم نیست. به همین دلیل، نباید از آن برای گواهی‌های SSL یا امضاهای دیجیتال استفاده شود. دولت آمریکا به جای MD5 نیاز به استفاده از SHA-2 دارد. با این حال، در کاربرد تجاری، بسیاری از فروشندگان نرم افزار هنگام انتشار پیچ‌های نرم افزار مقدار هش MD5 را منتشر می‌کنند تا مشتریان پس از دانلود بتوانند صحت نرم افزار را تأیید کنند.

الگوریتم MD6 مقدار هش متغیر را تولید می‌کند و یک عدد متغیر محاسباتی را انجام می‌دهد. اگرچه در ابتدا به عنوان کاندید SHA-3 معرفی شد، اما به دلیل مسائل اولیه که الگوریتم با حملات دیفرانسیل داشت (یک حمله کانال جانبی است که شرایط محیطی غیر منتظره مثل دما، ولتاژ، جریان الکتریکی، اورکلاک، میدان‌های الکترومغناطیسی و غیره را به یک عمل رمزنگاری به منظور آشکار کردن وضعیت آن عمل، منتقل می‌کند)، از آن صرف نظر شد. MD6 از زمان انتشار مجدد با این مسئله مستقر شده است. با این حال، این نسخه خیلی دیر بود که به عنوان استاندارد NIST SHA-3 پذیرفته شود.

• SHA / SHA-2 / SHA-3

Secure Hash Algorithm (SHA) خانواده‌ای از چهار الگوریتم است که توسط NIST منتشر شد. SHA-0، در ابتدا به عنوان SHA ساده گفته می‌شد زیرا هیچ "اعضای خانواده دیگری" نداشت، پس از انجام ۸۰ دور محاسبات (رایانش) در بلوک‌های ۵۱۲ بیتی، یک مقدار هش ۱۶۰ بیتی تولید می‌کند، SHA-0 هرگز بسیار محبوب نبود زیرا تصادم‌هایی در آن کشف شد. مانند SHA-0، SHA-1 بعد از انجام ۸۰ دور محاسبات در بلوک ۵۱۲ بیتی، مقدار هش ۱۶۰ بیتی تولید می‌کند. SHA-1 شکاف موجود در SHA-0 را اصلاح کرده که این امر مستعد حملات شد.

SHA-2 در واقع خانواده‌ای از توابع هش است که هر یک از آنها محدودیت‌های عملکردی متفاوتی را ارائه می‌دهند. خانواده SHA-2 به شرح زیر است:

SHA-224 بعد از انجام ۶۴ دور محاسبات در بلوک ۵۱۲ بیتی مقدار هش ۲۲۴ بیتی تولید می‌کند.

SHA-256 بعد از انجام ۶۴ دور محاسبات در بلوک ۵۱۲ بیتی مقدار هش ۲۵۶ بیتی تولید می‌کند.

SHA-384 بعد از انجام ۸۰ دور محاسبات در ۱۰۲۴ بیتی، مقدار هش ۳۸۴ بیتی تولید می‌کند.

SHA-512 بعد از انجام ۸۰ دور محاسبات در ۱۰۲۴ بیتی، مقدار هش ۵۱۲ بیتی تولید می‌کند.

SHA-512/224 بعد از انجام ۸۰ دور محاسبات در بلوک‌های ۱۰۲۴ بیتی، مقدار هش ۲۲۴ بیتی تولید می‌کند. تعیین ۵۱۲ در اینجا اندازه وضعیت داخلی را نشان می‌دهد.

SHA-512/256 بعد از انجام ۸۰ دور محاسبات در بلوک‌های ۱۰۲۴ بیتی، مقدار هش ۲۵۶ بیتی تولید می‌کند. بار دیگر، تعیین ۵۱۲ اندازه وضعیت داخلی را نشان می‌دهد.

SHA-3، مانند **SHA-2**، خانواده‌ای از توابع هش خواهد بود. **SHA-2** تاکنون شکست نخورده است. اندازه مقدار هش برای **SHA-3** از ۲۲۴ تا ۵۱۲ بیت است. اندازه بلوک از ۱-۵۷۶، ۱۵۲ است. **SHA-3** بطور پیش فرض ۱۲۰ دور محاسبات را انجام می‌دهد.

به خاطر داشته باشید که **SHA-1** و **SHA-2** امروزه هنوز هم در بسیاری موارد به کار گرفته می‌شود. **SHA-3** به دلیل برخی نقص امنیتی با دو استاندارد قبلی توسعه نیافت، اما در عوض به عنوان یک تابع هش جایگزین برای سایرین پیشنهاد شده است.

• HAVAL

یک تابع یک طرفه است که مقادیر هش با طول متغیر، از جمله ۱۲۸ بیت، ۱۶۰ بیت، ۱۹۲ بیت، ۲۲۴ بیت و ۲۵۶ بیت تولید می‌کند و از بلوک‌های ۱۰۲۴ بیتی استفاده می‌کند. تعداد دور محاسبات می‌تواند ۳، ۴ یا ۵ باشد. در صورت تولید یک مقدار هش ۱۲۸ بیتی با سه دور محاسبه، مشکلات تصادم (Collision) کشف می‌شود. در مورد سایر چاپ‌ها، هیچ گونه موضوعات کشف شده‌ای وجود ندارد.

• RIPEMD-160

اگرچه چندین تغییر در تابع هش **RIPEMD** وجود دارد. **RIPEMD-160** بعد از انجام ۱۶۰ دور محاسبه در بلوک ۵۱۲ بیتی، مقدار هش ۱۶۰ بیتی را تولید می‌کند.

• Tiger

یک تابع هش است که پس از انجام ۲۴ دور محاسبات در بلوک ۵۱۲ بیتی، مقادیر هش ۱۲۸، ۱۶۰ یا ۱۹۲ بیتی تولید می کند، که رایج ترین نسخه آن تولید مقادیر هش ۱۹۲ بیتی است. برخلاف (MD5، SHA-0، SHA-1، RIPEMD)، Tiger بر اساس معماری MD4 ساخته نشده است.

کد تصدیق پیام Message Authentication Code

در این بخش، در مورد سه نوع MAC بحث می کنیم که متخصصان امنیت باید با آنها آشنا باشند:

- HMAC

- CBC-MAC CMAC

- HMAC

HMAC ✓

هش (HMAC) MAC یک MAC دارای کلید است که شامل یک تابع هش با کلید متقارن است. HMAC یکپارچگی و تصدیق داده را ارائه می دهد. هر یک از توابع هش که قبلاً ذکر شده است می تواند با HMAC استفاده شود، نام HMAC همراه با نام تابع هش، مانند HMACSHA-1.

توانایی HMAC به قدرت تابع هش که شامل مقدار هش و اندازه کلید است، بستگی دارد. اندازه خروجی مقدار هش HMAC همان تابع هش اساسی است. HMAC می تواند به کاهش میزان تصادم تابع هش کمک کند.

مراحل اساسی یک فرآیند HMAC به شرح زیر است:

- ۱- فرستنده و گیرنده در مورد کدام کلید متقارن برای استفاده توافق دارند.
- ۲- فرستنده کلید متقارن را به پیام اضافه می کند.
- ۳- فرستنده الگوریتم هش را در پیام به کار برده و مقدار هش را بدست می آورد.
- ۴- فرستنده یک مقدار هش به پیام اصلی اضافه می کند و پیام جدید تولید شده را به گیرنده ارسال می کند.
- ۵- گیرنده پیام را دریافت کرده و کلید متقارن را به پیام متصل می کند.
- ۶- گیرنده الگوریتم هش را در پیام به کار برده و مقدار هش را بدست می آورد.

۷- اگر مقادیر هش یکسان باشند، پیام تغییر نمی‌کند. اگر مقادیر هش متفاوت باشد، پیام تغییر یافته است.

✓ CBC-MAC (Cipher Block Chaining MAC)

رمزگذاری زنجیره بلوک MAC نوعی رمزگذاری می‌باشد که در حالت CBC عمل می‌کند. CBC-MAC یکپارچگی و تصدیق داده را فراهم می‌کند.

مراحل اساسی یک فرآیند CBC-MAC به شرح زیر است:

۱- فرستنده و گیرنده توافق می‌کنند که از کد رمزگذاری شده بلوک متقارن استفاده کنند.

۲- فرستنده پیام را با بلوک متقارن در حالت رمزگذاری CBC رمزگذاری می‌کند. آخرین بلوک MAC است.

۳- فرستنده MAC را به پیام اصلی اضافه می‌کند، و فرستنده پیام جدید را به گیرنده ارسال می‌کند.

۴- گیرنده پیام را دریافت کرده و پیام را با بلوک متقارن در حالت رمزگذاری CBC رمزگذاری می‌کند.

۵- گیرنده MAC را بدست می‌آورد و آن را با MAC فرستنده مقایسه می‌کند.

۶- اگر مقادیر یکسان باشند، پیام تغییر نمی‌کند. اگر مقادیر متفاوت باشند، پیام تغییر می‌کند.

✓ CMAC

مبتنی بر رمزگذاری MAC (CMAC) به همان روش CBC-MAC عمل می‌کند اما توابع ریاضی بسیار بهتری دارد. CMAC با CBC-MAC به برخی از مسائل امنیتی می‌پردازد و برای همکاری با AES و 3DES تأیید شده است.

Salting

جداول جستجو و جداول رنگین کمان اینگونه کار می‌کنند زیرا هر گذرواژه دقیقاً به همان روش هش شده است. اگر دو کاربر گذرواژه یکسانی داشته باشند، گذرواژه آنها یکسان است. برای جلوگیری از حمله، متخصصان امنیت باید مطمئن شود که هر هشی به صورت تصادفی است. سپس، هنگامی که همان گذرواژه دو بار هش شده است، هش‌ها یکسان نمی‌باشند.

Salting به معنای اضافه کردن تصادفی داده به صورت تابع یک طرفه است که گذرواژه یا عبارت عبور را هش می‌کند. وظیفه اصلی Salting، دفاع در برابر حملات فرهنگ لغت در مقابل لیستی از هشهای گذرواژه و بر ضد حملات پیشگیرانه جدول رنگین کمان است. یک متخصص امنیت باید هش‌ها را با ضمیمه کردن یا آماده کردن به صورت یک رشته تصادفی به نام Salt قبل از هش کردن گذرواژه، تصادفی کند.

برای بررسی صحت یک گذرواژه، مهاجم به Salt نیاز دارد. Salt معمولاً در پایگاه داده حساب کاربر به همراه هش یا به عنوان بخشی از رشته هش خود ذخیره می‌شود. مهاجم از قبل نمی‌داند Salt چه خواهد بود، بنابراین نمی‌تواند جدول جستجوی یا جدول رنگین کمانی را تسخیر کند. اگر گذرواژه هر کاربر با Salt متفاوت علامت زده شود، حمله از نوع جدول معکوس صورت نمی‌گیرد.

در صورت استفاده از Salt، متخصصان امنیت باید از عدم استفاده مجدد و استفاده کوتاه مطمئن شوند. هر بار که ادمین یک حساب کاربری ایجاد کند یا کاربر گذرواژه خود را تغییر دهد، باید یک Salt تصادفی جدید ایجاد شود. یک قانون مناسب برای استفاده از Salt به اندازه خروجی تابع هش است. به عنوان مثال، خروجی SHA-256، ۲۵۶ بیت (۳۲ بایت) است، بنابراین Salt باید حداقل ۳۲ بایت تصادفی باشد.

Salt‌ها باید با استفاده از یک مولد عدد شبه تصادفی رمزنگاری امن تولید شوند (CSPRNG). همانطور که از نام این محصول پیداست، یک CSPRNG برای فراهم کردن سطح بالایی از تصادف طراحی شده است و کاملاً غیرقابل پیش بینی است.

حملات تجزیه و تحلیل رمزنگاری Cryptanalytic Attacks

حملات تجزیه و تحلیل رمزنگاری به حملات منفعل و فعال طبقه بندی می‌شوند. یک حمله منفعل معمولاً فقط برای کشف اطلاعات انجام می‌شود و تشخیص آن بسیار سخت تر است زیرا معمولاً با استراق سمع یا sniffing بسته انجام می‌شود. حملات فعال شامل یک مهاجم است که در واقع اقدام به انجام مراحل، مانند تغییر پیام یا تغییر فایل می‌کند. رمزنگاری معمولاً از طریق کلید، الگوریتم، اجرا، داده یا افراد مورد حمله قرار می‌گیرد. اما بیشتر این حملات در تلاشند تا کلید مورد استفاده را کشف کنند.

حملات تجزیه و تحلیل رمزنگاری که مورد بحث قرار می‌گیرند شامل موارد زیر است:

✓ حمله متن رمزگذاری شده Cipher text-only attack

- ✓ Known plaintext attack حمله متن ساده شناخته شده
- ✓ Chosen plaintext attack حمله متن ساده منتخب
- ✓ Chosen cipher text attack حمله به متن رمزگذاری شده منتخب
- ✓ Social engineering مهندسی اجتماعی
- ✓ Brute force نیروی بیرحمانه
- ✓ Differential cryptanalysis دیفرانسیل تحلیل رمزنگاری
- ✓ Linear cryptanalysis رمزنگاری خطی
- ✓ Algebraic attack حمله جبری
- ✓ Frequency analysis تجزیه و تحلیل فرکانس
- ✓ Birthday attack حمله تولد
- ✓ Dictionary attack حمله فرهنگ لغت
- ✓ Replay attack حمله مجدد
- ✓ Analytic attack حمله تحلیلی
- ✓ Statistical attack حمله آماری
- ✓ Factoring attack حمله فاکتورگیری
- ✓ Reverse Engineering مهندسی معکوس
- ✓ Meet-in-the-Middle حمله

• حمله متن رمزگذاری شده CIPHER text-only attack

یک مهاجم از چندین پیام رمزگذاری شده (متن رمزگذاری شده Ciphertext) برای مشخص کردن کلید بکاربرده شده در فرایند رمزگذاری استفاده می‌کند. اگرچه این نوع حمله بسیار رایج است، اما معمولاً موفقیت آمیز نیست، زیرا در مورد رمزگذاری بکاربرده شده اطلاعات کمی وجود دارد.

• حمله متن ساده شناخته شده Known plaintext attack

در حمله متن ساده شناخته شده، یک مهاجم از نسخه‌های متن ساده و متن رمزگذاری شده یک پیام برای کشف کلید استفاده می‌کند. این نوع حمله مهندسی معکوس، تجزیه و تحلیل فرکانس

یا نیروی بی رحمانه Brute Force را برای تعیین کلید پیاده سازی می کند تا همه پیام ها رمزگشایی شوند.

• حمله متن ساده منتخب Chosen plaintext attack

در یک حمله متن ساده، یک مهاجم متن ساده ای را برای رمزگذاری برای انتخاب متن رمزگذاری شده انتخاب می کند. مهاجم با ارسال پیام به انتظار اینکه کاربر آن پیام را به صورت متن رمزگذاری شده به کاربر دیگری می فرستد، ارسال می کند. مهاجم نسخه متن رمزگذاری شده پیام را ضبط می کند و سعی می کند با مقایسه نسخه متن ساده که در ابتدا با نسخه متن رمزگذاری شده گرفته شده، کلید را تعیین کند. بار دیگر، کشف اصلی هدف این حمله است.

• حمله متن رمزگذاری شده منتخب Chosen cipher text attack

یک حمله متن رمزگذاری شده برعکس یک حمله به متن ساده انتخاب شده است. در یک حمله متن رمزگذاری شده، یک مهاجم متن رمزگذاری شده را رمزگذاری می کند تا متن ساده را بدست آورد. این حمله دشوارتر است زیرا کنترل سیستمی که الگوریتم را اجرا می کند لازم است.

• مهندسی اجتماعی Social Engineering

حملات مهندسی اجتماعی علیه الگوریتم های رمزنگاری شده تفاوت چندانی با حملات مهندسی اجتماعی بر ضد هر حوزه امنیتی دیگر ندارد. مهاجمان سعی می کنند کاربران را برای دادن کلید رمزنگاری مورد استفاده، فریب دهند. روش های معمول مهندسی اجتماعی شامل ترس، به دام انداختن یا انگیزه (Intimidation, Enticement, Inducement) است.

• نیروی بیرحمانه Brute force

به عنوان مثال حمله بی رحمانه به گذرواژه ها، یک حمله بی رحمانه برضد الگوریتم رمزنگاری، از کلیه کلیدهای ممکن استفاده می کند تا زمانی که یک کلید کشف شود که متن رمزگذاری شده را با موفقیت رمزگشایی کند. این حمله به زمان و قدرت پردازشی زیادی نیاز دارد و انجام آن بسیار دشوار است.

• دیفرانسیل تحلیل رمزنگاری Differential cryptanalysis

همچنین به عنوان یک حمله کانال جانبی Side-Channel Attack نیز گفته می‌شود، زمان اجرا و قدرت مورد نیاز دستگاه رمزنگاری را اندازه گیری می‌کند. اندازه گیری‌ها به کلید و الگوریتم بکاربرده شده کمک می‌کنند.

• رمزنگاری خطی Linear Cryptanalysis

رمزنگاری خطی یک حمله ساده شناخته شده است که از تخمین خطی استفاده می‌کند، که رفتار بلوک رمزگذاری را توصیف می‌کند. مهاجم با دستیابی به پیام‌های متن ساده و متناسب با این نوع حمله، موفق تر عمل می‌کند.

• حمله جبری Algebraic Attack

حملات جبری وابسته به جبر است که توسط الگوریتم‌های رمزنگاری استفاده می‌شود. اگر یک مهاجم از آسیب پذیریهایی شناخته شده جبر سوء استفاده کند، به دنبال آن آسیب پذیری می‌تواند به مهاجم کمک کند تا کلید و الگوریتم مورد استفاده را تعیین کند.

• تجزیه و تحلیل فرکانس Frequency Analysis

این حمله به این واقعیت متکی می‌باشد که رمزهای جایگزینی و جابجایی منجر به ایجاد الگوهای مکرر در متن رمزگذاری شده می‌شوند. شناخت الگوهای هشت بیت و شمارش آنها می‌تواند به مهاجمان اجازه دهد از جایگزینی معکوس برای بدست آوردن پیام متن ساده استفاده کنند. تجزیه و تحلیل فرکانس معمولاً شامل ساخت نمودار است که تمام حروف الفبا را در کنار تعداد دفعاتی که حرف رخ می‌دهد، لیست می‌کند. بنابراین اگر حرف Q در لیست‌های تکرار بالاترین مقدار را داشته باشد، احتمال خوبی وجود دارد که این حرف در واقع پیام E باشد زیرا E در زبان انگلیسی پرکاربردترین حرف است. حرف متن رمزگذاری شده، در متن رمزگذاری شده با حرف متن ساده جایگزین شده است.

الگوریتم‌های امروزه بسیار پیچیده تر در نظر گرفته می‌شوند که مستعد این چنین نوع حمله‌ای نباشند.

• **حمله روز تولد Birthday**

حمله روز تولد از این پیش فرض استفاده می کند که پیدا کردن دو پیام که منجر به یک مقدار هش یکسان باشند، آسانتر از تطابق با یک پیام و مقدار هش آن است. اکثر الگوریتم های هش می توانند در مقابل حملات ساده Birthday مقاومت کنند.

• **حمله فرهنگ لغت Dictionary Attack**

شبیه به یک حمله نیروی بیرحمانه Brute force است، یک حمله فرهنگ لغت از تمام کلمات موجود در یک فرهنگ لغت استفاده می کند تا زمانی که یک کلید کشف شود که متن رمزگذاری شده را با موفقیت رمزگشایی کند. این حمله به زمان و قدرت پردازش زیادی نیاز دارد و انجام آن بسیار دشوار است و همچنین به یک فرهنگ لغت جامع از کلمات نیاز دارد.

• **حمله مجدد Replay Attack**

در حمله مجدد، یک مهاجم در تلاش برای فریب دستگاه دریافت کننده، همان داده ها را بارها و بارها ارسال می کند. این داده ها معمولاً اطلاعات احراز هویت هستند. بهترین اقدامات متقابل در برابر این نوع حمله، نشانگرهای زمانی و دنباله اعداد هستند.

• **حمله تحلیلی Analytic Attack**

در حملات تحلیلی، مهاجمان برای تعیین الگوریتم مورد استفاده از نقاط ضعف یا نقص ساختاری شناخته شده استفاده می کنند. اگر بتوان از یک ضعف یا نقص خاص بهره برداری کرد، احتمالاً الگوریتم خاصی مورد استفاده قرار می گیرد.

• **حمله آماری Statistical Attack**

در حالی که حملات تحلیلی به دنبال نقاط ضعف یا نقص ساختاری هستند، حملات آماری از نقاط ضعف آماری شناخته شده یک الگوریتم برای کمک به حمله استفاده می کنند.

• **حمله فاکتورگیری Factoring Attack**

با استفاده از راه حل های فاکتورگیری تعداد زیاد صورت می گیرد، یک حمله فاکتورگیری علیه الگوریتم RSA انجام می شود.

• مهندسی معکوس Reverse Engineering

یکی از رایج ترین حملات رمزنگاری است، مهندسی معکوس زمانی اتفاق می افتد که یک مهاجم کالای رمزنگاری شده خاصی را به منظور تلاش برای مهندسی معکوس محصول برای کشف اطلاعات محرمانه در مورد الگوریتم رمزنگاری بکار گرفته شده، خریداری کند.

• حمله Meet-in-the-Middle Attack

یک مهاجم سعی می کند الگوریتم را بشکند بوسیله رمزگذاری از انتها و رمزگشایی از سمت دیگر، برای اینکه مساله ریاضی بکار برده شده راتعیین کند.

تهدیدات جغرافیایی Geographical Threats

بسیاری از تهدیدها تابعی از موقعیت جغرافیایی تاسیسات یا مرکز است. در این بخش طیف گسترده ای از تهدیدها و موضوعات مورد بحث قرار می گیرد که برخی از این موارد فقط در مناطق خاص اعمال می شود. متخصص امنیت باید برای پیش بینی و کاهش این موارد آمادگی داشته باشد.

تهدیدات داخلی در مقابل تهدیدات خارجی Internal Versus External Threats

وقتی صحبت از تهدیدهای مربوط به امنیت فیزیکی دارایی ها می شود، می توانیم بحث را با تهدیدهایی که از خارج از سازمان و آنهایی که از درون سازمان به وجود می آیند، تنظیم کنیم. بسیاری از تکنیک های کاهش میزان بحث در بخش های بعدی به منظور حفظ امنیت محیط و یا دسترسی به ساختمان یا اتاق طراحی شده اند، در حالی که سایر تکنیک ها برای مقابله با تهدیدات کسانی که ممکن است دسترسی به اتاق یا ساختمان داشته باشند طراحی شده است. به عنوان مثال، حصار برقی اطراف تاسیسات به منظور جلوگیری از دسترسی به ساختمان توسط کسانی که نباید دسترسی داشته باشند (تهدید خارجی) طراحی شده است، در حالی که یک سیستم قفل درب در اتاق سرور که نیاز به کشیدن کارت کارمند دارد، طراحی شده برای جلوگیری از دسترسی کسانی که در حال حاضر در ساختمان هستند (تهدید داخلی).

تهدیدهای طبیعی Natural Threats

بسیاری از تهدیدات فیزیکی که باید مورد توجه قرار بگیرند، ناشی از نیروهای طبیعت است. ایجاد همه تأسیسات برای مقاومت در برابر شدیدترین طوفان ها، گردبادها و زمین لرزه ها از نظر اقتصادی مقرون به صرفه نیست زیرا در بسیاری از مناطق این رخدادهای به ندرت اتفاق می افتد. آنچه می توان انجام داد این است که یک ارزیابی واقع بینانه از شرایط آب و هوایی تاریخی یک منطقه و انجام یک هزینه محتاطانه و سودمندانه انجام شود تا مشخص شود کدام تهدیدات باید برطرف شود و کدام یک باید پذیرفته شود. در این بخش برخی از تهدیدات اصلی طبیعی مورد بحث قرار گرفته است.

طوفان / طوفان گرمسیری Hurricanes/Tropical Storms

در مناطقی خاص، طوفان ها و طوفان های گرمسیری آنقدر مکرر و غیرقابل پیش بینی هستند که تمام ساختمان ها را ملزم به تحمل نمونه های مناسب تر درمقابل این طوفان ها می کند. در مناطق دیگر، انجام این کار معنا ندارد اگرچه این طوفان ها هر از گاهی اتفاق می افتند. محل تأسیسات باید بیان کند که چه مقدار هزینه در کاهش خسارت های احتمالی این وقایع شده است.

گردبادها Tornadoes

اگرچه به نظر می رسد وقایع چند سال گذشته با این موضوع متناقض است، اما در مسافت های طولانی مناطق خاصی نسبت به سایر مناطق مستعد گردبادها هستند. مطالعه میزان و شدت گردبادها در یک منطقه از منظر تاریخی می تواند به تعیین معیارهای منطقی برای یک مکان خاص کمک کند.

توجه داشته باشید

در شیوع گردبادهای اخیر، بسیاری از برج های تلفن همراه کاملاً از کار افتاده اند. به ویژه در مناطق روستایی، برقراری ارتباط با عزیزان می تواند غیرممکن باشد. اما این مشکل نه تنها در مناطق روستایی رخ می دهد. در گردباد دالاس - فورت ورت در دسامبر سال ۲۰۱۵، افراد زیادی برای یافتن عزیزانشان به دلیل کمبود ارتباطات به مدت ۴۸ ساعت به طول انجامید. می توانید تصور کنید که این از دست دادن ارتباطات چگونه می تواند بر یک شرکت، مدرسه یا بیمارستان تأثیر بگذارد.

زلزله‌ها Earthquakes

در زلزله‌ها باید همانند طوفان‌ها، طوفان‌های گرمسیری و گردبادها رفتار شود. یعنی مکان تأسیسات خاص باید میزان آماده‌سازی و اقدامات لازم برای مقابله با این ریسک را نشان دهد. به عنوان مثال، تاسیساتی که در کالیفرنیا قرار دارد ممکن است بیشتر از حوادثی در جنوب شرقی ایالات متحده که این رویدادها بسیار نادر هستند، به این موضوع توجه کنند.

سیل Floods

همیشه باید سیل در نظر گرفته شود زیرا این یک رخداد است که می‌تواند با شرایط مناسب تقریباً در هر نقطه رخ دهد. در صورت امکان، سیستم‌های رایانه‌ای و تجهیزات را از روی زمین دور نگه داشته و اتاق‌های سرور و سیم‌کشی را در طبقه‌های مرتفع بنا کنید تا از آسیب‌هایی که حتی در یک سیل کوچک رخ می‌دهد، جلوگیری شود.

تهدیدات سیستم System Threats

برخی از تهدیداتی که وجود دارد ناشی از نیروهای طبیعی نیست بلکه از کار افتادن سیستم‌هایی است که خدمات اساسی مانند آب و برق را ارائه می‌دهند. اگرچه این مشکلات گاهی اوقات می‌تواند ناشی از حوادث طبیعت باشد، در این بخش دستورالعمل‌های تهیه و مقابله با این رخدادها را مورد بحث قرار می‌دهیم که می‌تواند در هر مکان و در هر نوع شرایط آب و هوایی رخ دهد.

برق Electrical

برق، حیات سازمان و به ویژه در رابطه با سیستم‌های محاسباتی است. خاموشی‌ها نه تنها یک دغدغه هستند بلکه می‌توانند به تجهیزات آسیب رسانده و باعث از بین رفتن داده‌ها شوند. علاوه بر این، وقتی این اتصالات وصل می‌شود، تا حدود زیادی شرکتها در جهان امروز متوقف می‌شوند. به همین دلیل، کلیه سیستم‌های مهم برای مأموریت باید دارای منبع تغذیه بدون وقفه (UPS) باشند که می‌توانند برق را به صورت کوتاه مدت تأمین کنند تا اینکه سیستم به طور کامل خاموش شود. در مواردی که برق باید بیش از چند دقیقه ادامه داشته باشد، ژنراتورهای موجود در محل را در اختیار قرار دهند تا بتوانند سیستم‌ها برای مدت طولانی‌تری کار کنند تا برق (الکتریسته) مجدداً راه اندازی شود.

همچنین سر و صدا، رطوبت، و خاموشی نیز از جمله مواردی است که در تأمین برق (الکتریسته) تأثیر می گذارد. دامنه رطوبت نسبی بهینه توصیه شده برای فعالیت با رایانه ۴۰٪ تا ۶۰٪ است. سیستم های بحرانی باید از شدت فشار و قدرت محافظت شوند، همچنین برای تجهیزات مناسب نیستند. دستگاه های تهویه که بین سیستم و منبع تغذیه قرار گرفته اند می توانند حتی به خارج از این نوسانات کمک کرده و از آسیب دیدن جلوگیری کنند.

سرانجام، شایع ترین علت آتش سوزی در مرکز رایانه ها سیستم های توزیع برق است. بررسی این سیستم ها بطور مرتب می تواند مشکلات را قبل از بروز آنها شناسایی کند.

ارتباطات Communications

محافظت از امنیت فیزیکی ارتباطات مانند ایمیل، تلفن، و سیستم های فکس، موضوعی است که مانع از دسترسی غیرمجاز به خطوط ارتباطات فیزیکی (کابل ها و غیره) و دسترسی فیزیکی و منطقی به تجهیزات مورد استفاده برای مدیریت این سیستم ها می شود.

به عنوان مثال، در مورد ایمیل، سرورهای ایمیل را باید قفل کرد و دسترسی به آنها از طریق شبکه باید با نام کاربری و گذرواژه های پیچیده کنترل شود.

در مورد دستگاه های فکس، پیاده سازی سیاست ها و رویه ها می تواند از دسترسی فکسهای حساس برای افراد غیر مجاز جلوگیری کند. در بعضی موارد، جلوگیری از انتقال برخی از اطلاعات با فکس ممکن است لازم باشد.

اکنون بسیاری از سیستم های تلفنی با استفاده از Voice over IP (VoIP) در شبکه داده ادغام شده اند. با استفاده از این سیستم ها، ممکن است روترها و سوئیچ ها در مدیریت سیستم تلفن درگیر شوند، باید از نظر فیزیکی قفل شده و از نظر منطقی دسترسی به شبکه به همان روشی که سرورهای ایمیل محافظت می شوند، حفاظت کرد. از آنجا که ایمیل و VoIP هر دو از شبکه داده استفاده می کنند، مطمئن شوید که کابل کشی در معرض دستکاری و تخریب قرار نمی گیرد.

برخی ملاحظات اضافی که می تواند بر بهبود فاجعه تأثیر بگذارد عبارتند از:

- اتصالات تحمل خطا به اینترنت مانند T1 را به عنوان اتصال اصلی و یک شماره گیری پشتیبان یا اتصال ماهواره ای را حفظ کنید.
- علاوه بر اتصالات تلفنی سازمان اصلی، ارتباطات تلفنی با کارمندان برقرار کنید. شماره تلفن و شماره خانه کارمندان را برای اطلاع رسانی شناسایی کنید.

- اتصالات رادیویی را در کل دانشگاه با Repeaterها برقرار کنید تا بتوانید در مواقع اضطراری ارتباط برقرار کنید. بسیاری از ارتباطات (مانند خطوط تلفن و تلفن‌های همراه) می‌توانند قطع شوند.

خدمات رفاهی Utilities

برخی از سیستم رفاهی، مانند آب و گاز می‌توانند از طریق مجاری و تونل‌هایی که ممکن است یک نقطه ورود غیر مجاز به ساختمان باشد، وارد تاسیسات شوند. چنین مجاری و تونل‌هایی که این فرصت را ارائه می‌دهند باید با سنسورها و مکانیسم‌های کنترل دسترسی، نظارت شوند. هر بخش مهمی از سیستم‌هایی که شیرهای برش خورده (والو) و سیستم خاموش شدن اضطراری در آن قرار دارند باید از نظر فیزیکی در برابر دستکاری‌های مخرب محافظت شوند. در بعضی موارد پوشاندن و محافظت از این شیرهای برش خورده (والو) و کنترل‌ها با استفاده از قفل ممکن است مفید باشد.

تهدیدات ناشی از انسان Human-Caused Threats

اگرچه بسیاری از تهدیدات فیزیکی که با آنها روبرو هستیم تابعی از وقایع طبیعی و اتفاقات تصادفی است، اما برخی از آنها هدفمند هستند. در این بخش برخی از تهدیدهای فیزیکی که توسط انسانهای بدخواه و بی دقت با آنها روبرو می‌شویم، مورد بررسی قرار گرفته است. این تهدیدها هم از نیروهای خارجی و هم نیروهای داخلی هستند.

✓ انفجارها Explosions

انفجارها می‌توانند هم عمدی و هم اتفاقی باشند. انفجارهای عمدی می‌تواند در اثر انگیزه‌های سیاسی رخ دهد و یا می‌تواند به طور ساده با عث خرابکاری شوند. انفجارهای تصادفی می‌تواند نتیجه عدم پیروی از رویه‌ها و عدم موفقیت اجزای فیزیکی باشند.

با توجه به انفجارهای عمدی، بهترین دفاع جلوگیری از دسترسی به مناطقی است که انفجارها می‌توانند صدمات قابل توجهی به اجزای عملیاتی سازمان مانند اتاق سرور، کمد سیم کشی و مناطقی که الکتریسیته و آب و برق در ساختمان وارد کنند. هنگامی که یک انفجار عمدی رخ داد، به طور معمول تصور می‌شود محل انفجار در جایی که بیشترین صدمه را دیده است، ایجاد شده است، بنابراین آن مناطق باید از حفاظت فیزیکی اضافی برخوردار باشد.

✓ آتش سوزی Fire

آتش سوزی می تواند در هر نقطه اتفاق بیفتد بنابراین همیشه مورد توجه قرار دارد. بعداً در این فصل، در مورد هر دو روش مهار آتش و روش های شناسایی آتش بحث می کنیم. تهدید آتش سوزی را در زمینه های تصادف و یک حمله عمدی می توان خطاب کرد. زنگ ایستگاه کمکی ممکن است در بسیاری موارد مفید باشد. این مکانیسم به طور خودکار باعث می شود تا زنگ خطر در مرکز داده منتقل شده و از طریق مدارهای مربوط به آتش نشانی محلی یا هشدار پلیس محلی برای انتقال به پلیس یا ایستگاه آتش نشانی محلی و ستادهای مناسب منتقل شود. مهار کننده های آتش با استفاده از سیستم استاندارد طبقه بندی شده در جدول ۳-۸ طبقه بندی می شوند. بعداً در این فصل، بیشتر در مورد مهار کننده های آتش و سیستم های سرکوب برای انواع مختلف بحث می کنیم.

Class	Type of Fire
Class A	Ordinary combustibles
Class B	Flammable liquids, flammable gases
Class C	Electrical equipment
Class D	Combustible metals
Class K	Cooking oil or fat

جدول ۳-۸: کلاس های مهار کننده آتش

با توجه به مصالح ساختمانی، طبق 2 ^ (ISC)، در یک مرکز پردازش اطلاعات کلیه دیوارها باید دارای توانمندی در مقابل حداقل دو ساعت آتش سوزی باشند. دانستن اینکه شایع ترین علت آتش سوزی در مرکز رایانه سیستم های توزیع برق است. صرف نظر از منبع آتش سوزی، اولین عملی که در صورت وقوع آتش سوزی انجام می شود، تخلیه کلیه پرسنل است.

✓ خرابکاری Vandalism

خرابکاری در بیشتر موارد باعث از بین رفتن دیوارها، حمام ها و مواردی از این دست می شود، اما در صورت دسترسی به اجزای مهم، می تواند عملیات را تحت تأثیر قرار دهد. کابل های بریده شده و دستگاه های شکسته شده از دلایل تأکید بر جلوگیری از دسترسی فیزیکی به این اجزاء هستند.

حتی وقتی همه اقدامات انجام شده باشد، خرابکاری هنوز هم می‌تواند مشکلاتی را ایجاد کند. به عنوان مثال، یک سرویس بهداشتی وصل شده می‌تواند در صورت عدم رعایت، کف را آب گرفته و به تجهیزات آسیب برساند.

✓ تقلب، کلاهبرداری Fraud

در زمینه امنیت فیزیکی، کلاهبرداری شامل دستیابی به سیستم‌ها، تجهیزات و یا تاسیسات از طریق فریب دادن است. به عنوان مثال، فردی که به عنوان یک مستخدم یا شخصی که از طریق سیستم کارت یک کارمند، وارد تسهیلات می‌شود، دسترسی فیزیکی از نوع کلاهبرداری محسوب می‌شود. سیستم‌های کنترل دسترسی فیزیکی برای جلوگیری از این نوع کلاهبرداری و خسارات ناشی از آن بسیار مهم هستند.

✓ سرقت Theft

جلوگیری از سرقت فیزیکی دارایی شرکت بستگی به جلوگیری از دسترسی فیزیکی به تاسیسات دارد. سرقت فیزیکی ریسکی است که به احتمال زیاد روی CIA تأثیر می‌گذارد. برای داراییهایی که از تاسیسات خارج می‌شوند، مانند لپ‌تاپ، ممکن است داده‌های حساس که رمزگذاری شده است بر روی آنها باشد، برای حفاظت از داده‌ها ترجیحاً از درایوهای رمزگذاری شده استفاده شود.

✓ تبانی Collusion

تبانی زمانی اتفاق می‌افتد که دو کارمند برای دستیابی به سرقت به نوعی همکاری می‌کنند که بدون دانش یا مسئولیت‌های ترکیبی آنها انجام نمی‌شود. از تفکیک مناسب وظایف استفاده شود، تا از یک فرد که به اندازه کافی یک فرآیند را کنترل می‌کند و اقدامات خود را پنهان می‌کند، جلوگیری شود.

محدود کردن دسترسی‌های خاص کارکنان، یک اپراتور را مجبور به تبانی با اپراتور دسته دیگری می‌کند تا به داده‌های غیرمجاز دسترسی داشته باشند. از نظر آماری برای یک نفر که به تنهایی کار می‌کند تبانی بسیار کم اتفاق می‌افتد. وقتی این واقعیت را در نظر می‌گیرید که معاوضه در تبادل یک خطر برای یکدیگر بوده، توجیه پذیر است.

✓ تهدیدها با انگیزه سیاسی Politically Motivated Threats

ممکن است به نظر برسد بعضی مواقع بسیاری از تهدیدها با انگیزه بیشتر سیاسی بوجود آمده است. شرکت معمولاً به طور ناخواسته به این مسئله کمک کرده، و وارد این تقابل ها شده است. این تهدیدات می تواند از نظر بهره وری از دست رفته، از بین رفتن دارایی های شرکت و حتی خطر فیزیکی برای کارمندان و افسران شرکت هزینه بر باشد. در این بخش برخی از اصلی ترین راه هایی که این تهدیدات در نظر گرفته شده است، و می توانند با یکسری اقدامات انجام شده باعث کاهش ریسک موجود در آنها شود، می پردازیم.

۱- اعتصاب Strikes

اگرچه اعتصابها ممکن است کمترین خطر از تهدیدهای موجود در این لیست باشند، اما هنوز هم می توانند به بنگاه اقتصادی آسیب وارد کنند. در کشورهایی مانند ایالات متحده، مقررات اساسی منظم ایجاد شده است که از بدتر شدن نتایج احتمالی جلوگیری می کند، اما حتی در این صورت هم اعتصاب منظم می تواند هزینه بهره وری را داشته باشد و بتواند به تصویر شرکت آسیب برساند. در کشورهای دیگر، اعتصابها می توانند بسیار خطرناک تر باشند، به ویژه هنگامی که سایر موضوعات سیاسی با موضوعات پولی در هم تنیده می شوند.

۲- شورش ها Riots

شورش ها اغلب به ظاهر از هیچ جایی اتفاق نمی افتند، اگرچه معمولاً از یک مسئله اساسی در برخی حادثه ها مشتعل می شود. این وقایع می تواند بسیار خطرناک باشد زیرا انبوه بزرگ جمعیت اغلب در فعالیت هایی شرکت می کنند که به طور معمول هیچ یک از افراد به تنهایی انجام نمی دهند. اغلب مشاهده می شود شرکت خواستار درک برخی از احساسات ناچیز یا اشتباهی است که آشوبگران رنج می برند. در این حالت شرکت و دارایی های آن به یک هدف بزرگ و تا حدودی آسان تبدیل می شوند.

۳- نافرمانی مدنی Civil Disobedience

نافرمانی مدنی امتناع عمدی از پیروی از برخی قوانین، خواسته ها و دستورات یک دولت است و معمولاً، گاهی اوقات، به عنوان مقاومت غیر خشونت آمیز تعریف می شود. یکی از نتایج فرعی این امر، اختلال در برخی فرایندها برای جلب توجه به درک بی عدالتی قانون یا نقض قانون است.

همچنین ممکن است خود را بعنوان عملی برضد برخی از اقدامات شرکت تصور کند که ممکن است غیرقانونی نباشد اما ممکن است توسط بعضی از گروه‌ها به نوعی مضر تلقی شود. در این صورت، امنیت فیزیکی تأسیسات مهم می‌شود، زیرا در بعضی موارد ممکن است برای آسیب رساندن به تأسیسات اقدام شود.

۴- اعمال تروریستی Terrorist Acts

تهدیدات مربوط به فعالیت‌های تروریستی به طور فزاینده‌ای باعث شده است تا نه تنها امنیت تأسیسات داخل و خارج از کشور بلکه امنیت جسمی کارگران و افسران نیز مورد توجه قرار گیرد. در بسیاری از موارد، صنایع خاص برنامه‌های اضطراری را برای رسیدگی به اقدامات تروریستی طراحی کرده اند، که بسیار مفید است. برای اطمینان از بهترین نتیجه ممکن در مورد اینگونه حمله، واکنش‌هایی وجود دارد که در مورد سناریوهای مشترک تکرار می‌شود.

۵- بمب گذاری Bombing

بمب گذاری تأسیسات یا دارایی‌های شرکت، یک اتفاق نادر است، امروزه دیگر در بسیاری از نقاط جهان چنین چیزی وجود ندارد. بطور فزاینده‌ای، شرکت به دنبال افزایش ملاحظاتمانند سطح آشفته‌گی محلی و ناآرامی سیاسی عمومی در منطقه قبل از انتخاب مکان‌های (سایت‌ها) شرکت است. در بسیاری موارد، یک تهدید ساده بمب برای اجرای برنامه‌های تخلیه که هم پرهزینه و هم مخرب می‌باشد، کافی است. با وجود این، برنامه‌های تخلیه که به تهدیدات و بمب گذاری‌های تروریستی می‌پردازد، به بخشی تفکیک ناپذیر از هرگونه سیاست امنیتی، به ویژه در برخی از نقاط جهان تبدیل شده است.

طراحی سایت و تأسیسات Site and Facility Design

برای بسیاری از سازمانهای آینده نگر، ملاحظات مربوط به امنیت فیزیکی در هنگام انتخاب و طراحی سایت آغاز می‌شود. این شرکت‌ها آموخته اند که ایجاد امنیت در مقایسه با وصله‌های (پچ‌ها) امنیتی پس از واقعیت آسان تر است. در این بخش، انتخاب سایت و شیوه‌های ساخت سایت که می‌تواند منجر به افزایش امنیت فیزیکی شود، پوشش داده شده است.

مدل دفاعی لایه‌ای Layered Defense Model

تمام امنیت فیزیکی باید در یک مدل دفاعی لایه‌ای Layered defense model مستقر شود. در چنین الگویی، اتکاء نباید بر اساس یک مفهوم امنیتی فیزیکی منسجم باشد بلکه باید بر استفاده از رویکردهای متعدد که از یکدیگر پشتیبانی می‌کنند، صورت گیرد. تئوری این است که اگر یک لایه دفاعی نتواند (مثلاً امنیت پیرامون) به عنوان لایه دیگر پشتیبان (مانند قفل درب اتاق سرور) عمل می‌کند. لایه بندی Layering در مفاهیم مورد بحث در این فصل می‌تواند امنیت کلی فیزیکی را تقویت کند.

CPTED

پیشگیری از جرم از طریق طراحی محیط Crime Prevention Through Environmental Design (CPTED) به طراحی تأسیسات از سطح پایه تا پشتیبانی از امنیت اطلاق می‌شود. در واقع یک مفهوم گسترده می‌باشد که می‌تواند برای هر پروژه (توسعه مسکن، ساختمانهای اداری و موسسات خرده فروشی) اعمال شود. آدرس ورودی ساختمان، محوطه سازی و طراحی داخلی است. هدف آن ایجاد اثرات رفتاری است که باعث کاهش جرم می‌شود. سه استراتژی اصلی راهنمایی CPTED در این بخش آورده شده است.

✓ کنترل دسترسی طبیعی Natural Access Control

مفهوم کنترل دسترسی طبیعی در مورد ورودی‌های تأسیسات صدق می‌کند که شامل قرار دادن درها، چراغها، نرده‌ها و حتی محوطه سازی است. این هدف برای دستیابی به اهداف امنیتی با کمترین مزاحمت و شیوه زیبایی شناختی می‌باشد. یک هدف واحد می‌تواند در بسیاری موارد برای تحقق چندین هدف امنیتی طراحی شود.

به عنوان مثال، بسیاری از ساختمان‌ها دارای تابلوها و یا صندوق پستی‌های بزرگی در قسمت جلوی ساختمان هستند که چراغ‌هایی روی آنها قرار دارد. این اشیاء دارای اهداف مختلفی هستند. آنها از ورود در برابر اتومبیل‌هایی که می‌توانند داخل ساختمان شوند حفاظت می‌کنند. چراغ‌ها همچنین ورودی را روشن تر کرده و باعث دلسرد شدن مجرم در عملیات تبهکاری می‌شود و در نهایت می‌توانند افراد را به سمت ورودی هدایت کند.

همچنین کنترل دسترسی طبیعی، ایده ایجاد مناطق امنیتی در ساختمان را ترغیب می‌کند. این مناطق قابل برچسب زدن است و از سیستم‌های کارتی می‌توان برای جلوگیری از دسترسی به

مناطق حساس تر استفاده شود. این مفهوم همچنین در به حداقل رساندن ورودی‌ها و کنترل دقیق آن ورودی‌ها ترغیب می‌کند. همچنین ورودی جداگانه‌ای را در قسمت پشت برای تامین کننده‌هایی (کارپردازان) که در دسترس عموم یا قابل مشاهده برای عموم نیست تشویق می‌کند.

✓ نظارت طبیعی Natural Surveillance

نظارت طبیعی استفاده از ویژگیهای فیزیکی محیطی برای ارتقاء میدان دید همه مناطق و در نتیجه دلسرد کردن جرم و تبهکاری در آن مناطق می‌شود. ایده این است که جریان مردم را به گونه‌ای تشویق کنیم که بیشترین درصد آنها در ساختمانهای پر جمعیت باشند، زیرا حضور مردم در یک منطقه باعث دلسرد شدن تبهکاری می‌شود. همچنین تلاش می‌شود میدان دید همه مناطق را به حداکثر برساند.

✓ تقویت سرزمین‌های طبیعی Natural Territorials Reinforcement

هدف از تقویت سرزمین‌های طبیعی ایجاد احساس جامعه در منطقه است و تلاش می‌شود تا حس مالکیت به کارکنان بخشیده شود. همچنین تلاش می‌شود مجرمان بالقوه احساس کنند که فعالیت‌های آنها در معرض خطر کشف قرار دارد و اغلب به شکل دیوارها، نرده‌ها، محوطه سازی و طراحی نور پیاده سازی می‌شود.

طرح امنیت فیزیکی Physical Security Plan

یکی دیگر از جنبه‌های مهم طراحی سایت و تاسیسات، همگرایی مناسب بین چیدمان فیزیکی و طرح امنیت فیزیکی است. دستیابی به اهداف CPTED همیشه امکانپذیر نیست و در مواردی دارای شکاف می‌باشد، طرح امنیت فیزیکی باید شامل سیاست‌ها و / یا روش‌هایی باشد که برای بستن هرگونه شکاف طراحی شده است. این طرح باید به موارد زیر پردازد.

فعالیت جنایی بازدارنده Deter Criminal Activity

هم چیدمان و هم سیاست‌های حمایتی باید جلوی فعالیت‌های مجرمانه را بگیرد. به عنوان مثال، هر چقدر بیشتر امکان دارد مناطق باز بوده و به راحتی مشاهده شود. باید حداقل مناطق جدا شده و تاریک وجود داشته باشد. علائمی که نشانگر دوربین یا نظارت بر روی محل و حضور نگهبانان هستند نیز می‌توانند به عنوان بازدارنده عمل کنند.

تأخیر مزاحمان Delay Intruders

یکی دیگر از ویژگیهای مفید برنامه امنیت فیزیکی، اضافه کردن موانع ورود به سیستم، مانند قفل ها، نرده ها و موانع است. هر روشی که باعث کند شدن و نظارت بر ورود افراد به تاسیسات می شود نیز می تواند کمک کند. هرچه فرد مزاحم با تأخیر بیشتری مواجه شود، احتمال وی در انتخاب کردن تاسیسات، کمتر شده و احتمال گرفتار شدن وی بیشتر می شود.

تشخیص مزاحمان Detect Intruders

سیستم ها و رویه هایی باید وجود داشته باشند که امکان شناسایی فعالیت مجرمانه را فراهم کند. سنسورهای حرکتی، دوربین ها و موارد مشابه اشکال تشخیص مزاحم هستند. ورود به سیستم برای همه بازدید کنندگان همچنین می تواند نوعی بازدارندگی باشد.

ارزیابی وضعیت Assess Situation

این طرح باید پرسنل و اقدامات خاصی را که هنگام وقوع یک رخداد انجام شود، شناسایی کند. جمع آوری لیستی از انواع حوادثی که حاکی از پاسخ قابل قبول، زمان پاسخ و نام مخاطب می باشد، امکان دارد مفید باشد. طرح های مکتوب که پیش از موعد تهیه شده اند، پاسخی بسیار مؤثرتر و مداوم ارائه می دهند.

واکنش به اغتشاشات و اختلالات Respond to Intrusions and Disruptions

این طرح همچنین باید در پیش بینی و توسعه واکنش های مناسب به افراد مزاحم و اختلالات رایج (قطع برق، مشکلات آب و برق و غیره) صورت گیرد. اگرچه پیش بینی هر رخداد احتمالی غیرممکن است، اما ایجاد یک لیست که می تواند مزاحمت ها و اختلالات احتمالی را پوشش دهد، قابل انجام است. سپس می توان پاسخهای نوشتاری از سوی کلیه پرسنل را برای اطمینان از یک واکنش مداوم و قابل پیش بینی در مورد این رخدادها ایجاد کرد.

مسائل مربوط به انتخاب تأسیسات Facility Selection Issues

هنگامی که یک سازمان به سمت تأسیسات جدید حرکت می‌کند و یا بزرگ می‌شود، فرصتی عالی است که می‌تواند مسائل مربوط به امنیت فیزیکی را در روند انتخاب سایت یا گسترش طرح (Plan) درج کند. در این بخش برخی موارد مهم را مشاهده می‌کنیم.

میدان دید Visibility

میزان میدان دید مورد نظر به سازمان و فرآیندهای انجام شده در محل کار بستگی دارد. در بعضی موارد داشتن دید بالا از محل برای تبلیغ برند یا راحتی مشتریان سودمند است. در موارد دیگر، مشخصات (پروفایل) سطح پایین تری می‌خواهد وقتی که عملیات حساس انجام می‌شود. در این صورت، احتمال استراق سمع خارج از محل کار از طریق پنجره در نظر گرفته می‌شود. همچنین توجه به مناطق مشترک نیز مهم است. در صورت امکان، مناطق نباید جدا یا تاریک شوند. مناطق مرئی با نورپردازی باشد تا از وقوع جرم خودداری شود. از جمله این موارد شامل راهروها، پارکینگ‌ها و سایر مناطق مشترک هستند.

محیط اطراف و اشخاص خارجی Surrounding Area and External Entities

توجه به محیطی که تأسیسات در آن قرار دارد نیز از اهمیت بالایی برخوردار است. چه نوع محله‌ای است؟ آیا منطقه‌ای است که میزان جرم بالایی دارد یا منطقه‌ای جدا می‌باشد؟ جداسازی می‌تواند مناسب باشد، ولی می‌تواند باعث جرم و جنایت شود که ممکن است برای یک دوره زمانی طولانی تر کشف نشود. همچنین فاصله تا ایستگاه‌های پلیس، تجهیزات پزشکی و ایستگاه‌های آتش نشانی را نیز در نظر بگیرید. در نهایت، ماهیت عملکرد مشاغل اطراف را در نظر بگیرید که آیا آنها تهدیداتی را برای فعالیتتان ایجاد می‌کنند.

دسترسی Accessibility

سهولت دسترسی کارمندان و افسران به تأسیسات مورد توجه است. شرایط ترافیکی که کارمندان با آن روبرو می‌شوند چیست؟ اگر این تأسیسات جدید جایگزین یک واحد قدیمی شود، آیا برای بخش عمده کارمندان ناخوشایند است؟ آیا ریسک از دست دادن کارمندان در هنگام رفت و آمد وجود دارد؟ آیا این مکان برای گزینه‌های حمل و نقل مانند ایستگاه‌های قطار و فرودگاه‌ها مناسب

است؟ اگر تعداد زیادی سفر مورد نیاز کارمندان باشد، دسترسی به آن می تواند مهم باشد. اگر اغلب به طور موقت میزبان کارمندان سایر مناطق یا شرکای تجاری هستید، اقامتگاهها در این نزدیکی مناسب هستند؟

ساخت و ساز Construction

موادی که برای ساخت تأسیسات مورد استفاده قرار می گیرد موضوع مهم دیگری است. اما مواردی که باید در اینجا مورد توجه قرار گیرند، صرفاً به شکل دیوارها و سقفها ختم نمی شوند، اگرچه این امر بسیار مهم است. سیستم های پشتیبانی ساخته شده در ساختمان نیز دارای اهمیت هستند و موارد زیر را شامل می شوند:

- دیوارها
- درب ها
- سقف
- پنجره ها
- کفپوش
- HVAC
- منبع تغذیه
- خدمات رفاهی
- شناسایی آتش و سرکوب

برخی ملاحظات ویژه شامل موارد زیر است:

- مطابق با 2^{ISC} ، تمام دیوارها باید دارای توانایی حداقل مقاومت دو ساعته در برابر آتش داشته باشند.
- درها باید در مقابل ورود اجباری مقاومت داشته باشند.
- مکان و نوع سیستم های مهار آتش باید مشخص باشد.
- کف سازی در اتاق های سرور و کمدهای سیم کشی باید بالا برده شود تا به کاهش آسیب های ناشی از سیل کمک کند.
- منابع برق پشتیبان و منبع متناوب باید وجود داشته باشند.
- واحدهای AC جداگانه باید اختصاص داده شوند و کیفیت هوا / رطوبت برای مراکز داده (Data Center) و اتاق های رایانه ای کنترل شود.

محفظه داخلی Internal Compartments

در بسیاری از مناطق یک تاسیسات، از پارتیشن‌ها برای تفکیک مناطق کاری استفاده می‌شود. این پارتیشن‌ها اگرچه همانند دیوارها می‌باشند، دیوارهای کامل نیستند و تا سقف امتداد ندارند. هنگامی که این رویکرد ساخت و ساز با سقف کاذب ترکیب شود، که در بسیاری از ساختمانها رایج است، فرصتی برای شخص فراهم می‌شود که از طریق سقف کاذب به اتاق مجاور دسترسی پیدا کند. کلیه اتاق‌هایی که نیاز به ایمن سازی دارند مانند اتاق‌های سرور و کمدهای سیم کشی نباید شامل این نوع دیوارها باشند.

اتاق‌های تجهیزات و رایانه Computer and Equipment Rooms

زمانی که در اتاق‌هایی هستیم که دارای تجهیزاتی هستند که از طریق دسترسی فیزیکی باید از آنها کنترل شود، مثل آنهایی که دارای سرورهای حساس و تجهیزات شبکه حساس هستند، اتاق‌های تجهیزات و رایانه باید همیشه قفل شده و دارای محافظ‌های ایمن و مناسب باشند:

- در صورت امکان اتاق تجهیزات و رایانه را در مرکز ساختمان قرار دهید.
- اتاق‌های رایانه و تجهیزات باید دارای یک واحد درب دسترسی یا محل ورود باشند.
- از طبقات بالای ساختمان‌ها برای اتاق‌های رایانه و تجهیزات خودداری کنید.
- سیستم‌های ضد حریق و سرکوب را اغلب تست و نصب کنید.
- کفپوش را نصب کنید.
- در صورت امکان منبع تغذیه جداگانه برای اتاق‌های رایانه و تجهیزات نصب کنید.
- فقط از درب‌های مستحکم استفاده کنید.

ساختمان و امنیت داخلی Building and Internal Security

اگرچه امنیت محل کار حائز اهمیت است، امنیت داخل ساختمان نیز همانطور که در مدل دایره متحدالمرکز مشخص شده است دارای اهمیت است. در این بخش موضوعات مربوط به فضای داخلی تأسیسات ارائه شده است.

درب ها Doors

انواع درب ها و مصالح درب را می توان در ساختمانها استفاده کرد. درب ها می توانند توخالی باشند، که در داخل ساختمان مورد استفاده قرار می گیرند، یا مستحکم که معمولاً در لبه ساختمان و در مکانهایی که امنیت بیشتری لازم دارد، استفاده می شوند. برخی از انواع درب ها که یک متخصص امنیت باید با آنها آشنا باشد و برای انتخاب محافظت آماده باشد عبارتند از:

- درب های هرمی یا گنبدی: به صندوق امانات یا اتاق های امنیتی منتهی می شود.
- درب های پرسنلی: توسط انسان برای ورود به تأسیسات استفاده می شود.
- درب های صنعتی: درب های بزرگی که امکان دسترسی به وسایل نقلیه بزرگتر را فراهم می کنند
- درب های دسترسی به وسیله نقلیه: درب های ورودی به پارکینگ یا تعداد زیادی از آن
- درب های ضد گلوله: درب هایی که برای مقاومت در برابر سلاح گرم طراحی شده اند.

انواع قفل درب Door Lock Types

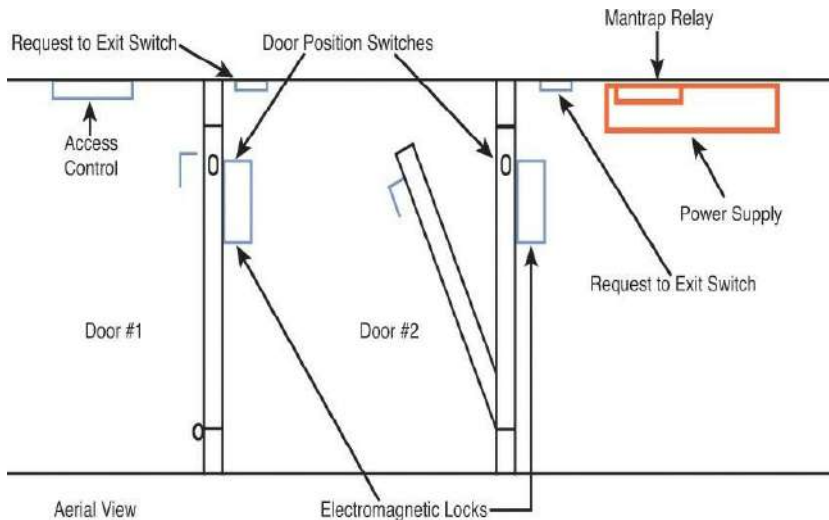
قفل درب ها می توانند مکانیکی یا الکترونیکی باشند. قفل های الکترونیکی Electric locks یا قفل های رمز گذاری شده Cipher Locks از یک صفحه کلید استفاده می کنند که برای باز کردن قفل به کد صحیح نیاز دارد. این درب ها قابل برنامه ریزی هستند و سازمان هایی که از آنها استفاده می کنند باید گذر وازه را به طور مکرر تغییر دهند. نوع دیگر سیستم امنیتی درب، دستگاه احراز هویت مجاور Proximity Authentication Device است که با استفاده از آن یک کارت قابل برنامه ریزی برای انتقال کد دسترسی به دستگاه یا با کشیدن کارت یا در برخی موارد فقط با مجاورت قرار دادن کارت، استفاده می شود. این دستگاه ها به طور معمول شامل اجزای کنترل دسترسی الکترونیکی زیر (EAC) زیر هستند:

- ✓ قفل الکترومغناطیسی Electromagnetic Lock
- ✓ خواننده معتبر Credential Reader
- ✓ یک سنسور درب بسته Closed door sensor

درب کنترل تردد و مانتراپ (تله آدمگیر) Turnstiles and Mantraps

دو نوع خاص از دستگاه کنترل دسترسی فیزیکی، مانتراپ‌ها و درب کنترل تردد هستند که نیاز به اشاره دارند. اگرچه ممکن است با یک درب کنترل تردد آشنا باشید، که می‌تواند با اسکن یا کشیدن کارت دسترسی باز شود، یک مانتراپ یک سیستم غیرمعمول است که شاید با آن آشنا نباشید.

مانتراپ مجموعه‌ای از دو درب است که یک اتاق کوچک بین آنها وجود دارد. کاربر در اولین بار تأیید می‌شود و سپس وارد اتاق می‌شود. در آن مرحله، تأییدیه‌های اضافی رخ می‌دهد (مانند یک نگهبان که شخص را بصری شناسایی می‌کند) و سپس از طریق درب دوم مجاز می‌شود. این درب‌ها معمولاً فقط در شرایط امنیتی بسیار بالا استفاده می‌شوند. مانتراپ‌ها همچنین به طور معمول نیاز دارند که درب اول قبل از اینکه درب دوم باز شود، بسته شود. شکل ۳-۲۰ طرح مانتراپ را نشان می‌دهد.

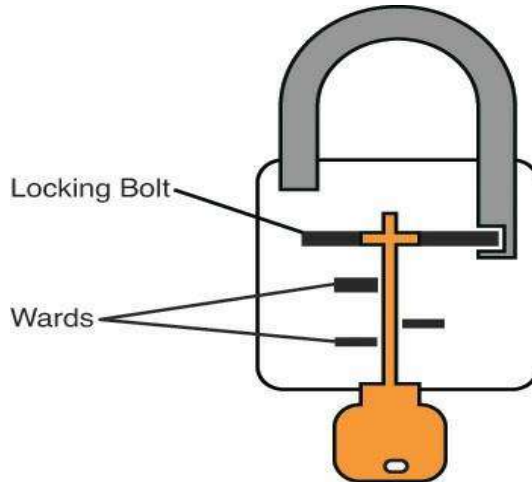


شکل ۳-۲۰: مانتراپ

قفل‌ها Locks

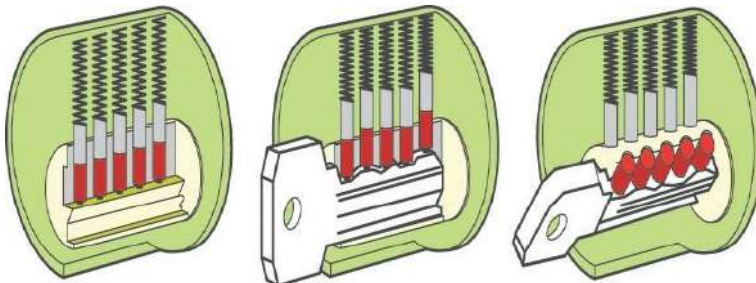
همچنین از قفل‌ها در جاهایی غیر از درب‌ها نیز استفاده می‌شود، مانند محافظت از کابینت و تجهیزات امن.

انواع قفل های مکانیکی که باید با آنها آشنا باشید عبارتند از:
قفل های نگهدارنده Warded locks: این قفلها دارای پیچ فنری هستند که شکافی در آن قرار دارد. این قفل دارای بخش ها یا طرح ریزی فلزی در داخل قفل است که با کلید مطابقت دارد و باز کردن قفل را امکان پذیر می کند. طراحی قفل دنده دار در شکل ۳-۲۱ نشان داده شده است.



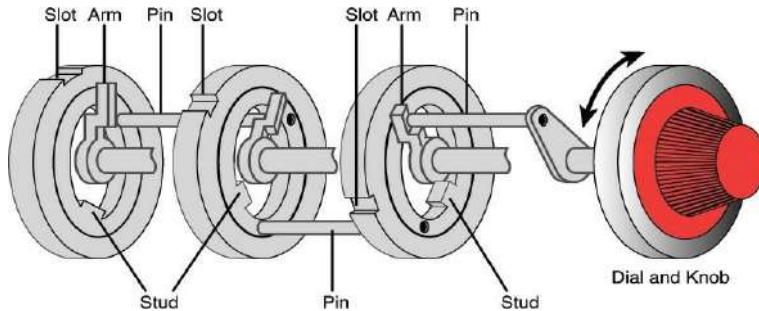
شکل ۳-۲۱: قفل دنده دار

قفل های گیره دار Tumbler locks: این قفلها دارای قطعات متحرک بیشتری نسبت به قفل نگهدارنده هستند و کلید، قطعه فلزی قفل را به ارتفاع صحیح بالا می برد. طراحی قفل گیره دار در شکل ۳-۲۲ نشان داده شده است.



شکل ۳-۲۲: قفل گیره دار

قفل‌های ترکیبی *Combination locks*: این قفل‌ها نیاز به چرخش قفل در الگویی دارند که در صورت صحیح، گیره‌ها را به سمت بالا کشیده و قفل باز می‌شود. طراحی قفل ترکیبی در شکل ۳-۲۳ نشان داده شده است.



شکل ۳-۲۳: قفل ترکیبی

در مورد قفل دستگاه، لپ تاپ‌ها آیتم اصلی هستند که باید محافظت شوند زیرا سرقت آنها بسیار آسان است. لپ تاپ‌ها بدون اینکه به قفل کابل محکم متصل شده باشند هرگز نباید در فضای باز قرار گیرند. این کابل‌های فولادی با روکش وینیل هستند که به لپ تاپ متصل می‌شوند و سپس به یک جسم قفل می‌شوند.

بیومتریک Biometrics

بالاترین سطح کنترل دسترسی فیزیکی و گرانترین برای استقرار، دستگاه بیومتریک است. وسایل بیومتریک در فصل ۵ به طور گسترده پوشش داده می‌شود.

ورودی‌های شیشه‌ای Glass Entries

ورودی‌های شیشه‌ای، که در بسیاری از تاسیسات رایج شده اند، شامل پنجره ها، درب‌های شیشه‌ای و دیوارهای شیشه‌ای هستند. شیشه متناسب با شرایط انتخاب می‌شود. یک متخصص امنیت باید با انواع شیشه‌های زیر آشنا باشد:

- ✓ استاندارد Standard: در منطقه مسکونی استفاده می‌شود و به راحتی شکسته می‌شود.
- ✓ آبدیده Tempered: با گرم کردن شیشه ایجاد می‌شود، که به آن استحکام بیشتری می‌بخشد.

✓ اکریلیک Acrylic: ساخته شده از پلی کربنات اکریلیک، بسیار قوی تر از شیشه معمولی است اما هنگام سوختن دود سمی تولید می کند.

✓ چند لایه Laminated: دو ورقه شیشه با یک غشای پلاستیکی بین آن، که شکستن آن را مشکل تر می کند.

در مناطقی که باید از شیشه معمولی استفاده شود ولی امنیت بسیار مورد توجه است، می توان از شیشه ای استفاده کرد که با سیم تعبیه شده تا احتمال شکستن و ورود آن را کاهش دهد. یک گزینه قوی تر همراه پنجره، نصب میله های فولادی است.

کنترل بازدید کنندگان Visitor Control

باید تعدادی از سیستم های شناسایی بازدید کنندگان و کنترل دسترسی آنها به تأسیسات، وجود داشته باشد. بهترین سیستم این است که همه بازدید کنندگان را قبل از ورود که می خواهند وارد سیستم شوند، از لحاظ حضور فردی بررسی شوند. اگر این امر غیرممکن باشد، گزینه دیگر تهیه یک نقطه ورود است که در آن بازدید کنندگان با یک درب قفل شده و یک تلفن فراهم می باشد که می تواند با تماس برای درخواست دسترسی، استفاده شود. هر یک از این روشها به سادگی برای جلوگیری از ورود افراد غیر مجاز در ساختمان و رفتن به جایی که آنها می خواهند کمک می کند.

بهترین کار دیگر در رابطه با بازدید کنندگان این است که همیشه یک پیمانکار، وی را برای رسیدن به مقصدش همراهی کند تا اطمینان حاصل شود که آنها به جایی که نباید بروند، دسترسی ندارند. در شرایط کم امنیت، این کار ممکن است لازم نباشد اما در مناطق با امنیت بالا توصیه می شود. در نهایت هم، همه ورود بازدیدها را وارد کنید.

اتاق تجهیزات Equipment Rooms

مناطق را که تجهیزات در آن ذخیره می شود قفل کرده و دسترسی به آنها را کنترل کنید. داشتن لیست موجودی دقیق کلیه تجهیزات برای کشف سرقت نیز حائز اهمیت است. برای مراکز داده و اتاق های سرور، موانع بالاتر می رود. در ادامه در این بخش اطلاعات بیشتری در مورد این موضوع وجود خواهد داشت.

مناطق کار Work Areas

به خاطر امنیت، برخی از سیستم‌ها باید در مناطق جداگانه قرار گیرند. در این بخش درمورد برخی مکانهای خاص که ممکن است اقدامات امنیتی اضافی لازم باشد، بحث می‌شود. بیشتر این اقدامات هم برای بازدید کنندگان و هم برای کارمندان اعمال می‌شود. ممنوعیت برخی از کارمندان در برخی مناطق ممکن است سودمند باشد.

مرکز داده امن Secure Data Center

مراکز داده باید با قفل از نظر فیزیکی ایمن باشند و نباید دارای سقف کاذب باشند. برخی ملاحظات اضافی برای اتاقهایی که وسایل زیادی در آن وجود دارد:

- نباید در طبقه بالا یا زیرزمین‌ها قرار داده شود.
- برای دسترسی آسان باید یک سوئیچ در نزدیکی درب قرار داشته باشد.
- برای این اتاقها HVAC جداگانه توصیه می‌شود.
- برای هشدار از مشکلات دما یا رطوبت باید ناظر محیطی Environmental Monitoring قرار داده شود.
- برای جلوگیری از آسیب رساندن از طریق آب باید کفها را بالاتر قرارداد.
- کلیه سیستم‌ها باید دارای UPS و تمام اتاق متصل به یک ژنراتور باشند.

محدوده منطقه کاری Restricted Work Area

این مرکز ممکن است مناطقی باشد که فقط به کارمندان درگیر فعالیت، محدود شود. در این موارد سیستم‌های دسترسی فیزیکی باید با استفاده از کارت‌های هوشمند، دستگاه‌های کارتخوان مجاور، صفحه کلید یا هر مکانیزم دسترسی فیزیکی دیگر که در این کتاب شرح داده شده، صورت گیرد.

مرکز رسانه‌های ذخیره سازی Media Storage Facilities

مرکز رسانه‌های ذخیره سازی عبارت است از یک ساختمان یا یک منطقه امن در داخل یک ساختمان که رسانه در آن ذخیره می‌شود. از آنجا که رسانه‌ها می‌توانند به اشکال مختلفی وجود داشته باشند، سازمانها باید قبل از انتخاب مرکز رسانه‌های ذخیره سازی، باید مشخص شود از

کدام نوع رسانه ذخیره سازی استفاده میکنند. اگر فقط نوار یا رسانه نوری ذخیره می شود، کافی است فقط یک صندوق اتفاء حریق را در مرکز داده های موجود سازمان نصب کرده و یک نسخه پشتیبان را در یک مکان از راه دور Remote Location ذخیره شود. با این حال، در برخی موارد، راه حل بسیار بزرگتر به دلیل میزان داده هایی که محافظت می شوند، ضروری است. در صورت نیاز به یک مرکز ذخیره سازی رسانه ای مجزا، سازمان باید مطمئن شود که این مرکز امنیت فیزیکی مناسبی را برای حفاظت از رسانه های ذخیره شده در آنجا فراهم می کند.

ذخیره سازی مدارک Evidence Storage

اگر سازمان شواهد و مدارکی را که برای تحقیق مهم است، جمع آوری کرده باشد، سازمان باید مطمئن شود که شواهد و مدارک از دسترس کاربران غیر مجاز محافظت می شود. فقط پرسنل درگیر در تحقیقات باید به مدارکی که ذخیره شده، دسترسی داشته باشند. مدارک و شواهد باید در یک اتاق دارای قفل ذخیره شده و دسترسی به مدارک باید ثبت شود. مدارک باید در زمان مناسب برای اجرای قانون تحویل داده شود. اگر نسخه های پشتیبان از مدارک دیجیتال در طول تحقیقات حفظ شوند، نسخه های پشتیبان نیز باید در یک فضای امن با دسترسی محدود به پرسنل قرار داده شود.

امنیت محیطی Environmental Security

اگرچه بیشتر ملاحظات مربوط به امنیت حول محور جلوگیری از سوءاستفاده قرار دارد، اما جلوگیری از صدمه دیدن داده ها و تجهیزات از شرایط محیطی نیز بر عهده تیم امنیت است زیرا این قسمت جزء در دسترس بودن (Availability) مثلث سیا می باشد.

حفاظت در مقابل آتش Fire Protection

حفاظت از آتش از تاریخچه طولانی تری نسبت به بسیاری از مباحث مطرح شده در این کتاب برخوردار است در حالی که هنوز ملاحظات سنتی در مورد جلوگیری از آتش سوزی و خسارت ناشی از آتش، صحیح است، اما وجود تجهیزات حساس رایانه ای نیاز به رویکردهای متفاوتی برای تشخیص و پیشگیری دارد که موضوع این بخش است.

شناسایی آتش Fire Detection

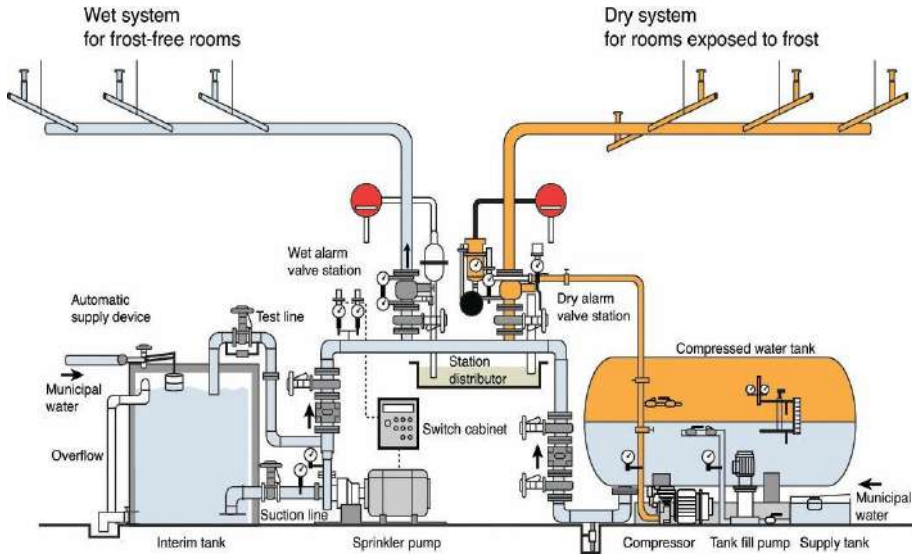
گزینه‌های مختلفی برای شناسایی آتش وجود دارد. انواع اصلی سیستم‌های تشخیص آتش به شرح زیر می‌باشد:

- ✓ عملیات دودزا Smoke-activated: با استفاده از دستگاه فوتوالکتریک برای تشخیص تغییرات نور ناشی از ذرات دود فعالیت می‌کند.
- ✓ گرم‌زدایی Heat-activated (که آن را حس گرمایشی Heat-sensing نیز می‌نامند): با شناسایی تغییرات دما عمل می‌کند. در صورت برآورده شدن درجه دما از پیش تعیین شده یا وقتی میزان افزایش مقدار مشخصی باشد، می‌تواند هشدار دهد.
- ✓ محرک به شعله ور شدن Flame-actuated: دستگاه‌های نوری که منطقه حفاظت شده را نظارت می‌کنند. معمولاً سریع‌تر به شناسایی آتش نسبت به دستگاه‌های غیر نوری واکنش نشان می‌دهند.

مهار آتش Fire Suppression

اگرچه مطمئناً کپسول آتش‌نشانی یک شکل دستی برای مهار آتش هست، اما سایر سیستم‌های خودکار نیز وجود دارد. باید با انواع سیستم آبپاش زیر آشنا باشید:

- **لوله مرطوب Wet pipe:** از آب موجود در لوله‌ها برای خاموش کردن آتش استفاده می‌شود. در بعضی از مناطق، ممکن است آب لوله‌ها یخ زده، و خسارت وارد کند. این موارد همچنین برای اتاق‌هایی که تجهیزات در اثر خیس شدن آسیب می‌بیند، توصیه نمی‌شود.
- **لوله خشک Dry pipe:** در این سیستم، آب در در مخزن نگهدارنده، نگهداری می‌شود. لوله‌ها هوای تحت فشار را در خود نگه می‌دارند که با شناسایی آتش باعث می‌شود فشار کاهش یابد و آب اجازه ورود به لوله و آبپاش‌ها را پیدا می‌کند، و احتمال خالی شدن به صورت تصادفی را به حداقل می‌رساند. شکل ۳-۲۴ مقایسه سیستم‌های مرطوب و خشک را نشان می‌دهد.



شکل ۳-۲۴: سیستم های لوله های مرطوب و خشک

- پیش فعال *Preaction*: مانند سیستم لوله های خشک عمل می کند به علاوه در نوک آبپاش یک اتصال حرارتی قابل احتراق وجود دارد که باید قبل از رها شدن آب ذوب شود. در حال حاضر این سیستم پیشنهادی برای اتاق های رایانه می باشد.
- سیل: *Deluge* اجازه می دهد مقدار زیادی آب داخل اتاق آزاد شود، بدیهی است که این امر گزینه مناسبی در محل نصب تجهیزات محاسباتی محسوب نمی شود.
- در یک زمان، سیستم های مهار آتش از گاز هالون استفاده می کردند که با سرکوب احتراق از طریق یک واکنش شیمیایی به خوبی عمل می کرد. با این حال، این سیستم ها دیگر مورد استفاده قرار نمی گیرند زیرا مشخص شده است که به لایه اوزون آسیب می رسانند.
- جایگزینی های تایید شده توسط EPA برای هالون شامل موارد زیر است:
 - آب، آرگون، NAF-S-III
 - FM-200 یکی دیگر از سیستم های مهار آتش است که در اتاق های رایانه می تواند به رایانه ها آسیب نرسانده و برای انسان بی خطر می باشد.

Power Supply

منبع تغذیه شرکت و کلیه تجهیزات می‌باشد. در این بخش به مسائل مربوط به برق مشترک و برخی از مکانیسم‌های پیشگیری و تکنیک‌های کاهشی می‌پردازیم که به شرکت اجازه می‌دهد تا هنگام بروز مشکلات برقی به فعالیت خود ادامه دهد.

انواع خاموشی

هنگام بحث در مورد مسائل مربوط به برق، باید با اصطلاحات زیر آشنا باشید:

Surge یک ولتاژ بلند مدت

Brownout افت بلند مدت در مصرف برق که زیر ولتاژ طبیعی است.

Fault قطع برق لحظه ای.

Blackout قطع برق بلند مدت.

Sags کاهش لحظه‌ای سطح برق

با این حال، مشکلات احتمالی برقی فراتر از دست دادن جزئی یا کامل برق است. خطوط برق می‌توانند نویز را نشان داده و در اتصالات شبکه تداخل ایجاد کنند. در صورتی که موتورهای الکتریکی بزرگ یا منبع انواع خاصی از نور، مانند روشنایی فلورسنت وجود داشته باشد، از کابل کشی محافظ برای جلوگیری از تداخل فرکانس رادیویی (RFI) و تداخل الکترومغناطیسی (EMI) استفاده می‌شود.

اقدامات پیشگیرانه Preventive Measures

اقداماتی برای جلوگیری از الکتریسیته ساکن و آسیب رساندن به مولفه‌های سازنده باید رعایت شود.

برخی اقدامات احتیاطی در مورد این موارد عبارتند از:

- ✓ از اسپری‌های ضد الکتریسیته ساکن استفاده کنید.
- ✓ سطح رطوبت مناسب را حفظ کنید.
- ✓ از تشک ضد اصطکاک و مچ بندها استفاده کنید.
- ✓ برای محافظت در برابر برق (تضعیف و جریان سریع و غیرعادی) و هر قطع شدن جزئی و کل برق، دستگاه‌های زیر قابل استفاده هستند:

- دستگاه‌های تهویه Power conditioners: بین پریز برق و دیواره دستگاه رفته و نوسانات قدرت تحویل شده به دستگاه را هموار کرده و از تضعیف و جریان سریع و غیرعادی محافظت کنید.
- منبع تغذیه بدون وقفه Uninterruptible power supplies (UPS): بین پریز برق و دیواره دستگاه رفته و در صورت از بین رفتن منبع دیواره، از یک باتری استفاده کنید.

HVAC

سیستم‌های گرمایشی و تهویه فقط برای راحتی کارمندان وجود ندارد. مقادیر عظیم تجهیزات محاسباتی (رایانشی) که توسط اکثر شرکتها گسترش یافته اند حتی انسانها هم وابسته به این سیستمها هستند. بدون داشتن شرایط محیطی مناسب، کار متوقف خواهد شد، برای تجهیزات محاسباتی (رایانشی) و دستگاههای زیربنایی مانند روتر و سوئیچ شرایط زیر مناسب نیست:

گرما: گرمای بیش از حد باعث راه اندازی مجدد و تصادف می‌شود.

رطوبت: باعث ایجاد مشکلات خوردگی در اتصالات می‌شود.

رطوبت کم: شرایط خشک، الکتریسیته ساکن را ترغیب کرده، که می‌تواند به تجهیزات آسیب برساند.

با توجه به دما، برخی از حقایق مهم که باید بدانید عبارتند از:

در ۱۰۰ درجه، آسیب به رسانه مغناطیسی شروع می‌شود.

در ۱۷۵ درجه، آسیب به رایانه‌ها و لوازم جانبی رخ می‌دهد.

در ۳۵۰ درجه، آسیب به محصولات کاغذی وارد می‌شود.

به طور خلاصه، لازم است شرایط لازم برای این دستگاه‌ها وجود باشد. به همین دلیل واحدهای AC باید نسبت به سایر سیستمهای HVAC به تجهیزات پردازش اطلاعات، منبع تغذیه جداگانه‌ای اختصاص دهند.

نشت آب و جاری شدن سیل Water Leakage and Flooding

به همان اندازه که سیستم‌های محاسباتی به گرما علاقه‌ای ندارند، همچنین به آب هم علاقه‌ای ندارند. همچنین می‌تواند صدمات گسترده‌ای به کفپوش‌ها، دیوارها و پایه و اساس تاسیسات وارد کند. ردیاب‌های آب باید در زیر طبقه‌ها و بالای سقف‌های کاذب قرار گیرند تا نشتی در سقف و آب زیر کف‌ها قبل از ایجاد مشکل بزرگتر تشخیص داده شود.

صحبت از طبقات مطرح شده، در مناطقی مانند کمد سیم کشی، مراکز داده و اتاق سرور، باید تمام طبقات بالا برده شوند تا در صورت افزایش آب، میزان خطای اضافی ارائه شود.

هشدارهای محیطی Environmental Alarms

خطایی که باعث می شود سیستم به دلیل محیطی که در آن نصب شده آسیب پذیر باشد، خطای محیطی Environmental Error نامیده می شود. با توجه به چالش های گوناگون ارائه شده توسط خواسته های محیطی که توسط تجهیزات محاسباتی در تاسیسات قرار داده شده و هزینه های رفع نشدن این نیازها، اقتضاء شرکت اینگونه می باشد که دارای سیستم هایی باشد که در صورت کمبود شرایط محیطی هشدار دهد. سیستم هشدار مانند ردیاب سنج، که رطوبت را رصد می کند، باید در مناطقی که تجهیزات حساس در آن قرار دارد، برقرار شود. سیستم همچنین باید دما را نیز کنترل کند. این نوع کنترل ها، کنترل فیزیکی به حساب می آیند.

امنیت تجهیزات Equipment Security

در تمام این کتاب بر امنیت فیزیکی تجهیزات تأکید شده است. در این بخش رویه های شرکتی مربوط به تجهیزات و رسانه ها و استفاده از گاوصندوق و اتاق های نگهدارنده برای محافظت از سایر دارایی های ارزشمند فیزیکی مورد بحث قرار می گیرد.

✓ رویه شرکت Corporate Procedures

امنیت فیزیکی تجهیزات و رسانه ها باید در سیاست ها و رویه های امنیتی شرکت طراحی شود. این رویه ها باید به موارد زیر پردازد.

✓ محافظت در مقابل مداخله کردن Tamper Protection

برای افراد غیرمجاز امکان دسترسی و تغییر پیکربندی دستگاهها وجود ندارد. این بدان معنی است که اقدامات دیگری در این بخش باید انجام شود تا از این امر جلوگیری شود. تنظیمات شامل پیش فرض، آسیب رساندن یا تغییر پیکربندی یک دستگاه است. برنامه های تأیید یکپارچگی باید توسط اپلیکیشن ها مورد استفاده قرار گیرد تا به دنبال مدارک و شواهدی که شامل دستکاری داده ها، خطاها و حذفیات باشند.

✓ رمزگذاری Encryption

رمزگذاری داده‌های حساس ذخیره شده در دستگاه‌ها می‌تواند در جلوگیری از قرار گرفتن در معرض افشاء داده‌ها در صورت سرقت یا در صورت دسترسی نامناسب دستگاه به ما کمک کند.

✓ فهرست موجودی Inventory

اگر هیچ سیستم شمارش کالا یا موجودی وجود نداشته باشد، تشخیص سرقت وسایل غیرممکن است. کلیه تجهیزات باید فهرست شوند و کلیه اطلاعات مربوط به هر دستگاه باید حفظ و به روز شود. این اطلاعات به صورت الکترونیکی و هم به صورت Hard copy حفظ شود.

محافظت فیزیکی از دستگاه‌های امنیتی Physical Protection of Security Devices دستگاه‌های امنیتی مانند فایروال‌ها، دستگاه‌های NAT و سیستم‌های تشخیص و جلوگیری از نفوذ باید بیشترین توجه را داشته باشند زیرا این امر به امنیت فیزیکی و منطقی مربوط می‌شود. فراتر از این، دستگاه‌هایی که می‌توانند به راحتی سرقت شوند مانند لپ تاپ، تبلت و تلفن‌های هوشمند، باید قفل شوند. اگر عملی نیست، این نوع دستگاه‌ها را روی یک جسم ثابت قفل کنید. نمونه مناسب از این قفل‌های کابردار هستند که برای لپ تاپ‌ها استفاده می‌شود.

✓ دستگاه‌های ردیابی Tracking Devices

هنگامی که این فناوری در دسترس است، ردیابی دستگاه‌های کوچک می‌تواند برای کاهش تلفات هر دو دستگاه و داده‌های آنها، همانطور که قبلاً پوشش داده شده است، استفاده شود. اکثر تلفن‌های هوشمند اکنون شامل نرم افزار ردیابی هستند که به ما امکان می‌دهد دستگاه را بعد از سرقت یا گم کردن با استفاده از ردیابی برج سلولی یا GPS، مکان یابی کنیم. این تکنولوژی را در صورت امکان استفاده کنید.

یکی دیگر از ویژگی‌های مفید موجود در همین نوع دستگاه‌ها، ویژگی پاک کردن از راه دور است، که اجازه می‌دهد تا یک سیگنال به دستگاه مسروقه ارسال شود و به آن دستور دهد داده‌های موجود در دستگاه را پاک کند. در نهایت، این دستگاه‌ها به طور معمول با قابلیت قفل از راه دور دستگاه در هنگام گم شدن نیز همراه هستند.

✓ رویه‌های رسانه قابل حمل Portable Media Procedures

همانطور که قبلاً ذکر شد، کنترل دقیق استفاده از دستگاه‌های رسانه قابل حمل می‌تواند به جلوگیری از خروج اطلاعات حساس از شبکه کمک کند، که شامل سی دی، دی وی دی، فلش مموری، درایو انگشت شست و هارد اکسترنال است. اگرچه قوانین کتبی باید در مورد استفاده از این دستگاه‌ها اعمال شود، اما استفاده از سیاست‌های امنیتی برای جلوگیری از کپی کردن داده‌ها در این نوع رسانه‌ها نیز امکانپذیر است. مجاز بودن کپی کردن داده‌ها در این نوع درایوها تا زمانی که داده‌ها رمزگذاری شوند نیز امکان پذیر است. اگر این عملکردها توسط سیستم عامل شبکه ارائه شده است، باید آنها را گسترش داد.

✓ صندوق امانات، گاوصندوق، قفل کردن Safes, Vaults, Locking

با توجه به محافظت از دارایی‌های فیزیکی مانند لپ تاپ، تلفن‌های هوشمند، تبلت و غیره، هیچ چیز نمی‌تواند از نظر فیزیکی دستگاه‌ها را به طور کامل قفل کند. در مواردی که امکان انجام این کار وجود دارد، قفسه‌های قفل شونده راه حل مناسبی برای ذخیره این دستگاه‌ها هستند. علاوه بر انتخاب قفل مناسب، باید تمام تجهیزات فهرست شوند و سیستمی برای حفظ کردن این شمارش‌ها طبق ورود و خروج دستگاه‌ها ساخته شود.

برخی از موارد به حفاظت بیشتری حتی از یک قفسه قفل شده احتیاج دارند. اسناد حقوقی مهم و سایر موارد با ارزش زیاد را در و صندوق امانات و گاوصندوق برای حفاظت از این موارد نگهداری شود. صندوق امانات نسوز و گاو صندوق‌ها می‌توانند باعث حفاظت از محتوا در هنگام آتش سوزی شود.

فصل ۴

ارتباطات و امنیت شبکه

(Communication and Network Security)

این فصل موضوعات زیر را در بر می گیرد:

- ❖ اصول طراحی شبکه امن Secure Network Design Principles: مفاهیم پوشش داده شده شامل مدل های OSI و TCP / IP هستند.
 - ❖ IP شبکه Networking: مفاهیم مورد بحث شامل پورتهای مشترک TCP / UDP ، آدرس دهی منطقی و فیزیکی، انتقال شبکه و انواع شبکه می باشد.
 - ❖ پروتکل ها و خدمات Protocols and Services: پروتکل ها و خدمات مورد بحث شامل پروتکل های ARP ، DHCP ، DNS ، FTP ، HTTP ، ICMP ، IMAP ، LDAP ، NAT ، NetBIOS ، POP ، PAT ، SMTP ، SNMP و پروتکل های چند لایه می باشد.
 - ❖ پروتکل های همگرا Converged Protocols: پروتکل های مورد بحث شامل FCoE ، MPLS ، VoIP و iSCSI هستند.
 - ❖ شبکه های بی سیم Wireless Networks: مفاهیم تحت پوشش شامل تکنیک های بی سیم، ساختار WLAN ، استانداردهای WLAN و امنیت WLAN است.
 - ❖ رمزنگاری ارتباطات Communications Cryptography: مفاهیم مورد بحث شامل رمزگذاری پیوند، رمزگذاری End-to-End، امنیت ایمیل و امنیت اینترنت است.
 - ❖ مؤلفه های امن شبکه Secure Network Components: مؤلفه های مورد بحث شامل سخت افزار، رسانه انتقال، دستگاه های کنترل دسترسی به شبکه، امنیت Endpoint و شبکه های توزیع محتوا هستند.
 - ❖ کانالهای ارتباطی امن Secure Communication Channels: کانالهای مورد بحث شامل صدا، همکاری چندرسانه ای، دسترسی از راه دور و شبکه های مجازی هستند.
 - ❖ حملات شبکه Network Attacks: مفاهیم مورد بحث شامل حملات کابل کشی، حملات مؤلفه شبکه، حملات ICMP ، حملات DNS ، حملات ایمیل، حملات بی سیم، حملات از راه دور و سایر حملات است.
- هنگامی که داده ها در حالت ساکن (بر روی هارد دیسک) و در حالت انتقال (انتقال از طریق شبکه) هستند، از داده های حساس باید محافظت شود. علاوه بر این، ارتباطات حساس از انواع دیگر مانند ایمیل، پیام های فوری و مکالمات تلفنی نیز باید در برابر چشم و گوش کنجکاوانه محافظت شوند. بسیاری از فرایندهای ارتباطی اطلاعات را به شکلی ارسال می کنند که اگر با آنالایزر پروتکل یا sniffer به دام بیفتند، قابل خواندن و درک هستند.

در دنیای ارتباطات امروز، باید فرض کنید که ارتباطات شما چگونه ممکن است تصرف شود. همچنین باید گام‌های محافظت یا اقدامات لازم رمزنگاری انتقال را انجام دهید تا برای کسی که آنها را تصرف کرد بی فایده باشد. این فصل حفاظت انتقال سیمی و بی سیم و دستگاه‌های شبکه‌ای که انتقالات را انجام می‌دهند، و همچنین برخی اصول شبکه‌ای که برای درک امنیت انتقال مورد نیاز است را پوشش می‌دهد.

اصول طراحی شبکه امن

برای پیکربندی صحیح ارتباطات و امنیت شبکه، متخصصان امنیت باید اصول طراحی شبکه امن را درک کنند. آنها باید بدانند که چگونه می‌توانند یک شبکه را درست تنظیم کرده که در آینده به حداقل تنظیم مجدد نیاز داشته باشد. برای استفاده از اصول طراحی شبکه امن، متخصصان امنیت باید مدل‌های OSI و TCP / IP را درک کنند.

مدل OSI

درک کامل از شبکه نیاز به درک اتصال سیستم‌های باز Open Systems Interconnection (OSI) دارد. مدل OSI ایجاد شده در دهه ۱۹۸۰ توسط سازمان بین‌المللی برای استاندارد سازی ISO به عنوان بخشی از مأموریت خود برای ایجاد مجموعه پروتکلی که به عنوان استاندارد برای همه فروشندگان مورد استفاده قرار بگیرد، مدل OSI فرایند ارتباطات را به لایه‌هایی تقسیم بندی کرد. اگرچه مجموعه پروتکل آن به عنوان استاندارد به کار نرفت (پروتکل کنترل انتقال / پروتکل اینترنت TCP / IP به تصویب رسید)، این مدل از زمان ایجاد تا کنون، توسعه فناوری را هدایت می‌کند. همچنین به نسل دانشجویان کمک کرده است تا روند ارتباطات شبکه بین دو سیستم را درک کنند. مدل OSI فرایند را به هفت لایه یا مازول تقسیم می‌کند. فواید انجام این کار عبارتند از:

- ✓ این فرایند ارتباط را به لایه‌هایی با واسطه‌های استاندارد بین لایه‌ها تقسیم می‌کند و باعث می‌شود بدون ایجاد تغییر در لایه‌های دیگر، تغییرات و پیشرفت در یک لایه فراهم شود.
- ✓ یک چارچوب مشترک را برای توسعه دهندگان سخت افزار و نرم افزار فراهم می‌کند و باعث تقویت قابلیت همکاری می‌شود.

معماری سیستم های باز متعلق به هیچ فروشنده ای نیست و به عنوان یک طرح یا الگویی برای کار با توسعه دهندگان عمل می کند. پروتکل های مختلفی در لایه های مختلف این مدل فعالیت می کنند. پروتکل مجموعه ای از قواعد ارتباطی است که دو سیستم باید برای برقراری ارتباط از آن استفاده کرده و آنرا درک کنند. برخی پروتکل ها به خدمات پروتکل دیگری بستگی دارند و به همین ترتیب، این پروتکل ها به عنوان تیم برای انجام انتقال فعالیت می کنند، دقیقاً مثل تیمی که در اداره پست است که نامه های شما را تحویل می دهد، برخی افراد مرتب می کنند، برخی دیگر تحویل می دهند و برخی دیگر محموله های گمشده را ردیابی می کنند.

مدل OSI و مدل TCP / IP، که در بخش بعدی توضیح داده شده است، اغلب برای توصیف فرآیند موسوم به ایجاد بسته Packet Creation یا کپسوله سازی Encapsulation استفاده می شوند. تا زمانی که یک بسته برای نگهداری داده ها ایجاد نشود، نمی توان آن را در رسانه انتقال ارسال کرد. با یک رویکرد مدولار، امکان تغییر پروتکل یا اضافه شدن پروتکل جدید بدون نیاز به بازنویسی کل پشته پروتکل (یک اصطلاح برای همه پروتکل هایی که در همه لایه ها با هم کار می کنند) انجام می شود. این مدل دارای هفت لایه است. در این بخش عملکرد هر لایه و رابطه آن با لایه فوقی و زیری آن در مدل مورد بحث قرار می گیرد. لایه ها با شماره گذاری که از انتهای مدل لایه ۱، لایه فیزیکی شروع می شود، بیان می شود.

فرآیند ایجاد یک بسته یا کپسوله سازی از لایه ۷ لایه Application به جای لایه ۱ شروع می شود، بنابراین ما درمورد فرایندی که از لایه ۷ شروع می شود بحث کرده و به لایه ۱ می رسیم. لایه فیزیکی، جایی که بسته در رسانه انتقال داده می شود.

لایه کاربردی Application Layer

لایه کاربردی (لایه ۷) همان جایی است که فرایند کپسوله سازی آغاز می شود. این لایه داده های خام را از اپلیکیشن در حال استفاده دریافت می کند و خدماتی مانند انتقال پرونده و تبادل پیام به اپلیکیشن (و به این ترتیب کاربر) را ارائه می دهد. نمونه ای از پروتکل که در این لایه کار می کند، پروتکل انتقال Hypertext (HTTP) است که برای انتقال صفحات وب از طریق شبکه استفاده می شود. نمونه های دیگر پروتکل هایی که در این لایه کار می کنند عبارتند از پرس و جو DNS، انتقال FTP و انتقال ایمیل SMTP، DHCP، DHCPv6 نیز در این لایه کار می کنند. واسطه های اپلیکیشن کاربر از طریق یک واسط استاندارد به نام واسط برنامه نویسی برنامه API با این پروتکل های اپلیکیشن ارتباط دارد. پروتکل لایه Application داده های خام را دریافت کرده

و آن را در مکانی به نام واحد داده پروتکل PDU قرار می‌دهد. هنگامی که این روند تا لایه ۴ پایین می‌رود، این PDUها دارای اسامی استاندارد هستند، اما در لایه‌های ۵ تا ۷ به سادگی PDU را "داده" می‌نامیم.

لایه نمایشی Presentation Layer

اطلاعاتی که در لایه ۷ ایجاد شده است سپس به لایه ۶ یعنی لایه Presentation ارائه می‌شود. هر لایه تغییری در داده‌های دریافت شده از لایه بالای خود ایجاد نمی‌کند. فقط اطلاعات را به بسته در حال توسعه اضافه می‌کند. در مورد لایه Presentation، اطلاعاتی اضافه می‌شود که در صورت لزوم قالب بندی اطلاعات را استاندارد می‌کند.

لایه ۶ یا Presentation وظیفه نحوه ارائه داده‌های مربوط به لایه Application یا ارائه شده به لایه Application را در دستگاه مقصد (توضیح کامل تر در بخش "Encapsulation") را بر عهده دارد و در صورت نیاز به ترجمه بین قالبها، از آن مراقبت خواهد کرد. همچنین با نوع داده درون بسته و برنامه کاربردی که ممکن است برای خواندن آن در دستگاه مقصد مورد نیاز باشد، ارتباط برقرار می‌کند.

این لایه از دو زیرلایه تشکیل شده است: عنصر خدمات مشترک سرویس اپلیکیشن CASE و عنصر سرویس اپلیکیشن مشخص (SASE). زیر لایه CASE به لایه Application خدمات ارائه می‌دهد و خدمات را از لایه Session درخواست می‌کند. SASE از خدمات خاص اپلیکیشن پشتیبانی می‌کند.

لایه جلسه Session Layer

لایه جلسه Session یا همان لایه ۵ وظیفه اضافه کردن اطلاعاتی را به بسته دارد که باعث می‌شود یک جلسه ارتباطی بین یک سرویس یا اپلیکیشن در دستگاه منبع با همان سرویس یا اپلیکیشن در دستگاه مقصد امکان پذیر باشد. این فرآیند را با روشی که جلسه‌ای بین دو دستگاه فیزیکی برقرار می‌شود، اشتباه نگیرید. این عمل نه تنها در این لایه بلکه در لایه‌های ۳ و ۴ رخ می‌دهد. این جلسه پس از انجام جلسه فیزیکی بین رایانه‌ها ساخته شده و بسته می‌شود.

اپلیکیشن یا سرویس مورد استفاده بین دو سیستم با شناسه‌ای به نام شماره پورت ارتباط برقرار می‌کند. این اطلاعات به لایه Transport منتقل می‌شود و از این شماره‌های پورت نیز استفاده می‌کند.

لایه انتقال Transport Layer

پروتکل‌ها در لایه Transport یا لایه ۴ کار می‌کنند تا جلسه‌ای بین دو سیستم فیزیکی برقرار شود. خدمات ارائه شده می‌توانند بستگی به پروتکل انتقال مورد استفاده، به صورت اتصال گرا Connection-oriented یا بدون اتصال Connectionless باشند.

بخش "TCP/IP Model" رایج ترین مجموعه پروتکل استاندارد شبکه بکارگرفته شده در پروتکل‌های انتقال خاص مورد استفاده TCP / IP را با جزئیات بیشتر مورد بحث قرار می‌گیرد.

لایه Transport تمام اطلاعات را از لایه‌های ۷، ۶، ۵ دریافت می‌کند و اطلاعات پروتکل انتقال در حال استفاده را مشخص کرده و شماره پورت خاصی را که پروتکل لایه ۷ مورد نیاز را مشخص می‌کند، اضافه می‌کند. در این لایه، PDU یک قطعه یا سگمنت نامیده می‌شود زیرا این لایه یک انتقال بزرگی را گرفته و آن را به قطعات کوچکتر تقسیم می‌کند تا برای انتقال کارآمدتر روی محیط استفاده شود.

لایه شبکه Network Layer

در لایه ۳ یا لایه شبکه، اطلاعات موردنیاز برای مسیر یابی بسته اضافه می‌شود. این به صورت آدرس منطقی مبدأ و مقصد است (به معنای آدرسی که به یک دستگاه اختصاص داده شده و قابل تغییر است). در TCP / IP، از نظر آدرس IP مبدأ و مقصد است. آدرس IP شماره‌ای است که به طور جداگانه میزبان را از سایر دستگاه‌های شبکه متمایز می‌کند. این مبتنی بر یک سیستم شماره گذاری است که باعث می‌شود رایانه‌ها (و روترها) امکان شناسایی دستگاه مقصد در شبکه محلی یا یک شبکه از راه دور را داشته باشند. هر زمان که یک بسته نیاز به شبکه یا زیر شبکه دیگری برای ارسال داشته باشد (آدرس IP در قسمت بعدی قرار دارد)، باید مسیریابی شود و اطلاعات مورد نیاز برای انجام این کار اضافه شود. در این لایه، PDU را بسته Packet نیز می‌گویند.

لایه پیوند داده Data Link Layer

لایه Data Link یا همان لایه ۲ وظیفه تعیین آدرس فیزیکی مقصد را دارد. دستگاه‌های شبکه دارای آدرس‌های منطقی (آدرس‌های IP) هستند و واسطه‌های شبکه‌ای که در اختیار دارند دارای یک آدرس فیزیکی (یک آدرس دسترسی به رسانه‌ها MAC) هستند که از نظر ماهیت دائمی

هستند. هنگامی که انتقال از دستگاه مسیریابی به دستگاهی دیگر منتقل می‌شود، در هر توقف، جفت آدرس مبدأ و مقصد تغییر می‌کند، در حالی که آدرس‌های منطقی مبدأ و مقصد (در بیشتر موارد آدرس‌های IP) ندارند.

این لایه وظیفه مشخص کردن آنچه را که آدرسهای MAC در هر هاپ (رابط روتر) قرار داده و همچنین اضافه کردن آنها به این قسمت از بسته را دارد. بخش بعدی "TCP/IP Model" نحوه عملکرد در TCP / IP را نشان می‌دهد. پس از انجام این کار، PDU را فریم نیز می‌نامیم. در برخی از شبکه‌ها، لایه Data Link از جمله کنترل دسترسی رسانه‌ها (MAC) و زیرمجموعه‌های کنترل پیوند منطقی (LLC) بحث شده است. در لایه Data Link، پروتکل IEEE 802.2 LLC با همه لایه‌های IEEE 802 MAC قابل استفاده است.

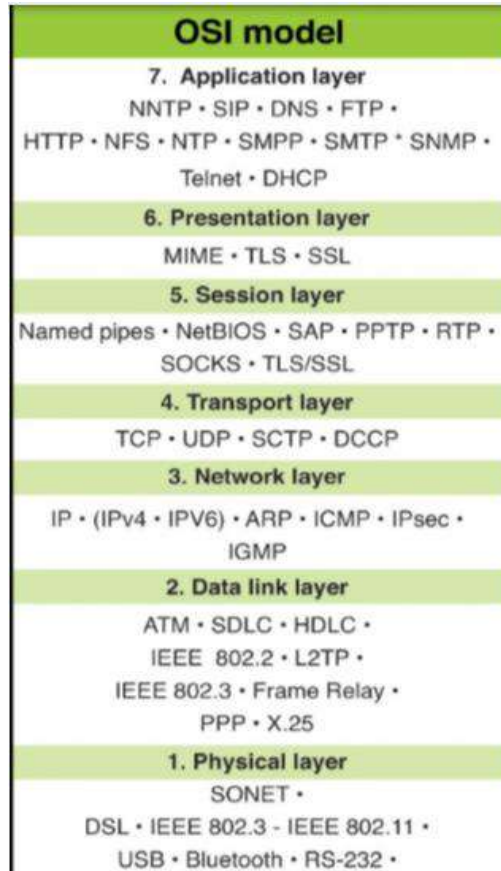
اتفاق دیگری که مخصوص این لایه است. نه تنها یک هدر در لایه ۲ روی بسته قرار می‌گیرد، بلکه یک تریلر نیز در قسمت انتهای فریم وجود دارد. از اطلاعات موجود در این تریلر برای تأیید اینکه هیچ یک از داده‌های موجود مسیر تغییر نیافته یا آسیب ندیده است، استفاده می‌شود.

لایه فیزیکی Physical Layer

سرانجام، بسته یا فریم، (همانطور که در لایه ۲ گفته می‌شود) توسط لایه Physical لایه ۱ دریافت می‌شود. لایه ۱ وظیفه تبدیل اطلاعات به بیت (صفرها و یکها) و ارسال آن روی رسانه را دارد. نحوه دستیابی به این امر می‌تواند با توجه به رسانه مورد استفاده متفاوت باشد. به عنوان مثال، در یک شبکه سیمی، صفرها و یکها به عنوان بار الکتریکی نشان داده می‌شوند. در شبکه بی سیم، با تغییر امواج رادیویی نمایش داده می‌شوند. در یک شبکه نوری، با نور نمایش داده می‌شوند. توانایی مسیریابی همان بسته از طریق رسانه‌های مختلف، نمونه خوبی از استقلال لایه‌ها است. با حرکت PDU از طریق انواع مختلف رسانه، لایه فیزیکی تغییر خواهد کرد اما تمام اطلاعات موجود در لایه‌های ۲ تا ۷ نخواهد بود. به طور مشابه، هنگامی که یک فریم از روترها یا هاپ عبور می‌کند، آدرس‌های MAC تغییر می‌کنند اما هیچ یکی از اطلاعات در لایه‌های ۳ تا ۷ تغییر نمی‌کند. لایه‌های بالایی برای خدمات مختلف به لایه‌های پایین بستگی دارد، اما لایه‌های پایین اطلاعات لایه بالایی را بدون تغییر می‌گذارند.

شکل ۴-۱ پروتکل‌های معمول ترسیم شده در مدل OSI را نشان می‌دهد. از آنجا که TCP / IP استاندارد فعلی برای انتقال است، مقایسه این دو مدل مفید است. اگرچه تعداد لایه‌های مختلفی

دارند و برخی از اسامی لایه ها با هم متفاوت هستند، اما روند یکسویه ایجاد بسته یا کپسوله سازی را توصیف می کنند.

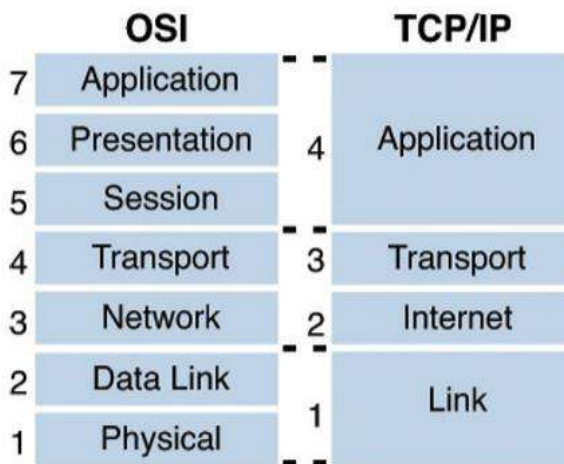


شکل ۴-۱: نقشه برداری پروتکل

مدل TCP / IP

پروتکلها هنگام توسعه مدل OSI که بعضاً به عنوان پروتکل OSI خوانده می شوند، استاندارد برای اینترنت نبودند. همانطور که امروزه می دانیم اینترنت ریشه در یک شبکه وسیع WAN دارد که توسط وزارت دفاع آمریکا (DOD) تهیه شده است و TCP / IP پروتکل تهیه شده برای آن شبکه است. اینترنت شبکه ای جهانی شامل شبکه های عمومی و ارائه دهندگان خدمات اینترنت ISP در سراسر جهان است. این مدل شباهت های بسیاری با مدل OSI دارد، که غیر منتظره

نیست زیرا آنها هر دو روند ایجاد بسته یا کپسوله سازی را توصیف می کنند. تفاوت در این است که مدل OSI فرایند را به هفت لایه تقسیم بندی می کند، در حالی که مدل TCP / IP آن را به چهار لایه تقسیم می کند. اگر آنها را در کنار هم بررسی کنید، آشکار می شود که بسیاری از عملکردهای مشابه در لایه ها اتفاق می افتند، در حالی که مدل TCP / IP سه لایه برتر مدل OSI را در یک و دو لایه پایین OSI ترکیب می کند. شکل ۴-۲ این دو مدل را در کنار یکدیگر نشان می دهد.



شکل ۴-۲: مدل های OSI و TCP / IP

مدل TCP / IP تنها چهار لایه دارد، در این بخش به بررسی چهار لایه و عملکردها و روابط آنها با یکدیگر و لایه هایی در مدل OSI می پردازیم.

لایه کاربردی Application Layer

اگرچه لایه Application در مدل TCP / IP به نام لایه بالایی در مدل OSI و به همان نام است، لایه Application در مدل TCP / IP شامل تمام عملکردهای انجام شده در لایه های ۵ تا ۷ در مدل OSI است. همه نقشه عملکردشان کامل نیستند زیرا هر دو مدل صرفاً مفهومی هستند. در داخل لایه کاربردی، اپلیکیشن ها داده های کاربر را ایجاد می کنند و این داده ها را به سایر فرآیندها یا اپلیکیشن های میزبان دیگر انتقال می دهند. به همین دلیل، گاهی اوقات به عنوان لایه فرآیند به فرآیند Process-to-Process نیز گفته می شود.

نمونه هایی از پروتکل هایی که در این لایه کار می کنند SMTP ، SSH، FTP ، HTTP هستند. این پروتکل ها در بخش "پروتکل ها و خدمات" بعداً در این فصل مورد بحث قرار خواهد گرفت. با این حال، معمولاً به آن، پروتکل های لایه بالاتر نیز گفته می شود که عملکرد خاصی را انجام می دهند، در حالی که پروتکل های موجود در مجموعه TCP / IP که در لایه های انتقال و اینترنت کار می کنند، به نمایندگی از پروتکل های لایه بالاتر، مکان و خدمات تحویل را انجام می دهند. تعداد پورت این پروتکل های لایه بالاتر و برنامه هایی که از طرف آنها عملکردی دارند، به دستگاه دریافت کننده معرفی می شوند و شماره پروتکل یا سرویس را مشخص می کند. بسیاری از شماره های پورت استاندارد شده اند. به عنوان مثال، سیستم نام دامنه DNS با شماره پورت استاندارد ۵۳ مشخص می شود. بخش پورتهای مشترک TCP / UDP این شماره پورت ها را با جزئیات بیشتری پوشش می دهد.

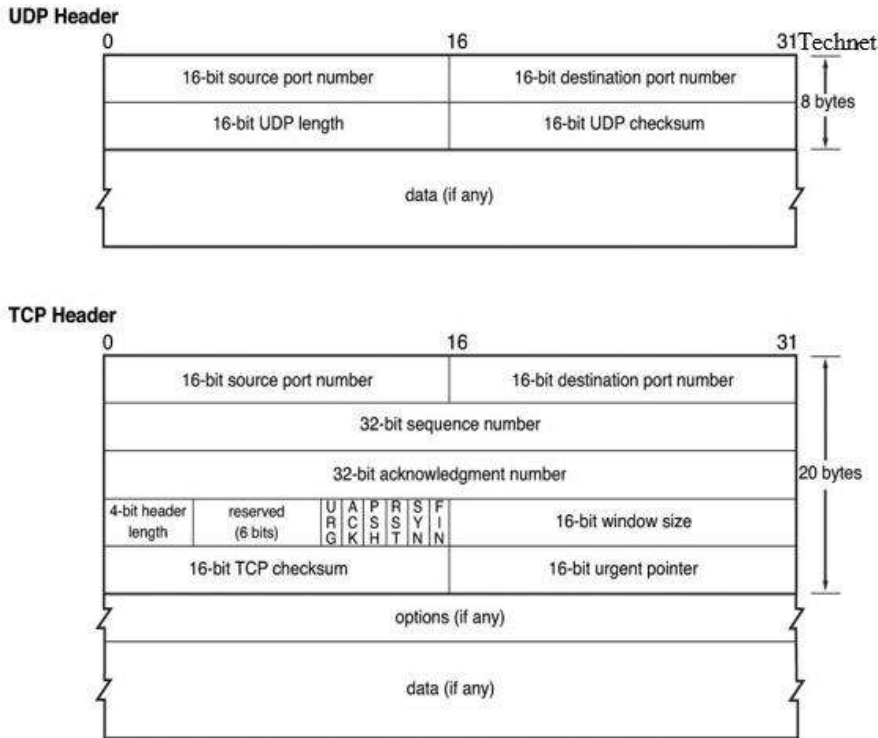
لایه انتقال Transport Layer

لایه های انتقال مدل OSI و مدل TCP / IP عملکرد مشابهی را انجام می دهند، یعنی باز کردن و حفظ ارتباط بین میزبانها. باید قبل از شروع جلسه بین فرآیندها اتفاق بیفتد، همانطور که در بخش لایه کاربردی نیز توضیح داده شده، می تواند انتقال در TCP / IP از دو طریق انجام شود: بدون اتصال و اتصال گرا Connectionless و Connection-oriented. انتقال اتصال گرا به این معنی است که قبل از انتقال هرگونه داده، اتصال برقرار می شود، در حالی که در انتقال بدون اتصال این کار انجام نمی شود. یکی از دو پروتکل مختلف لایه انتقال برای هر فرآیند استفاده می شود. اگر یک پروتکل انتقال اتصال گرا مورد نیاز باشد، از پروتکل کنترل انتقال (TCP) استفاده می شود. اگر این روند بدون اتصال باشد، از پروتکل User Datagram Protocol (UDP) استفاده می شود.

توسعه دهندگان اپلیکیشن می توانند از TCP یا UDP به عنوان پروتکل لایه انتقال به کار برده شده توسط اپلیکیشن استفاده کنند. علی رغم پروتکل انتقال بکاربرده شده، اپلیکیشن یا خدمات توسط شماره درگاه و پروتکل انتقال TCP یا UDP برای دستگاه گیرنده شناسایی می شود.

اگرچه TCP عملکرد و قابلیت اطمینان بیشتری را فراهم می کند، اما در مقایسه با UDP سربار مورد نیاز این پروتکل، قابل توجه می باشد. این بدان معنی است که درصد بسیار بیشتری از بسته در هنگام استفاده از TCP از هدر تشکیل می شود تا هنگام استفاده از UDP.

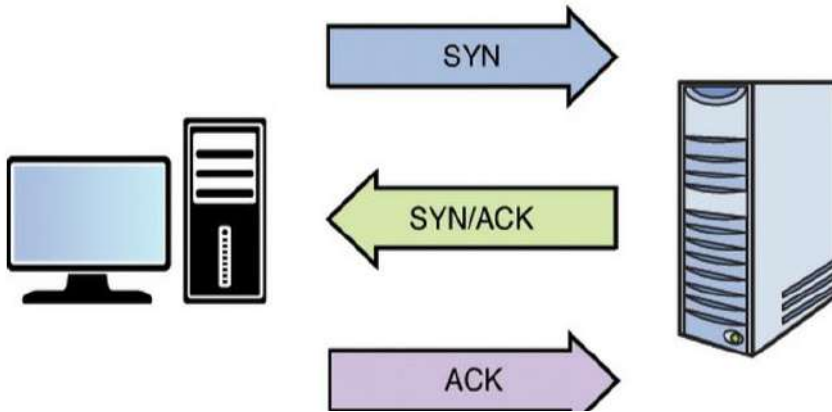
این امر برای فراهم کردن زمینه های مورد نیاز برای نگهداری اطلاعات مورد نیاز برای ارائه خدمات اضافی لازم است. شکل ۴-۳ مقایسه های بین اندازه دو هدر مربوطه را نشان می دهد.



شکل ۴-۳: هدرهای IP / TCP و UDP

هنگامی که یک اپلیکیشن برای استفاده از TCP نوشته شده است، قبل از انتقال هر گونه داده، اتصال بین دو میزبان برقرار می‌شود. این با استفاده از فرایندی که به عنوان دسته‌ی ۳ مرحله‌ای (Three-Way Handshake) TCP شناخته می‌شود رخ می‌دهد. این فرآیند به طور دقیق دنبال شده، و هیچ داده‌ای تا زمان کامل شدن انتقال نمی‌یابد. شکل ۴-۴ مراحل این فرآیند را نشان می‌دهد. مراحل به شرح زیر است:

۱. رایانه اول بسته‌ای را با مجموعه پرچم SYN (یکی از فیلدهای هدر TCP) ارسال می‌کند، که نشان دهنده تمایل به ایجاد یک اتصال است.
۲. میزبان دریافت کننده، دریافت این بسته را تایید می‌کند و با فرستادن بسته‌ای با مجموعه‌ای از پرچم‌های SYN و ACK، تمایل به ایجاد یک حالت اتصال را نشان می‌دهد.
۳. میزبان اول با ارسال یک بسته نهایی فقط با مجموعه پرچم‌های ACK، تکمیل فرایند اتصال را تأیید می‌کند.



شکل ۴-۴: دستهدی سه طرفه TCP

بنابراین با استفاده از سربرار اضافی برای استفاده از TCP دقیقاً چه چیزی حاصل می‌شود؟ در زیر نمونه‌هایی از عملکردهای ارائه شده با TCP آورده شده است:

- ✓ تحویل تضمین شده Guaranteed Delivery: اگر میزبان گیرنده به طور خاص دریافت هر بسته را تأیید نکند، سیستم ارسال کننده بسته را دوباره ارسال می‌کند.
- ✓ توالی Sequencing: امروزه در شبکه‌های مسیریابی شده، بسته‌ها ممکن است مسیرهای مختلفی را برای رسیدن به گیرنده طی کنند و ممکن است به ترتیبی که ارسال شده اند، نرسند. تعداد دنباله اضافه شده به هر بسته اجازه می‌دهد تا میزبان گیرنده با استفاده از این اعداد، کل انتقال را مجدداً جمع کند.
- ✓ کنترل جریان Flow Control: میزبان گیرنده قابلیت ارسال بسته‌های تصدیق Acknowledgement Packets را به شما می‌دهد تا اگر نتواند بسته‌های آن را به همان سرعتی که می‌رسند پردازش کند به فرستنده سیگنال دهد تا انتقال را به کندی انجام دهد.

بسیاری از اپلیکیشن‌ها به خدمات ارائه شده توسط TCP احتیاج ندارند و نمی‌توانند سربرار مورد نیاز TCP را تحمل کنند. در این موارد، از UDP استفاده می‌شود، که بدون هیچ گونه ضمانت تحویل، بر اساس "بهترین تلاش Best Effort" عملیات ارسال را انجام می‌دهد. در بسیاری موارد، برخی از این عملکردها به جای تکیه بر پروتکل لایه Transport، توسط پروتکل لایه Application ارائه می‌شوند.

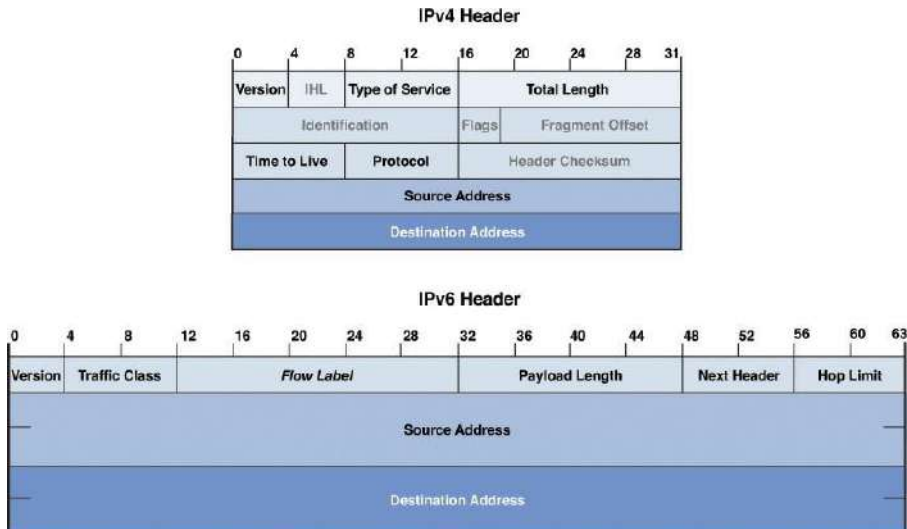
لایه اینترنت Internet Layer

لایه انتقال نمی‌تواند حالت اتصال برقرار کند و با استفاده از UDP ارسال شود، تا زمانی که مکان و مسیر مقصد تعیین شود، که در لایه اینترنت رخ می‌دهد. چهار پروتکل در مجموعه TCP / IP که در این لایه کار می‌کنند عبارتند از:

- پروتکل اینترنت (IP) Internet Protocol مسئول قرار دادن آدرس‌های IP منبع و مقصد در بسته، برای مسیریابی بسته به مقصد است.
 - پروتکل کنترل پیام اینترنت (ICMP) Internet Control Message Protocol توسط دستگاه‌های شبکه برای ارسال پیام در مورد موفقیت یا عدم موفقیت در ارتباطات استفاده می‌شود و همچنین توسط انسان برای عیب‌یابی استفاده می‌شود. وقتی از دستورات PING یا TRACEROUTE / TRACERT استفاده می‌کنیم، از ICMP استفاده می‌شود.
 - پروتکل مدیریت گروه اینترنت (IGMP) Internet Group Management Protocol : هنگام استفاده از Multicasting، که نوعی ارتباط است که به وسیله آن یک میزبان به جای یک میزبان واحد به نام انتقال Unicast، برای همه میزبان‌ها به نام انتقال Broadcast، به گروهی از میزبان‌های مقصد ارسال شده و مورد استفاده قرار می‌گیرد. سه نسخه IGMP وجود دارد. نسخه ۲ دو نوع پرس و جو (Query) اضافه می‌کند: پرس و جو عمومی و پرس و جو اختصاصی گروه و نسخه ۳ پرس و جو عضویت را اضافه می‌کند.
 - پروتکل تفکیک آدرس (ARP) Address Resolution Protocol: آدرس IP قرار داده شده در بسته را به یک آدرس فیزیکی (که به آن آدرس MAC در اترنت گفته می‌شود) تجزیه می‌کند.
- رابطه IP و ARP شایسته بحث بیشتری می‌باشد. IP، آدرس‌های مبدا و مقصد را در هدر بسته قرار می‌دهد. همانطور که قبلاً دیدیم، وقتی یک بسته در یک شبکه قرار می‌گیرد، آدرس‌های IP مبدا و مقصد هرگز تغییر نمی‌کنند اما لایه ۲ یا آدرس‌های MAC در هر روتر تغییر می‌کنند. ARP از فرآیندی به نام پخش ARP Broadcast برای یادگیری واسط آدرس MAC مطابق با آدرس IP هاپ بعدی استفاده می‌کند. بعد از انجام این کار، هدر لایه ۲ جدید ایجاد می‌شود. باز هم، هیچ چیز دیگری در لایه بالاتر در این فرآیند تغییر نمی‌کند، به استثنا لایه ۲.

این نکته خوبی را در مورد نقشه برداری ARP در مدل TCP / IP ایجاد می کند. اگرچه ما معمولاً ARP را در لایه اینترنت قرار می دهیم، اطلاعاتی که از این فرآیند حاصل می شود در لایه پیوند یا لایه ۲ می باشد، که در لایه بعدی مورد بحث قرار می گیرد.

درست همانطور که لایه Transport یک هدر به بسته اضافه می کند، لایه اینترنت نیز همین کار را انجام می دهد. یکی از پیشرفتهای IPv6، ساده سازی هدر IP است. اگرچه همان اطلاعات در هدر موجود است و هدر بزرگتر است، اما ساختار بسیار ساده تری دارد. شکل ۴-۵ مقایسه این دو را نشان می دهد.



شکل ۴-۵: هدرهای IPv4 و IPv6

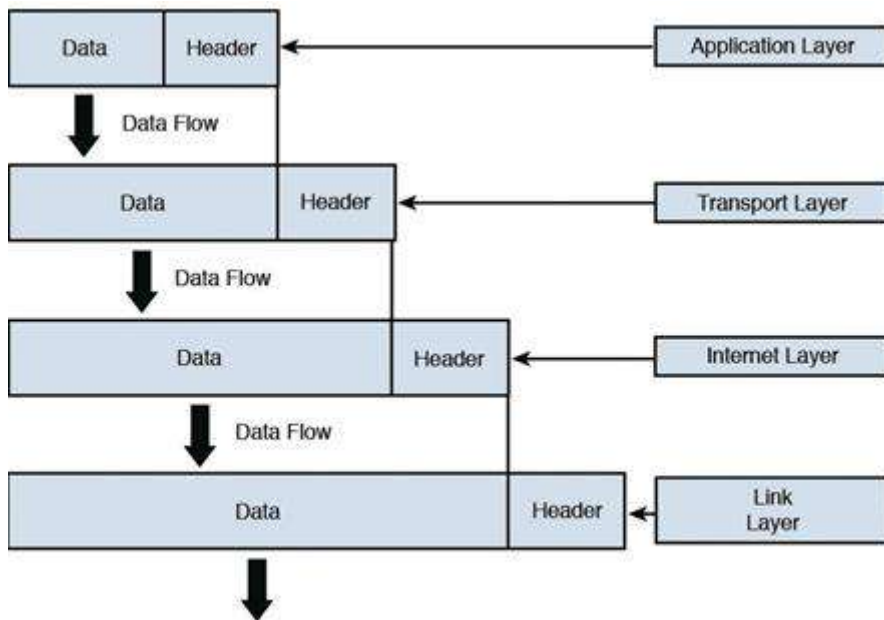
لایه پیوند Link Layer

مدل TCP / IP، لایه پیوند لایه Network Access نیز نامیده می شود و خدمات ارائه شده توسط لایه پیوند و لایه های فیزیکی در مدل OSI را ارائه می دهد. آدرس های MAC مبدا و مقصد در هدر این لایه قرار می گیرند. یک تریلر نیز در این لایه بر روی بسته قرار داده شده است و اطلاعاتی در این تریلر وجود دارد که می تواند برای تأیید یکپارچگی داده ها از آن استفاده شود. همانطور که در بخش مدل OSI در اوایل این فصل بحث شد، این لایه همچنین مربوط به قرار دادن بیت ها در رسانه (Media) است. باز هم، روش دقیق اجرا با رسانه انتقال فیزیکی متفاوت

است. ممکن است از نظر ضربه‌های الکتریکی Electrical Impulses، امواج نور یا امواج رادیویی باشد.

کپسوله سازی Encapsulation

در هر مدل با ایجاد بسته، اطلاعات در هر لایه به هدر اضافه می‌شود و سپس پیش از انتقال، تریلر روی بسته قرار می‌گیرد. این فرآیند کپسوله سازی نامیده می‌شود. دستگاه‌های واسطه Intermediate devices مانند روترها و سوئیچ‌ها فقط لایه‌های مربوط به آن دستگاه را می‌خوانند (برای سوئیچ، لایه ۲ و برای روتر، لایه ۳). گیرنده نهایی کل هدر هر لایه را خاموش کرده و از اطلاعاتی که در هدر قرار دارد توسط لایه متناظر با دستگاه ارسال کننده استفاده می‌کند. این فرآیند تخریب کپسوله سازی De-Encapsulation نامیده می‌شود. شکل ۴-۶ یک نمایش تصویری از کپسوله سازی را نشان می‌دهد.



شکل ۴-۶: کپسوله سازی

IP Networking

اکنون که اصول طراحی امن و مدل های OSI و TCP / IP را درک کرده اید، وقت آن رسیده است تا عمیق تر به IP Networking بپردازیم. پروتکل اینترنت (IP) پروتکل اصلی ارتباطات در مجموعه TCP / IP است و وظیفه انتقال داده ها در مرزهای شبکه را بر عهده دارد. در این بخش پورت های مشترک TCP / UDP، آدرس دهی منطقی و فیزیکی، انتقال شبکه و انواع شبکه را در بر می گیرد.

پورتهای مشترک TCP / UDP

هنگامی که لایه Transport شماره پورت مورد نیاز سرویس یا اپلیکیشن مورد نیاز دستگاه مقصد را از لایه Application دریافت می کند، در هدر به عنوان شماره پورت TCP یا UDP ثبت می شود. هر دو UDP و TCP از ۱۶ بیت در هدر برای شناسایی این پورت ها استفاده می کنند این شماره درگاه ها مبتنی بر نرم افزار یا منطقی هستند که ۶۵۵۳۵ امکان وجود دارد. شماره پورت به روش های مختلف و بر اساس سه محدوده تعیین می شود:

✓ پورت های سیستم یا مشهور (0-1023)

✓ پورت های کاربر (1024-49151)

✓ پورت های پویا و / یا خصوصی (49152-65535)

پورت های سیستم طبق کارگاه RFC 6335 توسط کارگروه مهندسی اینترنت IETF برای پروتکل های ردیابی استاندارد اختصاص داده می شوند. پورت های کاربر را می توان در اداره شماره های اختصاص داده اینترنت IANA ثبت کرد و با استفاده از "بررسی تخصصی" مطابق با RFC 6335، به سرویس یا اپلیکیشن اختصاص داد. پورت های دینامیکی یا پویا هنگام دسترسی به یک سرویس یا اپلیکیشن در دستگاه دیگر، توسط دستگاه های مبدا به عنوان پورتهای مبدا استفاده می شوند. به عنوان مثال، اگر رایانه A یک بسته FTP را ارسال کند، پورت مقصد پورت سیستم یا مشهور برای FTP خواهد بود و مبدا توسط رایانه به طور تصادفی از محدوده دینامیکی یا پویا انتخاب می شود.

به ترکیبی از آدرس IP مقصد و شماره پورت مقصد، سوکت (Socket) گفته می شود. رابطه بین این دو مقدار را می توان در صورت مشاهده مثل یک آدرس ساختمان دفترکار درک کرد. این ساختمان دفترکار دارای آدرس خیابان است، اما آدرس باید دارای یک مجموعه اتاق باشد زیرا

ممکن است هزاران (در این حالت ۶۵۵۳۵) اتاق در ساختمان وجود داشته باشد. به هر دو مورد نیازی باشد تا اطلاعات از کجا بدست می‌آید.

به عنوان یک متخصص امنیت، باید از تعداد پورت‌های سیستم سرویس مشترک آگاه باشید. در بسیاری از موارد، قوانین فایروال و لیست‌های کنترل دسترسی (ACL) بر اساس شماره پورت آنچه به جای نام سرویس یا اپلیکیشن مجاز یا رد شده است، نوشته یا پیکربندی شده اند. در جدول ۴-۱ تعدادی از پورت‌های مهم تر ذکر شده است. برخی از آنها بیش از یک پورت استفاده می‌کنند.

Application Protocol	Transport Protocol	Port Number
Telnet	TCP	23
SMTP	UDP	25
HTTP	TCP	80
SNMP	TCP and UDP	161 and 162
FTP	TCP and UDP	20 and 21
FTPS	TCP	989 and 990
SFTP	TCP	22
TFTP	UDP	69
POP3	TCP and UDP	110
DNS	TCP and UDP	53
DHCP	UDP	67 and 68
SSH	TCP	22
LDAP	TCP and UDP	389
NetBIOS	TCP and UDP	137 (TCP), 138 (TCP), and 139 (UDP)
CIFS/SMB	TCP	445
NFSv4	TCP	2049
SIP	TCP and UDP	5060
XMPP	TCP	5222
IRC	TCP and UDP	194
RADIUS	TCP and UDP	1812 and 1813
rlogin	TCP	513
rsh and RCP	TCP	514
IMAP	TCP	143
HTTPS	TCP and UDP	443
RDP	TCP and UDP	3389
AFP over TCP	TCP	548

جدول ۴-۱ شماره‌های آدرس رایج TCP / UDP آدرس منطقی و فیزیکی

در طی فرآیند کپسوله سازی در لایه ۳ مدل OSI، IP آدرس های مبدا و مقصد را در بسته قرار می دهد. سپس در لایه ۲ آدرسهای MAC مبدا و مقصد مطابق با ARP تعیین شده در بسته قرار می گیرند. آدرس های IP نمونه هایی از آدرس دهی منطقی هستند و آدرس های MAC نمونه ای از آدرس های فیزیکی هستند. آدرس های IP منطقی تلقی می شوند زیرا این آدرس ها توسط انسان اداره می شوند و در هر زمان قابل تغییر هستند. از طرف دیگر آدرسهای MAC برای همیشه به کارتهای واسط دستگاهها اختصاص داده می شوند زمانیکه واسطها ساخته می شوند. البته توجه این نکته حائز اهمیت است که اگرچه این آدرس ها دائمی هستند اما می توانند از این طریق جعل شوند. با این حال، هنگامی که این کار انجام شد، هکر در واقع در حال تغییر آدرس فیزیکی نیست بلکه به واسط کاربری می گوید تا یک آدرس MAC متفاوت را در هدرهای لایه ۲ قرار دهد.

در این بخش هر دو نوع آدرس با تمرکز ویژه ای در مورد نحوه استفاده از آدرس های IP برای ایجاد شبکه های جداگانه یا زیر شبکه در شبکه بزرگتر مورد بحث قرار می گیرد. همچنین در مورد چگونگی ارتباط و استفاده از آدرس های IP و آدرس های MAC در هنگام انتقال شبکه بحث می شود.

IPv4

آدرس های IPv4 دارای ۳۲ بیت هستند و می توانند به صورت باینری (دودویی) یا به صورت نقطه ای اعشاری نمایش داده شوند. تعداد آدرس های IP ممکن با استفاده از ۳۲ بیت را می توان با بالا بردن شماره ۲ (تعداد مقادیر ممکن در سیستم شماره دودویی) به توان ۳۲ محاسبه کرد. نتیجه این ۴,۲۹۴,۹۶۷,۲۹۶ است که به نظر می رسد آدرس IP به اندازه کافی باشد. اما با انفجار اینترنت و افزایش تعداد دستگاه هایی که به آدرس IP نیاز دارند، این تعداد ثابت شده است که ناکافی می باشد.

با توجه به فرسودگی احتمالی فضای آدرس IPv4، روشهای مختلفی برای حفظ آدرسهای IP عمومی (بیشتر مورد آن روی یک بیت، اما در حال حاضر اینها آدرسهایی هستند که استفاده از آنها در اینترنت قانونی است) اجرا شده اند، از جمله استفاده از آدرس های خصوصی و ترجمه آدرس شبکه NAT، که در بخش های بعدی مورد بحث قرار می گیرد. راه حل نهایی تصویب IPv6 بود، یک سیستم جدیدتر که از ۱۲۸ بیت استفاده می کند و اجازه می دهد تا به اندازه کافی آدرس

IP برای هر مرد، زن و کودک در این سیاره وجود داشته باشد تا به اندازه کل فضای شماره گذاری IPv4 آدرس IP داشته باشد.

آدرس‌های IP که با فرمت نقطه‌ای دهگان اعشاری Dotted-Decimal نوشته می‌شوند، فرمی می‌باشد که معمولاً انسان‌ها با آنها کار می‌کنند که دارای چهار فیلد به نام اکتت‌ها و بوسیله نقاط از هم تفکیک شده اند. به هر فیلد یک اکتت Octet گفته می‌شود زیرا وقتی آدرس‌ها را با فرمت باینری مشاهده می‌کنیم، ۸ بیت را به صورت دودویی اختصاص می‌دهیم تا هر عدد دهگان را در قالب ارقام دهگان، نشان دهیم. بنابراین، اگر به آدرس 216.5.41.3 نگاهی بیندازیم، چهار عدد دهگان توسط نقاط تفکیک می‌شوند که در صورت مشاهده در دودویی یا باینری، هر کدام ۸ بیت را نشان می‌دهد. در زیر نسخه باینری همین آدرس وجود دارد:

۱۱۰۱۱۰۰۰,۰۰۰۰۰۱۰۱,۰۰۱۰۱۰۰۱,۰۰۰۰۰۰۱۱

۳۲ بیت در آدرس کل و ۸ بیت در هر اکتت وجود دارد.

ساختار آدرس دهی IPv4 باعث تقسیم شبکه به زیربخشهایی به نام زیر شبکه‌ها می‌شود. هر آدرس IP همچنین دارای مقدار همراهی لازم به نام ماسک زیر شبکه Subnet Mask است. از ماسک زیر شبکه برای مشخص کردن اینکه کدام قسمت از آدرس، قسمت شبکه و کدام قسمت میزبان است استفاده می‌شود. قسمت شبکه در سمت چپ آدرس مشخص می‌کند که نشان می‌دهد دستگاه در کدام شبکه قرار دارد در حالی که قسمت میزبان در سمت راست، دستگاه را در آن شبکه شناسایی می‌کند. شکل ۴-۷ بخش شبکه و میزبان سه کلاس پیش فرض آدرس IP را نشان می‌دهد.

Class A Subnet Mask	Network	Host	Host	Host
	255	0	0	0

Class B Subnet Mask	Network	Network	Host	Host
	255	255	0	0

Class C Subnet Mask	Network	Network	Network	Host
	255	255	255	0

شکل ۴-۷: بیت های شبکه و میزبان

وقتی سیستم IPv4 برای اولین بار ایجاد شد، فقط سه ماسک فرعی پیش فرض وجود داشت، و تنها سه اندازه شبکه داشت که بعداً ثابت شد که ناخوشایند بوده و باعث هدر رفتن آدرس های IP عمومی است.

سرانجام سیستمی به نام مسیریابی بین دامنه بدون کلاس Classless Inter-Domain Routing (CIDR) به تصویب رسید که از ماسک های زیر شبکه ای استفاده می کند که امکان می دهد تا زیر شبکه یا زیرمجموعه ها را از شبکه های امکان پذیر کلاس اصلی قبل از CIDR تهیه کند. CIDR فراتر از حد امتحان Cissp است اما ارزش دانستن آن را دارد.

می توانید اطلاعات بیشتری در مورد نحوه کار CIDR را در لینک زیر کسب کنید.

<http://searchnetworking.techtarget.com/definition/CIDR>

کلاس IP

Subnetting کلاسیک یا قبل CIDR پنج کلاس شبکه ایجاد کرد. هر کلاس طیف وسیعی از آدرس های IP را نشان می داد. جدول ۴-۲ پنج کلاس را نشان می دهد. فقط سه مورد اول A، B

و C برای دستگاههای شبکه اختصاصی استفاده می‌شود. محدوده دیگر برای استفاده ویژه می‌باشد.

Class	Range	Mask	Initial Bit Pattern of First Octet	Network/Host Division	Technet
Class A	0.0.0.0–127.255.255.255	255.0.0.0	01	net.host.host.host	
Class B	128.0.0.0–191.255.255.255	255.255.0.0	10	net.net.host.host	
Class C	192.0.0.0–223.255.255.255	255.255.255.0	11	net.net.net.host	
Class D	224.0.0.0–239.255.255.255	Used for multicasting			
Class E	240.0.0.0–255.255.255.255	Reserved for research			

جدول ۴-۲: آدرس دهی IP کلاسیک

همانطور که مشاهده می‌کنید، مقدار کلیدی که هنگام حرکت از یک کلاس به طبقه دیگر تغییر می‌کند، مقدار اوکت اول (اولی در سمت چپ) است. آنچه ممکن است فوراً آشکار نباشد اینست که وقتی از یک کلاس به کلاس دیگر می‌روید، خط تقسیم بین قسمت میزبان Host و قسمت شبکه Net نیز تغییر می‌کند. این جایی است که مقدار ماسک زیر شبکه وارد می‌شود. وقتی ماسک با آدرس‌های IP روی هم قرار می‌گیرد، هر اکتت در ماسک زیر شبکه که ۲۵۵ تایی می‌باشد یک قسمت شبکه است و هر اکتتی که در آن ۰ است یک قسمت میزبان است. مورد دیگر که باید به آن اشاره کنیم این است که هر کلاس اولین دو بیت از اولین اکتت دارای الگوی مشخصی است. به عنوان مثال، هر آدرس IP که در موقعیت‌های بیت اول از ۰۱ شروع می‌شود باید در کلاس A باشد، همانطور در جدول ۴-۲ ذکر شده است.

اهمیت قسمت شبکه این است که دو دستگاه باید مقادیر یکسان را در قسمت شبکه به اشتراک بگذارند تا در یک شبکه باشند. اگر این کار را نکنند، قادر به برقراری ارتباط نخواهند بود.

آدرسهای عمومی در مقابل آدرسهای IP خصوصی Public Versus Private IP Addresses

راه حل اولیه مورد استفاده (هنوز در حال استفاده) برای رفع فرسودگی فضای IPv4 شامل استفاده از آدرس‌های خصوصی و NAT است. سه محدوده آدرس IP کنار گذاشته شد تا فقط در

شبکه‌های خصوصی مورد استفاده قرار گیرد که در اینترنت قابل رویت نیست. RFC 1918 محدوده آدرس IP خصوصی را در جدول ۳-۴ تنظیم کرده است تا برای این منظور استفاده شود. از آنجا که این آدرس‌ها در شبکه عمومی قابل رویت نیستند، آنها باید قبل از ارسال به اینترنت به آدرس‌های عمومی ترجمه شوند.

Class	Range
Class A	10.0.0.0–10.255.255.255
Class B	172.16.0.0–172.31.255.255
Class C	192.168.0.0–192.168.255.255

جدول ۳-۴: دامنه‌های آدرس IP خصوصی

ترجمه آدرس شبکه (NAT) Network address translation

ترجمه آدرس شبکه (NAT) خدماتی است که می‌تواند توسط روتر یا سرور تهیه شود. دستگاهی که خدمات را ارائه می‌دهد بین LAN و اینترنت قرار دارد. وقتی بسته‌ها باید به اینترنت بروند، ابتدا بسته‌ها از طریق سرویس NAT بکارگرفته می‌شوند. سرویس NAT آدرس IP خصوصی را به یک آدرس عمومی که در اینترنت قابل رویت است تغییر می‌دهد. وقتی پاسخ از وب برگردانده شد، سرویس NAT آن را دریافت می‌کند، آدرس را به آدرس IP خصوصی اصلی برگردانده و آن را به مبدأ می‌فرستد.

این ترجمه می‌تواند به صورت یک به یک انجام شود (یک آدرس خصوصی به یک آدرس عمومی)، اما برای ذخیره آدرس‌های IP، معمولاً سرویس NAT تمام شبکه خصوصی را با یک آدرس IP عمومی نشان می‌دهد. به این فرآیند ترجمه آدرس پورت (Port Address Translation (PAT گفته می‌شود. این نام از آنجا ناشی می‌شود که سرویس NAT با ثبت آدرس خصوصی و شماره پورت منبع (معمولاً یک شماره منحصر به فرد) که هنگام ساخت بسته‌ها انتخاب شده اند، مشتری‌های خصوصی را از یکدیگر تفکیک می‌کنند.

اجازه دادن اطلاعات به نمایندگی از یک شبکه کامل (شاید هزاران رایانه) با یک آدرس عمومی منفرد در ذخیره آدرس‌های IP عمومی کاملاً مؤثر بوده است. با این حال، بسیاری از اپلیکیشن‌ها از طریق NAT عملکرد مناسبی ندارند و بنابراین هرگز به عنوان راه حل دائمی برای رفع کمبود آدرس‌های IP دیده نمی‌شود و راه حل IPv6 است.

IPv4 در مقابل IPv6

IPv6 بیشتر برای رفع مشکل مسئله فرسودگی فضای IPv4 ساخته شده است. اگرچه آدرس دهی خصوصی و استفاده از NAT به تاخیر غیر قابل اجتناب کمک کرده است، اما استفاده از NAT مجموعه مشکلات خاص خود را بوجود می‌آورد. سیستم IPv6 از ۱۲۸ بیت استفاده می‌کند، بنابراین تعداد زیادی آدرس ممکن را ایجاد کرده که انتظار می‌رود در طول سالها، برای بسیاری از آنها کافی باشد.

جزئیات IPv6 فراتر از حد امتحان Cissp است اما این آدرس‌ها متفاوت از آدرس‌های IPv4 هستند زیرا از یک فرمت متفاوت و از سیستم شماره Hexadecimal استفاده می‌کنند، بنابراین حروف و اعدادی در آنها وجود دارد مانند آنچه در آدرس MAC مشاهده می‌شود، و هشت قسمت وجود دارد که توسط دو نقطه یا کالن جدا شده اند. در اینجا به عنوان مثال آدرس IPv6 آورده شده است:

2001:00000:4137:9e76:30ab:3035:b541:9693

بسیاری از ویژگیهای امنیتی که افزودنیهای IPv4 بودند مانند IPsec در IPv6 ساخته شده اند و باعث افزایش امنیت آن می‌شوند. علاوه بر این، در حالی که پروتکل پیکربندی Dynamic Host (DHCP) با IPv6 قابل استفاده است، امکان میزبانی روتر محلی خود، پیکربندی خود و کشف آدرس‌های IP همسایگان را در اختیار میزبان قرار می‌دهد. سرانجام، ترافیک پخش Broadcast Traffic به طور کامل در IPv6 از بین می‌رود و جایگزین ارتباطات Multicast می‌شود.

آدرس دهی MAC

همه بحثی که در مورد آدرس دهی تا کنون مورد توجه قرار گرفت در لایه ۳ اعمال می‌شود، یعنی آدرس IP.

در لایه ۲، آدرسهای فیزیکی قرار دارند. در اترنت به این آدرس ها، MAC گفته می‌شود، و به آنها آدرس فیزیکی نیز گفته می‌شود زیرا این آدرسهای ۴۸ بیتی که به صورت هگزادسیمال بیان شده اند، به طور دائم به واسطه‌های شبکه دستگاهها اختصاص داده می‌شوند. در اینجا مثالی از آدرس

MAC آورده شده است 01:23:45:67:89:ab

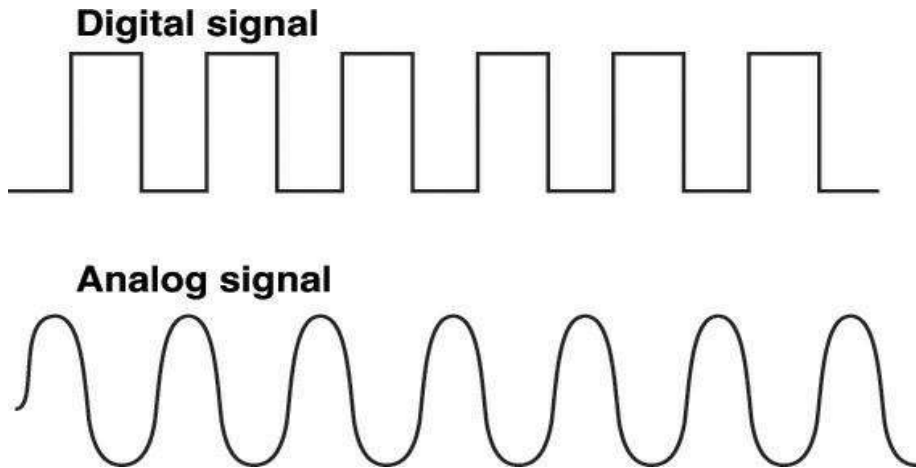
با انتقال بسته در یک شبکه، در هر روتر و سپس دوباره هنگام ورود به شبکه مقصد، آدرس های MAC مبدأ و مقصد تغییر می کنند. با استفاده از فرآیندی به نام ARP Broadcast، آدرس هاپ بعدی را به آدرس MAC تبدیل می کند. آدرس های MAC منحصر به فرد هستند. و از این واقعیت ناشی می شود که هر تولید کننده مجموعه ای از مقادیر متفاوتی را در ابتدای آدرس به نام شناسه سازمانی منحصر به فرد (Organizationally Unique Identifier (OUI را به آن اختصاص داده است. هر تولید کننده اطمینان می دهد که هیچ نسخه ای در OUI خود اختصاص نمی دهد. OUI سه بایت اول آدرس MAC می باشد.

انتقال شبکه Network Transmission

با استفاده از چندین فرآیند ممکن، داده ها می توانند با انواع مختلف رسانه ها ارتباط برقرار کنند. این ارتباطات همچنین می تواند دارای چندین ویژگی باشد که باید درک شوند. در این بخش برخی از رایج ترین روش ها و ویژگی های آنها مورد بحث قرار می گیرد.

آنالوگ در مقابل دیجیتال Analog Versus Digital

داده ها را می توان به روش های مختلف در یک رسانه نشان داد. در یک رسانه سیمی، داده ها می توانند به صورت آنالوگ یا دیجیتال منتقل شوند. آنالوگ داده ها را به صورت صوت Sound نشان می دهد، در تلفن آنالوگ استفاده می شود. سیگنال های آنالوگ با دیجیتال تفاوت دارند زیرا تعداد نامحدودی از مقادیر ممکن است. اگر به یک سیگنال آنالوگ روی یک نمودار نگاه کنید، به نظر می رسد که موج از بالا به پایین می رود. شکل ۴-۸ یک شکل موج آنالوگ را نسبت به شکل دیجیتال نشان می دهد.



شکل ۴-۸: سیگنال‌های دیجیتال و آنالوگ

سیگنال دیجیتال از طرف دیگر، که مورد استفاده در بیشتر انتقال‌های رایانه‌ای می‌باشد، دارای تعداد نامحدودی از مقادیر ممکن نیست، بلکه فقط دو مورد است: روشن و خاموش. در شکل ۴-۸، یک سیگنال دیجیتال که بر روی نمودار نشان داده شده است، مثل الگوی اره دندانه دار است. سیگنال‌های دیجیتال معمولاً نسبت به آنالوگ ارجحیت دارد زیرا آنها قابل اطمینان تر و حساسیت کمتری نسبت به نویز روی خط دارند و انتقال اطلاعات بیشتر در همان خط با کیفیت بالاتر، و در مسافت طولانی تر نسبت به آنالوگ نیز امکان پذیر می‌باشد.

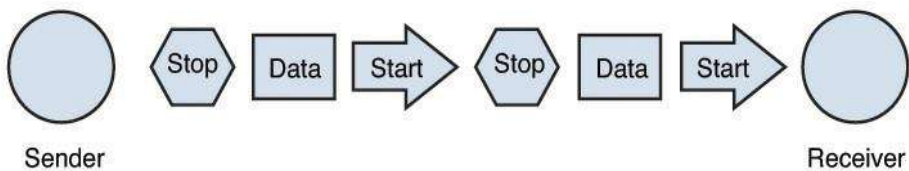
ناهمگام در مقابل همگام Asynchronous Versus Synchronous

وقتی دو سیستم در حال برقراری ارتباط هستند، نه تنها نیاز به نمایش داده‌ها در یک قالب مشابه (آنالوگ / دیجیتال) دارند بلکه باید از همان تکنیک همگام سازی استفاده کنند. این فرآیند به گیرنده، زمانی که یک ارتباط خاص شروع می‌شود و پایان می‌یابد را می‌گوید، بنابراین مکالمات دو طرفه می‌توانند بدون صحبت کردن روی یکدیگر اتفاق بیفتند. دو نوع تکنیک شامل انتقال ناهمگام و انتقال همگام می‌باشد.

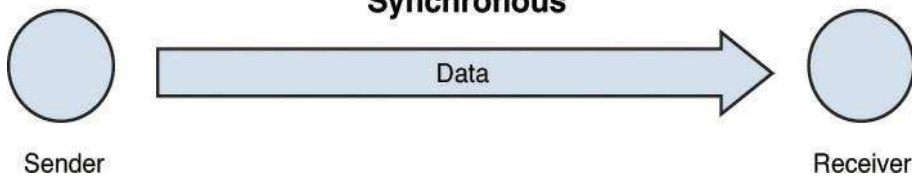
با انتقال ناهمگام، سیستم‌ها از بیت‌های شروع و توقف (Start, Stop) برای برقراری ارتباط هنگام شروع و توقف هر بایت استفاده می‌کنند. این روش همچنین از بیت‌های یکسان Parity Bits برای اطمینان از عدم تغییر هر بایت یا خراب شدن در مسیر استفاده می‌کند و این سربار اضافی را به گیرنده انتقال می‌دهد.

انتقال همگام از یک مکانیزم ساعت برای همگام سازی فرستنده و گیرنده استفاده می کند. داده ها در یک جریان از بیت ها بدون شروع، بدون توقف یا بدون بیت یکسان منتقل می شوند. این مکانیزم ساعت در پروتکل لایه ۲ تعبیه شده است. از فرم متفاوتی برای بررسی خطا (بررسی افزونگی چرخه ای یا CRC) استفاده می کند و برای انتقال های پر سرعت و با حجم زیاد ارجحیت دارد. شکل ۴-۹ مقایسه تصویری این دو روش را نشان می دهد.

Asynchronous



Synchronous



شکل ۴-۹: ناهمزمان در مقابل همزمان

باند گسترده در مقابل پهنای باند Broadband Versus Baseband

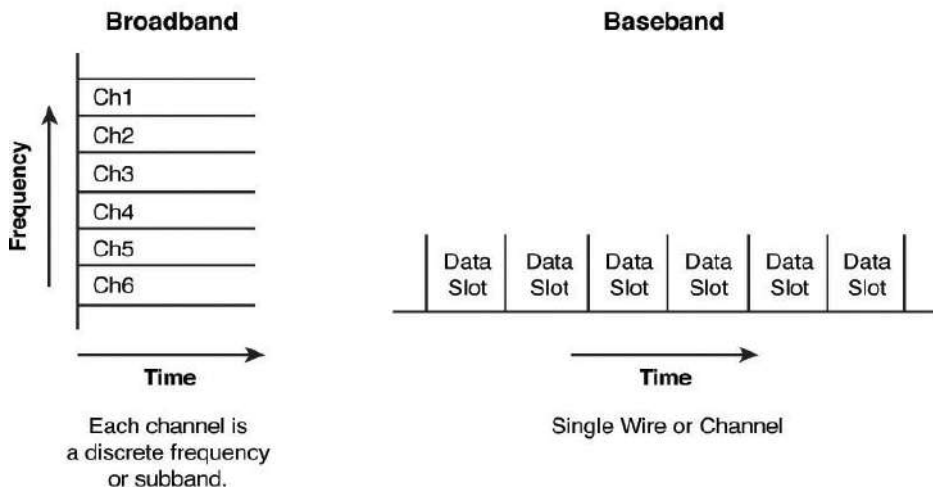
همه انتقال داده ها از یک کانال ارتباطی استفاده می کنند. انتقال چندگانه ممکن است نیاز به استفاده از همان کانال داشته باشد. اشتراک این رسانه به دو روش مختلف قابل انجام است: Broadband یا Baseband، که تفاوت در نحوه اشتراک رسانه می باشد.

در پهنای باند Baseband، از کل رسانه برای یک انتقال واحد استفاده می شود و پس از آن به انواع مختلف انتقال، اسلات زمانی برای استفاده از این مدار واحد اختصاص داده می شود. به این روش Time Division Multiplexing (TDM) گفته می شود، Multiplexing فرآیند استفاده از همان رسانه برای انتقال های متعدد است. ارسالها به جای ارسال همزمان در یک نوبت صورت می گیرند.

از طرف دیگر باند گسترده Broadband، رسانه را در فرکانس‌های مختلف تقسیم می‌کند، فرایندی به نام Frequency Division Multiplexing (FDM) این مزیت را دارد که اجازه استفاده همزمان از رسانه را می‌دهد.

نمونه‌ای از انتقال باند گسترده Broadband، خط مشترک دیجیتال Digital Subscriber Line (DSL) است که در آن سیگنال‌های تلفن با یک فرکانس و داده‌های رایانه روی فرکانس دیگری ارسال می‌شود. به همین دلیل است که می‌توانید همزمان با تلفن صحبت کرده و از وب استفاده کرد. شکل ۴-۱۰ این دو فرآیند را نشان می‌دهد.

Broadband versus Baseband



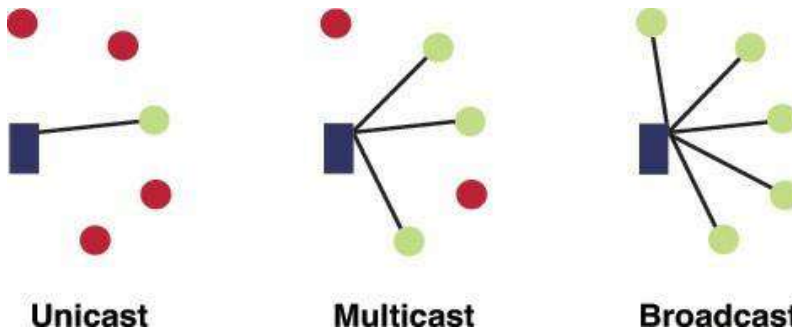
شکل ۴-۱۰: باند گسترده در مقابل پهنای باند

Broadcast, Multicast, Unicast

هنگامی که سیستم‌ها در یک شبکه ارتباط برقرار می‌کنند، ممکن است سه نوع انتقال را ارسال کنند. این روشها از نظر میزان پذیرش آنها به شرح زیر است:

- ✓ **Unicast** انتقال از یک سیستم به سیستم واحد دیگر. یک به یک به حساب می‌آید.
- ✓ **Multicast** یک سیگنال توسط همه افراد در گروهی به نام گروه چند مرحله‌ای دریافت می‌شود. این یک به چند نفر در نظر گرفته می‌شود.
- ✓ **Broadcast** انتقال ارسال شده توسط یک سیستم واحد به کلیه سیستمهای شبکه. این یک به همه در نظر گرفته می‌شود.

شکل ۴-۱۱ سه روش را نشان می دهد.



شکل ۴-۱۱: Unicast, Multicast, Broadcast

سیم در مقابل بی سیم Wired Versus Wireless

همانطور که احتمالاً می دانید، تمام انتقال ها از طریق اتصال سیمی اتفاق نمی افتد. حتی در رده اتصالات سیمی، نحوه نمایش صفرها و یکها به روشهای مختلفی قابل انجام است. در یک سیم مسی، یکها و صفرها با تغییر در ولتاژ سیگنال نشان داده می شوند، در حالی که در یک کابل فیبر نوری، با دستکاری یک منبع نور (لیزر یا دیودهای تابشگر LED) ارائه می شوند.

در انتقال بی سیم، امواج رادیویی یا امواج نور برای نشان دادن صفرها و یکها دستکاری می شوند. هنگامی که از فناوری مادون قرمز استفاده می شود، این کار با نور مادون قرمز انجام می شود. با استفاده از شبکه های بی سیم WLAN، امواج رادیویی برای نمایش صفرها و یکها دستکاری می شوند. این تفاوت ها در نحوه نمایش بیت ها در لایه پیوند داده و لایه فیزیکی مدل OSI رخ می دهد. وقتی یک بسته از یک بخش بی سیم شبکه به یک بخش سیمی می رود، این دو لایه تنها لایه هایی هستند که تغییر می کنند.

هنگامی که از یک محیط فیزیکی مختلف استفاده می شود، به طور معمول یک پروتکل لایه ۲ متفاوت فراخوانی می شود. به عنوان مثال، در حالی که داده ها از طریق شبکه سیمی اترنت عبور می کنند، از استاندارد ۸۰۲.۳ استفاده می شود. با این حال، هنگامی که داده ها به بخش بی سیم شبکه می رسند، به یک پروتکل لایه ۲ متفاوت نیاز دارد. با توجه به فن آوری مورد استفاده، می تواند (WLAN) 802.11 یا (WiMAX) 802.16 باشد.

توانایی بسته برای عبور از انواع مختلف رسانه‌ها تنها نشانه دیگری از استقلال لایه‌های OSI است. اطلاعات در لایه‌های ۳ تا ۷ بدون تغییر می‌باشند علیرغم اینکه چه تعداد انتقال لایه ۲ باید صورت گیرد تا اطلاعات به مقصد نهایی خود برسند.

انواع شبکه Network Types

تاکنون در مورد توپولوژی‌ها و فناوری‌های شبکه بحث کرده ایم، بنابراین اکنون بیا بید به روش سومی برای توصیف شبکه‌ها بپردازیم: نوع شبکه. نوع شبکه به دامنه شبکه اشاره دارد. آیا این یک شبکه LAN یا WAN است؟ آیا بخشی از شبکه داخلی است یا یک اکسترانت است؟ در این بخش انواع مختلف شبکه مورد بحث و تفکیک قرار می‌گیرد.

LAN

ابتدا اجازه دهید درباره آنچه شبکه محلی (LAN) را محلی می‌کند صحبت کنیم. اگرچه از نظر کلاسیک ما از شبکه محلی به عنوان شبکه‌ای که در یک مکان قرار دارد مانند یک اداره فکر می‌کنیم، مراجعه به شبکه LAN به عنوان گروهی از سیستم‌هایی که از طریق اتصال سریع متصل هستند صحیح‌تر است. هدف این بحث، ارتباطی با بیش از ۱۰ مگابیت بر ثانیه است. ممکن است خیلی سریع به نظر نرسد، اما با WAN مقایسه می‌شود. حتی یک اتصال T1 تنها ۱,۵۴۴ Mbps است. با استفاده از این معیار، اگر یک کمپ شبکه تنها یک اتصال WAN بین دو ساختمان داشته باشد، آنگاه این دو شبکه به جای یک LAN واحد به عنوان دو LAN در نظر گرفته می‌شوند. با این حال، در بیشتر موارد، شبکه‌ها در یک کمپ واحد معمولاً با اتصال WAN متصل نیستند، به همین دلیل معمولاً در یک مکان واحد، LAN به عنوان شبکه تعریف می‌شود.

اینترانت Intranet

در محدوده یک شبکه واحد، برای اهداف امنیتی می‌توان زیر مجموعه‌هایی ایجاد کرد. LAN ممکن است به یک اینترانت و یک اکسترانت تقسیم شود. اینترانت شبکه داخلی شرکت است. یک شبکه قابل اعتماد محسوب می‌شود و به طور معمول دارای هرگونه اطلاعات و سیستم‌های حساس است و باید حداکثر حفاظت را با دیواره آتش و مکانیزم‌های احراز هویت قوی داشته باشد.

اکسترانت Extranet

یک اکسترانت شبکه‌ای است که منطقاً از شبکه داخلی جداست و در آنجا منابعی که از خارج به آن دسترسی پیدا می‌کنند، موجود است. دسترسی ممکن است به مشتریان، شرکای کسب و کار و معمولاً به عموم مردم اعطا شود. کلیه ترافیک بین این شبکه و اینترنت باید از نزدیک کنترل و ایمن شود. هیچ چیزی از یک ماهیت حساس نباید در اکسترانت قرار گیرد.

MAN

شبکه کلانشهر (MAN) نوعی شبکه محلی است که منطقه بزرگی مانند مرکز شهر را در بر می‌گیرد. در بسیاری از موارد این ستون فقرات Backbone است که برای اتصال LAN ها به شبکه فراهم می‌شود. معمولاً در یک MAN از سه فناوری استفاده می‌شود:

✓ واسط داده فیبرنوری توزیع شده (FDDI) Fiber Distributed Data Interface

✓ شبکه نوری همزمان (SONET) Synchronous Optical Networking

✓ مترو اترنت Metro Ethernet

حلقه‌های FDDI و SONET که هر دو به کابل کشی از نوع فیبر نوری متکی هستند، می‌توانند مناطق بزرگی را به خود اختصاص دهند و کسب و کارها می‌توانند با استفاده از اتصالات T1، قسمت کوچکی از T1 (Fractional T1) یا اتصالات T3 به حلقه‌ها وصل شوند. همانطور که قبلاً دیدید، حلقه‌های FDDI یک حلقه مضاعف با تحمل خطا هستند. SONET نیز دارای سیستم خودبهبودی Self-healing است، به این معنی که اگر خط خراب شود، دارای یک حلقه دوبر با یک خط پشتیبان می‌باشد.

مترو اترنت Metro Ethernet استفاده از فناوری اترنت در یک منطقه گسترده است، که می‌تواند اترنت خالص یا ترکیبی از اترنت و فناوری‌های دیگر مثل فناوری‌های ذکر شده در این بخش باشد. اترنت سنتی (نوع مورد استفاده در شبکه LAN) از مقیاس پذیری کمتری برخوردار است، اغلب با فناوری Multiprotocol Label Switch (MPLS) ترکیب شده است، که قادر به حمل بسته‌های مختلف از جمله اترنت است.

MAN های با توانایی کمتر اغلب از MAN هایی با ظرفیت بالاتر تغذیه می‌شوند. از نظر مفهومی، می‌توان معماری MAN را به سه بخش تقسیم کرد: مشتری، تجمیع و لایه اصلی، Customer, Aggregation, Core layer. بخش مشتری، حلقه محلی است که از مشتری به شبکه تجمیع

متصل می‌شود، و سپس در هسته پر سرعت تغذیه می‌شود. هسته پر سرعت مجموع شبکه‌ها را به یکدیگر متصل می‌کند.

WAN

WANها برای اتصال LAN و MAN به یکدیگر استفاده می‌شوند. برای این اتصالات می‌توان از بسیاری از فناوری‌ها استفاده کرد. آنها از نظر ظرفیت و هزینه متفاوت هستند و دسترسی به این شبکه‌ها از یک شرکت ارتباطات از راه دور خریداری می‌شود. WAN نهایی اینترنت است که ستون فقرات جهانی همه MANها و LANها را بهم متصل می‌کند. با این حال، همه WANها به اینترنت متصل نمی‌شوند زیرا برخی از آنها شامل پیوندهای اختصاصی هستند که فقط شرکتی که برای آنها هزینه پرداخت می‌کند، دسترسی دارد.

پروتکل‌ها و خدمات Protocols and Services

پروتکل‌ها و خدمات بسیاری در طی این سال‌ها ایجاد شده‌اند تا قابلیت‌هایی را به شبکه‌ها اضافه کنند. در بسیاری از موارد، این پروتکل‌ها در لایه کاربردی Application مدل OSI قرار دارند. این پروتکل‌های لایه Application معمولاً یک عملکرد خاص را انجام می‌دهند و به پروتکل‌های لایه پایین در مجموعه TCP/IP و پروتکل‌های موجود در لایه ۲ (مانند اترنت) برای انجام خدمات مسیریابی و تحویل، تکیه می‌کنند.

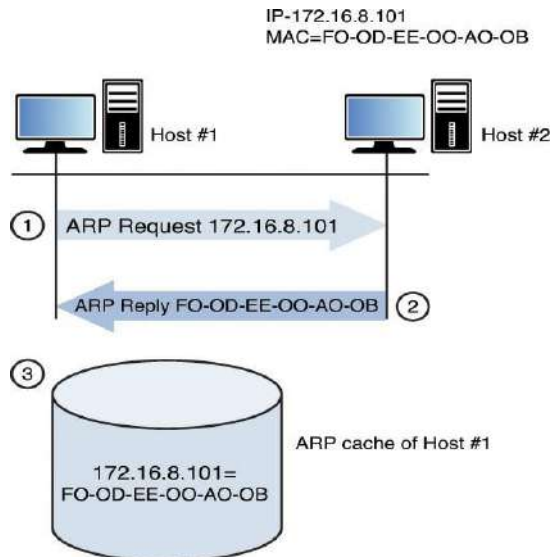
در این بخش برخی از مهمترین پروتکل‌ها و خدمات از جمله برخی از مواردی که در لایه Application کار نمی‌کنند، با تمرکز روی عملکرد و شماره پورت هرکدام پوشش داده می‌شود. اعداد پورت برای آگاهی از دیدگاه امنیتی حائز اهمیت است زیرا در بسیاری از موارد هنگام پیکربندی قوانین فایروال، به شماره‌های پورت ارجاع داده می‌شود. در مواردی که شماره پورت یا پروتکل مرتبط باشد، به آنها نیز ارجاع داده می‌شود.

ARP

پروتکل تفکیک آدرس (Address Resolution Protocol (ARP)، یکی از پروتکل‌های موجود در مجموعه TCP/IP، که در لایه ۳ مدل OSI کار می‌کند. اطلاعاتی که از آن بدست آورده می‌شود در لایه ۲ به کار گرفته می‌شود. وظیفه ARP این است که آدرس IP مقصد قرار داده شده در هدر توسط IP را با یک لایه ۲ یا آدرس MAC ترکیب کند. به یاد داشته باشید، هنگامی که

فریم ها یا قاب ها روی یک بخش محلی منتقل می شوند، انتقال طبق آدرس های MAC صورت می گیرد و از طریق آدرس های IP انجام نمی شود، بنابراین این اطلاعات باید شناخته شده باشند. هر زمان که یک بسته به شبکه ارسال شود، در هر هاپ روتر (در شبکه های کامپیوتری هاپ Hop قسمتی از یک مسیر Path بین مبدا و مقصد بسته اطلاعاتی است. بسته های اطلاعاتی از طریق روترهای موجود در شبکه بین مبدا و مقصد بسته پیموده می شوند. هر بسته اطلاعاتی زمانی که از یک روتر در شبکه عبور می کند یک عمل هاپ انجام می شود.) و دوباره در زیر شبکه مقصد، جفت آدرس MAC مبدا و مقصد تغییر می کند اما آدرس های IP مبدا و مقصد این کار را انجام نمی دهند. روندی که ARP برای اجرای این مقررات از آن استفاده می کند، پخش ARP نامیده می شود.

ابتدا با ناحیه ای از حافظه به نام کش ARP، مشورت صورت می گیرد. اگر آدرس MAC اخیراً ترکیب شده است، نقشه برداری در کش قرار خواهد گرفت و پخش Broadcast لازم نیست. اگر این رکورد از کش خارج شده باشد، ARP یک فریم پخش را به شبکه محلی ارسال می کند که همه دستگاه ها دریافت می کنند. دستگاهی که دارای آدرس IP می باشد با آدرس MAC خود پاسخ می دهد. سپس ARP آدرس MAC را در فریم قرار داده و فریم را ارسال می کند. شکل ۴-۱۲ این روند را نشان می دهد.



شکل ۴-۱۲: پخش ARP

DHCP

پروتکل پیکربندی میزبان پویا (Dynamic Host Configuration Protocol (DHCP) خدماتی است که می‌تواند برای خودکار کردن فرایند اختصاص پیکربندی IP به دستگاه‌های موجود در شبکه مورد استفاده قرار گیرد. پیکربندی دستی یک آدرس IP، ماسک زیر شبکه، دروازه پیش فرض Default Gateway و سرور DNS نه تنها وقت گیر است بلکه مملو از فرصت برای خطای انسانی است. استفاده از DHCP نه تنها می‌تواند این کار را به صورت خودکار انجام دهد بلکه می‌تواند مشکلات شبکه را نیز از این خطای انسانی برطرف کند.

DHCP یک برنامه مشتری / سرور است. همه سیستم عامل‌های مدرن دارای یک سرویس دهنده DHCP هستند و مؤلفه سرور می‌تواند بر روی یک سرور یا روی یک روتر پیاده سازی شود. هنگامی که رایانه‌ای که به عنوان مشتری DHCP پیکربندی شده است، شروع می‌شود، یک فرآیند دقیق چهار مرحله‌ای را برای بدست آوردن پیکربندی خود انجام می‌دهد. از نظر مفهومی، مشتری برای آدرس IP سرور DHCP پخش می‌کند. همه دستگاه‌ها این پخش Broadcast را دریافت می‌کنند، اما فقط سرورهای DHCP پاسخ می‌دهند. دستگاه، پیکربندی ارائه شده توسط اولین سرور DHCP را که می‌شنود می‌پذیرد. این فرایند از چهار بسته با نامهای مشخص استفاده می‌کند (شکل ۴-۱۳). DHCP از پورت‌های ۶۷ و ۶۸ UDP استفاده می‌کند. پورت ۶۷ داده‌ها را به سرور می‌فرستد، و پورت ۶۸ داده‌ها را برای مشتری ارسال می‌کند.



شکل ۴-۱۳: DHCP

DNS

درست همانطور که DHCP ما را از نیاز به پیکربندی دستی تنظیمات IP هر سیستم راحت می‌کند، Domain Name System (DNS) همه انسان‌ها را از دانستن آدرس IP هر رایانه‌ای که می‌خواهند با آن ارتباط برقرار کنند، راحت می‌کند. در نهایت، باید یک آدرس IP برای اتصال به

رایانه دیگر شناخته شود. DNS نام رایانه (یا در مورد وب، نام دامنه) را در یک آدرس IP قرار می دهد.

DNS یکی دیگر از برنامه های مشتری / سرور است که مشتری در کلیه سیستم عامل های مدرن گنجانده است. قسمت سرور بر روی یک سری از سرورهای DNS مستقر در شبکه محلی و اینترنت قرار دارد. هنگامی که یک مشتری DNS باید آدرس IP را که با نام رایانه یا نام دامنه خاصی همراه است، بداند، از سرور محلی DNS درخواست می کند. اگر سرور DNS محلی نتیجه ای نداد، با سایر سرورهای DNS از طرف مشتری تماس گرفته می شود، آدرس IP را یاد گرفته و آن اطلاعات را به مشتری DNS منتقل می کند. DNS از پورت 53 UDP و پورت 53 TCP استفاده می کند. سرورهای DNS برای تبادل اطلاعات از پورت 53 TCP استفاده می کنند، و مشتری های DNS از پورت 53 UDP برای نمایش داده ها استفاده می کنند.

FTP, FTPS, SFTP

پروتکل انتقال فایل (FTP) File Transfer Protocol و نسخه های امن تر آن FTPS و SFTP، فایل ها را از یک سیستم به سیستم دیگر منتقل می کند. FTP از این جهت که نام کاربری و گذرواژه به صورت واضح منتقل می شود، ناامن می باشد. نسخه اصلی Cleartext از پورت TCP 20 برای داده ها و پورت TCP 21 به عنوان کانال کنترل استفاده می کند. استفاده از FTP در هنگام توجه به امنیت توصیه نمی شود.

در واقع FTP است که پروتکل های رمزنگاری شده از Transport Layer Security (TLS) و Secure Sockets Layer (SSL) را پشتیبانی می کند. FTPS از پورت های TCP 989 و 990 استفاده می کند.

FTPS یکسان نیست و نباید با نسخه امن دیگر FTP و SSH، یعنی پروتکل انتقال فایل (SFTP) اشتباه گرفته شود. این یک پسوند پروتکل (SSH) Secure Shell است. تعداد نسخه های مختلف وجود داشته که نسخه ۶ جدیدترین آنها می باشد. از آنجا که از SSH برای انتقال فایل استفاده می کند، از پورت TCP 22 استفاده می شود.

Trivial FTP (TFTP) از احراز هویت استفاده نمی کند و از طریق پورت UDP 69 اجرا می شود.

HTTP, HTTPS, SHTTP

یکی از پروتکل‌های رایج امروزه پروتکل انتقال (HTTP) Hypertext و نسخه‌های امن آن، HTTPS و SHTTP است. این پروتکل برای مشاهده و انتقال صفحات وب یا محتوای وب استفاده می‌شود. نسخه اصلی (HTTP) رمزگذاری ندارد، بنابراین وقتی امنیت یک دغدغه می‌باشد، باید یکی از دو نسخه مطمئن استفاده شود. HTTP از پورت 80 TCP استفاده می‌کند.

در HTTPS پروتکل SSL / TLS در بالای پروتکل HTTP قرار دارد، بنابراین قابلیت‌های امنیتی SSL / TLS را به ارتباطات HTTP استاندارد اضافه می‌کند و اغلب برای وب سایت‌های امن استفاده می‌شود زیرا به هیچ نرم افزاری یا تنظیماتی در سرویس گیرنده وب برای عملکرد امن نیاز ندارد. هنگامی که از HTTPS استفاده می‌شود، از پورت ۸۰ استفاده نمی‌شود. در عوض، از پورت ۴۴۳ استفاده می‌کند.

برخلاف HTTPS، که کل ارتباطات را رمزگذاری می‌کند، SHTTP فقط داده‌های صفحه ارائه شده را رمزگذاری می‌کند و داده‌هایی از قبیل زمینه‌های POST را ارسال می‌کند و شروع پروتکل را تغییر نمی‌دهد. پردازش SecureHTTP و HTTP می‌تواند در همان پورت TCP، پورت ۸۰ کار کنند. این نسخه بندرت استفاده می‌شود.

ICMP

پروتکل کنترل پیام اینترنت (ICMP) Internet Control Message Protocol در لایه ۳ (لایه شبکه) مدل OSI فعالیت می‌کند و توسط دستگاه‌ها برای انتقال پیام‌های خطا در رابطه با مشکلات انتقال استفاده می‌شود. همچنین پروتکل مورد استفاده در هنگام کار با دستورات پینگ و ردیابی برای رفع مشکلات اتصال به شبکه می‌باشد.

ICMP خطاهای شبکه و تراکم شبکه را اعلام می‌کند. همچنین در عیب یابی کمک کرده و Timeout را اعلام می‌کند.

ICMP پروتکلی است که می‌تواند بر اساس عملکرد آن، چندین حمله شبکه‌ای را اعمال کند و به همین دلیل بسیاری از شبکه‌ها، مسدود کردن ICMP را انتخاب می‌کنند.

IMAP

پروتکل دسترسی به پیام اینترنت (IMAP) Internet Message Access Protocol یک پروتکل لایه کاربردی برای بازیابی ایمیل است. آخرین نسخه آن IMAP4 است. این پروتکل ایمیل

مشتری است که برای دسترسی به ایمیل از سرور استفاده می شود. بر خلاف POP3، سرویس ایمیل مشتری دیگر که فقط می تواند پیامها را از سرور دانلود کند، IMAP4 به شخص امکان می دهد یک نسخه را دانلود کند و یک نسخه را روی سرور قرار دهد. IMAP4 از پورت ۱۴۳ استفاده می کند. یک نسخه امن نیز وجود دارد به نام IMAPS، که در واقع IMAP بر روی SSL می باشد که از پورت ۹۹۳ استفاده می کند.

LDAP

پروتکل دسترسی دایرکتوری سبک (LDAP) Lightweight Directory Access Protocol یک پروتکل پرس و جو دایرکتوری است که براساس سری X.500 استانداردهای شبکه رایانه ساخته شده است. پیاده سازی فروشنده LDAP شامل Microsoft's Active Directory Services, Novell's eDirectory, and Sun's Network Information Service (NIS)، که به طور پیش فرض، LDAP از پورت TCP / UDP 389 استفاده می کند.

NAT

ترجمه آدرس شبکه (NAT) Network Address Translation سرویسی است که آدرسهای IP خصوصی را در آدرسهای IP عمومی نقشه برداری می کند.

NetBIOS

شبکه عمومی ورودی / خروجی سیستم NetBIOS یک API است. NetBIOS از طریق TCP / (NetBT) IP در پورت های 137، TCP138، TCP139 اجرا می شود.

NFS

Network File System (NFS) یک پروتکل اشتراک گذاری فایل مشتری / سرور است که در UNIX / Linux استفاده می شود. نسخه ۴ جدیدترین نسخه NFS است. NFS امن (SNFS) محرمانه بودن را با استفاده از استاندارد رمزگذاری دیجیتال Digital Encryption Standard (DES) ارائه می دهد.

PAT

ترجمه آدرس پورت (PAT) Port address translation یک نسخه خاص از NAT است که از یک آدرس IP عمومی استفاده کرده تا چندین آدرس IP خصوصی را نشان دهد. عملکرد آن در بخش "آدرس دهی منطقی و فیزیکی" در اوایل این فصل مورد بحث قرار گرفته است.

POP

Post Office Protocol یا POP یک پروتکل بازیابی ایمیل لایه کاربردی است. POP3 جدیدترین نسخه می‌باشد و فقط برای دانلود پیام‌ها امکان پذیر است و قابلیت‌های اضافی ارائه شده توسط IMAP4 را ندارد. POP3 از پورت ۱۱۰ استفاده می‌کند. نسخه‌ای که از طریق SSL اجرا شده نیز وجود دارد که از پورت ۹۹۵ استفاده می‌کند.

CIFS / SMB

Common File File System (CIFS) / Block Message Block (SMB) یک پروتکل اشتراک گذاری فایل است که از پورت 445 TCP استفاده می‌کند.

SMTP

POP و IMAP پروتکل‌های ایمیل مشتری هستند که برای بازیابی ایمیل مورد استفاده قرار می‌گیرند، اما وقتی سرورهای ایمیل با یکدیگر در حال گفتگو هستند از پروتکل به نام Simple Mail Transfer Protocol (SMTP) استفاده می‌کنند، که یک پروتکل استاندارد لایه کاربردی است، همچنین پروتکل مورد استفاده مشتری‌ها برای ارسال ایمیل می‌باشد. SMTP از پورت ۲۵ استفاده می‌کند، و هنگامی که از طریق SSL اجرا شود، از پورت ۴۶۵ استفاده می‌کند. SMTP پیشرفته یا Enhanced SMTP (ESMTP) اجازه می‌دهد تا اندازه فیلد بزرگتر و دستورات SMTP موجود گسترده باشد.

SNMP

پروتکل مدیریت شبکه ساده (Simple Network Management Protocol (SNMP یک پروتکل لایه کاربردی است که برای بازیابی اطلاعات از دستگاه‌های شبکه و ارسال تغییرات پیکربندی به آن دستگاه‌ها استفاده می‌شود. SNMP در TCP از پورت 162 و در UDP از پورت 161 و 162 استفاده می‌کند.

دستگاههای SNMP در جوامع ساماندهی شده اند و باید با نام آن جامعه شناخته شود که به اطلاعات دسترسی داشته یا از آن به یک دستگاه ارسال شود. همچنین می توان از گذرواژه استفاده کرد. نسخه های 1 و 2 SNMP در معرض Sniffing قرار دارند و همه نسخه ها مستعد حملات بی رحمانه Brute-Force به رشته های جامعه و گذرواژه مورد استفاده هستند. پیش فرض اسامی رشته های جامعه، که به طور گسترده ای شناخته شده است، اغلب در جای خود باقی مانده است. آخرین نسخه، SNMPv3، امن ترین آن می باشد.

پروتکل های چند لایه Multi-Layer Protocols

بسیاری از پروتکل های چند لایه مانند FTP و DNS روی یک لایه واحد از مدل OSI کار می کنند. با این حال، بسیاری از پروتکل ها در چندین لایه از مدل OSI کار می کنند. بهترین نمونه TCP/IP / می باشد، در واقع پروتکل شبکه ای است که در اینترنت و در اکثر قریب به اتفاق شبکه های محلی (LAN) استفاده می شود.

بسیاری از پروتکل های چند لایه به عنوان بخشی از پروتکل های اختصاصی طراحی شده اند و به آنچه امروزه هستند تبدیل شده اند. امروزه از پروتکل های چند لایه برای کنترل مؤلفه های مهم زیرساخت مانند شبکه های برق و سیستم های کنترل صنعتی (ICS) استفاده می شود. از آنجا که این مؤلفه های مهم زیرساخت در ابتدا برای استقرار از طریق اینترنت طراحی نشده بودند چالش های منحصر به فردی به وجود آمده است. استقرار نرم افزار آنتی ویروس در ICS تقریباً غیرممکن است. بسیاری از ICS ها بدون هیچ تصویری به امنیت فیزیکی خود سیستم کنترل، نصب می شوند. برخلاف سیستم های IT، تأخیر در ICS به دلیل حساس بودن زمان پاسخگویی به شرایط اضطراری قابل قبول نیست. ICS ها معمولاً عمر بسیار طولانی تری نسبت به سیستم IT دارند. در دسترس بودن ICS ها معمولاً ۳۶۵/۷/۲۴ است، در حالی که یک سیستم IT می تواند دوره های کوتاه عدم دسترسی را تحمل کند. وقتی این مسائل و سایر مسائل را در نظر می گیرید، می توانید به راحتی بفهمید که چرا یک سازمان باید هنگام استقرار ICS که از پروتکل های چند لایه استفاده می کند، پیامدهای امنیتی را کاملاً در نظر بگیرد. استفاده از پروتکل تولید شده توسط فروشنده همیشه جوابگو نیست زیرا پروتکل های تهیه شده توسط فروشنده بدون توجه به امنیت مربوط به کنترل زمان و دستگاه می باشد.

پروتکل شبکه توزیع شده نسخه ۳، Distributed Network Protocol version 3 (DNP3) یک پروتکل چند لایه است که بین قطعات در سیستم های اتوماسیون فرایند در شرکت های آب و

برق استفاده می‌شود. این ارتباطات بین انواع مختلفی از تجهیزات جمع‌آوری داده‌ها و کنترل‌ها ایجاد شده است. این امر نقش مهمی در سیستم‌های نظارتی و جمع‌آوری داده‌ها یا SCADA دارد.

پروتکل‌های همگرا Converged Protocols

همگرایی IP شامل حمل انواع مختلف ترافیک از طریق یک شبکه است. ترافیک شامل صدا، فیلم، داده و تصاویر است. این پروتکل مبتنی بر پروتکل اینترنت (IP) است. هنگامی که همگرایی IP مستقر شد، یک پلتفرم واحد برای همه نوع ترافیک استفاده می‌شود، که شامل همه دستگاه‌ها است. این اپلیکیشن از اپلیکیشن‌های چندرسانه‌ای پشتیبانی می‌کند. مدیریت و انعطاف‌پذیری شبکه به دلیل وجود راه‌اندازی یکنواخت و امکان قالب‌بندی الگوهای ارتباطی بسیار بهبود یافته است. کیفیت خدمات (QoS) می‌تواند مستقر شود تا مدیران بتوانند مطمئن شوند که برخی خدمات دارای اولویت بالاتری نسبت به سایر خدمات هستند. اجرای همگرایی IP شامل کانال فیبرنوری از طریق اترنت یا Fibre Channel over Ethernet (FCoE)، تعویض برچسب Multiprotocol Label Switching (MPLS)، Voice over IP (VoIP) و واسط سیستم رایانه‌ای کوچک اینترنت یا iSCSI است.

FCoE

Fiber Channel over Ethernet (FCoE) پروتکلی است که فریم‌های کانال فیبر نوری را از طریق شبکه‌های اترنت کپسوله می‌کند، از این طریق به کانال فیبرنوری اجازه می‌دهد تا ضمن حفظ پروتکل کانال فیبرنوری، از شبکه اترنت ۱۰ گیگابیتی یا بالاتر استفاده کند. FCoE از پورت‌های زیر برای برقراری ارتباط بین دستگاه‌های FCoE استفاده می‌کند:

- ✓ پورت شبکه (N): یک گره یا یک نود را به یک کانال فیبرنوری که به یک نود سوییچ شده است، وصل می‌کند. به آن پورت نود Node port نیز گفته می‌شود.
- ✓ پورت فابریک (F): کانال فیبر فابریک را به یک نود از سوییچ متصل می‌کند.
- ✓ پورت (L) loop: یک نود را از یک نود به حلقه (Loop) کانال فیبر نوری وصل می‌کند.
- ✓ پورت (NL) Network + loop: از نود به هر دو حلقه و سوییچ متصل می‌شود.
- ✓ پورت فابریک + (FL) loop: از سوییچ به حلقه و سوییچ متصل می‌شود.

- ✓ پورت توسعه (E) port Extender : کانال فیبر نوری به صورت آشنایی به یکدیگر سوئیچ می شوند و بدین ترتیب فابریک را توسعه می یابد.
 - ✓ پورت عمومی (G) port General : انواع دیگر پورت را تقلید می کند.
 - ✓ پورت (EX) External : یک روتر کانال فیبر نوری و یک سوئیچ کانال فیبر نوری را بهم متصل می کند. پورت EX در سمت روتر قرار دارد و پورت E در سمت سوئیچ قرار دارد.
 - ✓ پورت (TE) Trunking E : مسیریابی چندگانه مجازی SAN یا VSAN را مجاز کرده و عملکردهای پورت E استاندارد را ارائه می دهد.
- FCoE دارای چندین مزیت از جمله موارد زیر است: تکنسین ها یا کارشناسان فنی فقط باید یک بار عملیات سیم کشی را به سرور انجام دهند، به کابل ها و آداپتورهای کمتری نیاز دارند، I / O از تهیه نرم افزار استفاده می کند، واسطه با SAN های موجود کانال فیبر نوری امکان پذیر است و از دروازه ها (Gateways) استفاده نمی شود.

MPLS

تعویض برچسب چند پروتکل (MPLS) Multiprotocol Label Switching داده ها را از یک نود به سمت دیگر بر اساس برچسب های مسیر کوتاه به جای آدرس های شبکه طولانی مسیریابی می کند و از یک جستجوی پیچیده در یک جدول مسیریابی اجتناب می کند. همچنین شامل توانایی کنترل مکان و چگونگی مسیریابی ترافیک می باشد، خدمات انتقال داده را در همان شبکه ارائه می دهد و انعطاف پذیری شبکه را از طریق دوباره مسیریابی سریع MPLS بهبود می بخشد. MPLS از برچسب تغییر مسیر (LSP) Label Switched Path استفاده می کند که یک تونل یک طرفه بین روترها است. شبکه MPLS امکان دارد از نقشه های زیر استفاده کند:

Label edge router (LER) : اولین روتر که بسته ای را درون LSP کپسوله می کند و انتخاب مسیر را انجام می دهد. معمولاً به آن نود ورودی Ingress node نیز گفته می شود.

Label switching router (LSR) : یک روتر که MPLS را در جایی در امتداد LSP انجام می دهد. به این نود ترانزیت Transit node نیز گفته می شود.

Egress node : آخرین روتر در پایان یک LSP

هنگام خاتمه LSP، از تهی مطلق یا صریح (Implicit, Explicit Null) استفاده می شود. تهی های مطلق هنگام رسیدن به بعد از آخرین هاپ، برچسب را حذف می کنند. تهی های صریح برچسب را تا آخرین روتر نگه می دارند.

وقتی MPLS به عنوان بخشی از VPN قرار دارد، می‌توان از نقش‌های روتر زیر استفاده شود:
روتر ارائه دهنده Provider (P) router: ستون فقرات روتر که فقط برچسب (Label) سوئیچینگ را انجام می‌دهد.

روتر ارائه دهنده لبه Provider edge (PE) router: روتر که با مشتری روبرو می‌شود که برچسب زدن و تحمیل برچسب را انجام می‌دهد. همچنین می‌تواند چندین سرویس را خاتمه دهد.

روتر لبه مشتری Customer edge (CE) router: روتر مشتری که روتر PE با آن ارتباط برقرار می‌کند.

MPLS از دو دستور پروتکل مسیریابی استفاده می‌کند:
 پروتکل توزیع برچسب Label Distribution Protocol (LDP) و پروتکل رزرو منابع با مهندسی ترافیک Resource Reservation Protocol with Traffic Engineering (RSVP-TE).
 RSVP-TE بسیار پیچیده تر از LDP است. LDP، بیشتر در MPLS VPN استفاده می‌شود، در حالی که RSVP-TE برای مهندسی ترافیک مورد نیاز است.

VoIP

پروتکل Voice over Internet (VoIP) شامل فناوری‌هایی است که ارتباطات صوتی و جلسات چندرسانه‌ای را از طریق شبکه‌های IP مانند اینترنت ارائه می‌دهند. VoIP را تلفنهای IP، تلفن اینترنتی، تلفن باند گسترده Broadband و خدمات تلفن باند گسترده نیز می‌نامند. VoIP را می‌توان با استفاده از انواع مختلفی از پروتکل‌ها از جمله

H.323 ✓

پروتکل شروع جلسه Session Initiation Protocol (SIP) ✓

پروتکل کنترل دروازه رسانه‌ها Media Gateway Control Protocol (MGCP) ✓

پروتکل انتقال در زمان واقعی Real-time Transport Protocol (RTP) پیاده سازی کرد.

Internet Small Computer System Interface (iSCSI)

واسط سیستم رایانه‌ای کوچک اینترنت iSCSI اجازه می‌دهد تا دستورات SCSI به صورت End-to-End از طریق LAN، WAN یا TCP از طریق اینترنت ارسال شوند. این امر باعث تشییت ذخیره سازی و بهبود فاجعه می‌شود. iSCSI دارای چندین مزیت از جمله موارد زیر است:

تکنسین‌ها فقط باید یک بار به سرور سیم کشی کنند و به کابل‌ها و آداپتورهای کمتری نیاز دارد، از یک مدل عملیاتی جدید استفاده می‌شود و پشتیبانی گسترده‌ای از صنعت از جمله درایورهای iSCSI فروشنده، Gateway‌ها و آرایه‌های ذخیره سازی iSCSI بومی وجود دارد.

شبکه‌های بی سیم یا وایرلس Wireless Networks

شاید ناحیه شبکه‌ای که ادمین‌های بیشتری را هوشیار می‌کند، بخش وایرلس شبکه می‌باشد. در اوایل استقرار WLAN 802.11، به خاطر ترس از حفره‌های امنیتی بود که به سادگی از وایرلس استفاده نمی‌کردند. با این حال، آشکار شد که کاربران نه تنها خواستار این امر بودند، بلکه در برخی موارد کاربران AP‌های خانگی را به کار گرفته و آنها را قلاب کرده (Hooking) و ناگهان یک شبکه وایرلس بوجود می‌آمد.

امروزه امنیت WLAN به حدی تکامل یافته است که دیگر امنیت دلیل موجهی برای جلوگیری از وایرلس نمی‌باشد. در این بخش نگاهی به پروتکل‌های مورد استفاده در وایرلس، روش‌های مورد استفاده برای تبدیل داده‌ها به امواج رادیویی، توپولوژی‌های مختلفی که در آن می‌توان WLAN‌ها مستقر شده و اقدامات امنیتی که باید انجام شود ارائه می‌شود.

GSM و OFDMA, CDMA, TDMA, FDMA, VOFDM, OFDM, DSSS, FHSS

هنگامی که داده‌ها، کنترل کننده واسط شبکه اینترنت (NIC) Network Interface Controller را ترک می‌کنند و از طریق شبکه ارسال می‌شوند، یک و صف‌هایی که داده‌ها را تشکیل می‌دهند با ولتاژهای الکتریکی مختلف نمایش داده می‌شوند. در وایرلس، این اطلاعات باید در امواج رادیویی ارائه شود. تعدادی روش مختلف برای انجام این عمل وجود دارد که اصطلاحاً مدولاسیون Modulation نام دارد. همچنین باید برخی از اصطلاحات اضافی برای درک هوشمندانه وایرلس درک شود، و تکنیک‌های مورد استفاده در WLAN‌ها و تکنیک‌های مورد استفاده در شبکه‌های سلولی را پوشش دهد.

تکنیک‌های 802.11

تکنیک‌های زیر در WLAN ها استفاده می‌شود:

✓ طیف گسترده پرتاب فرکانس (Frequency Hopping Spread Spectrum (FHSS)

DSSS و FHSS بخشی از استاندارد اصلی 802.11 بودند. FHSS از این جهت منحصر به فرد است که فرکانس‌ها یا کانال‌ها را هر چند ثانیه در یک مجموعه الگو Set pattern تغییر می‌دهد که فرستنده و گیرنده آن را می‌شناسند. این یک معیار امنیتی نیست زیرا الگوهای آن به خوبی شناخته شده است، هرچند که ضبط ترافیک را دشوار می‌کند و کمک می‌کند تا با استفاده از فرکانس، جایی که تداخل (Inference) در آن وجود دارد، از تداخل جلوگیری کند. اصلاحات بعدی در استاندارد 802.11 این فناوری را شامل نمی‌شود. همچنین می‌تواند حداکثر ۲ مگابیت بر ثانیه بدست آورد.

✓ طیف گسترده توالی مستقیم (Direct Sequence Spread Spectrum (DSSS)

DSSS و FHSS بخشی از استاندارد اصلی 802.11 بودند. DSSS یک روش مدولاسیون است که در 802.11b استفاده می‌شود. تکنیک مدولاسیون مورد استفاده در وایرلس تأثیر زیادی در توان دارد. انتقال همزمان در طیف را بر خلاف متوقف کردن از یکدیگر به مانند FHSS، پخش می‌کند. همچنین اجازه می‌دهد تا حداکثر ۱۱ مگابیت بر ثانیه بدست آورد.

✓ تعدد انعطاف پذیری بخش فرکانس متعامد

Orthogonal Frequency Division Multiplexing (OFDM)

OFDM یک تکنیک پیشرفته تر از مدولاسیون است که در آن تعداد زیادی از سیگنال‌های زیر حامل (Sub-Carrier) متعامد نزدیک به هم برای انتقال داده‌ها در چندین جریان داده موازی استفاده می‌شود. در 802.11a, 802.11ac, 802.11g, 802.11n استفاده می‌شود. این سرعت را تا ۵۴ مگابیت بر ثانیه امکان پذیر می‌کند.

✓ بردار چند برابر سازی بخش فرکانس متعامد

Vectored Orthogonal Frequency Division Multiplexing (VOFDM)

VOFDM توسعه یافته توسط سیسکو، از تنوع ویژه‌ای برای افزایش نویز، تداخل و تحمل چند برابر استفاده می‌کند.

تکنیک‌های بی سیم سیار و سلولی

در شبکه‌های سلولی از روشهای زیر استفاده شده است:

○ دسترسی چندگانه به فرکانس (FDMA) Frequency Division Multiple Access

یکی از تکنیک‌های مدولاسیون است که در شبکه‌های بی سیم سلولی مورد استفاده قرار می‌گیرد. این محدوده فرکانس را به باندها تقسیم کرده و یک باند را به صورت مشترک اختصاص می‌دهد. در شبکه‌های سلولی G1 مورد استفاده قرار گرفت.

○ دسترسی چندمنظوره زمانی (TDMA) Time Division Multiple Access

تقسیم کانال‌ها در اسلات‌های زمانی و اختصاص اسلات به تماس، سرعت را بیش از FDMA افزایش می‌دهد. همچنین به جلوگیری از استراق سمع تماس‌ها کمک می‌کند.

○ دسترسی چندگانه تقسیم کد (CDMA) Code Division Multiple Access

تماس یا انتقال یک کد منحصر به فرد اختصاص می‌دهد و داده‌ها را در طیف پخش می‌کند و به یک تماس امکان می‌دهد از همه فرکانس‌ها استفاده کند.

○ دسترسی چندگانه بخش فرکانس متعامد (OFDMA) Orthogonal Frequency Division Multiple Access

با تقسیم فرکانسها در کانالهای فرعی، FDMA را یک قدم بیشتر می‌برد. این روش مورد نیاز دستگاه‌های 4G است.

○ سیستم جهانی ارتباطات سیار (GSM) Global System for Mobile Communications

(GSM) نوعی تلفن سلولی است که شامل یک تراشه ماژول هویت مشترک (SIM) Subscriber Identity Module است. این تراشه‌ها حاوی اطلاعاتی در مورد مشترکان هستند و برای عملکرد آن باید در تلفن موجود باشد. یکی از خطرات این تلفن‌ها شبیه سازی تلفن‌های همراه یا Cloning است، روندی که در آن نسخه‌هایی از تراشه سیم ساخته می‌شود که به یک کاربر دیگر امکان برقراری تماس به عنوان کاربر اصلی را می‌دهد. رمزنگاری کلید مخفی (با استفاده از یک کلید مخفی مشترک) در

هنگام انجام احراز هویت بین تلفن و شبکه استفاده می‌شود. این استاندارد جهانی پیش فرض برای ارتباطات سیار می‌باشد.

ماهواره‌ها Satellites

ماهواره‌ها می‌توانستند برای ارائه خدمات تلویزیون و داشتن خدمات مدتی از آن، بکار برده شوند، اما اکنون می‌توان از آنها برای ارائه دسترسی اینترنت به منازل و مشاغل نیز استفاده کرد. این ارتباط دو طرفه است نه یک طرفه که با خدمات تلویزیون انجام می‌شود و به طور معمول با استفاده از فناوری مایکروویو انجام می‌شود. در بیشتر موارد، دانلودها از سیگنال‌های ماهواره‌ای صورت می‌گیرد، در حالی که آپلودها از طریق یک خط زمینی اتفاق می‌افتد.

از فن آوری مایکروویو همچنین می‌توان برای انتقال زمینی Terrestrial Transmission استفاده کرد که به معنای ایستگاه زمینی به ایستگاه زمینی و نه ماهواره به زمین است. ارتباطات ماهواره‌ای بسیار کند است اما در مکان‌های دور افتاده که راه حل دیگری در دسترس نیست بسیار مفید است.

ساختار WLAN

قبل از اینکه بتوانیم در مورد 802.11 وایرلس، که به عنوان WLAN شناخته شده است، بحث کنیم، باید در مورد مؤلفه‌ها و ساختار یک WLAN بحث کنیم.

نقطه دسترسی Access Point

نقطه دسترسی (AP) یک فرستنده و گیرنده بی سیم است که به قسمت سیمی شبکه وصل می‌شود و یک نقطه دسترسی به این شبکه را برای دستگاه‌های بی سیم فراهم می‌کند. در برخی موارد سوئیچ‌های بی سیم هستند و در موارد دیگر نیز روتر هستند. AP‌های اولیه دستگاه‌هایی بودند که تمام کارایی آنها در هر دستگاه وجود داشته است، اما به طور فزاینده‌ای این AP‌های "Fat" یا هوشمند با AP‌های "Thin" جایگزین شده‌اند که در واقع فقط آنتن‌هایی هستند که به یک سیستم مرکزی به نام کنترلر وصل می‌شوند.

SSID

شناسه مجموعه خدمات (Service set identifier) (SSID) نام یا مقداری است که برای شناسایی WLAN از سایر WLAN ها اختصاص داده شده است. SSID می تواند توسط AP پخش شود همانطور که در یک Hot spot سیار رایگان انجام می شود یا می تواند پنهان شود. هنگامی که پنهان است، یک ایستگاه بی سیم باید با پروفایلی که شامل SSID است پیکربندی شود. اگرچه برخی تصور می کنند که SSID به عنوان یک اقدام امنیتی پنهان می شود، اما اقدامی مؤثر نیست زیرا مخفی کردن SSID یک نوع فریم، فقط روشنی فریم را از بین می برد، در حالی که هنوز در سایر انواع فریم وجود دارد و با Sniffing شبکه بی سیم می توان به راحتی بدست آورد.

وضعیت زیرساخت در مقابل وضعیت Ad Hoc، Infrastructure Mode Versus Ad Hoc Mode

در بیشتر موارد، WLAN حداقل یک AP را شامل می شود. هنگامی که یک AP وجود دارد، WLAN در وضعیت زیرساخت کار می کند، در این وضعیت، تمام انتقال ها بین ایستگاه ها یا دستگاه ها از طریق AP انجام می شود و هیچ ارتباط مستقیمی بین ایستگاه ها رخ نمی دهد. در وضعیت Ad Hoc، AP وجود ندارد و ایستگاه ها یا دستگاه ها مستقیماً با یکدیگر ارتباط برقرار می کنند.

استانداردهای WLAN

استاندارد بی سیم 802.11 اصلی بارها اصلاح شده است تا ویژگی ها و قابلیت هایی اضافه شود. در این بخش به بحث در مورد این اصلاحات می پردازیم که بعضاً به عنوان استاندارد از آنها یاد می شود، گرچه واقعاً اصلاحاتی روی استاندارد اصلی هستند.

802.11

استاندارد اصلی 802.11 استفاده از FHSS یا DSSS را پشتیبانی می کند و عملیات پشتیبانی در دامنه فرکانس ۲،۴ گیگاهرتز با سرعت ۱ Mbps و ۲ Mbps را مشخص می کند.

802.11a

اولین اصلاحیه استاندارد 802.11a بود. این استاندارد استفاده از OFDM را فرا می خواند. از آنجا که برای ارتقاء سخت افزار به تجهیزات موجود نیاز دارد، این استاندارد برای مدتی محدود به نظر

می‌رسید. در فرکانس متفاوتی نسبت به 802.11 (۵ گیگاهرتز) فعالیت می‌کند و با استفاده از پشتیبانی OFDM سرعت‌های حداکثر ۵۴ Mbps را پشتیبانی می‌کند.

802.11ac

استاندارد 802.11 ac مانند استاندارد 802.11 a در فرکانس ۵ گیگاهرتز کار می‌کند. مهمترین ویژگی این استاندارد توان چند ایستگاه WLAN حداقل ۱ گیگابیت بر ثانیه و توان یک پیوند تنها ۵۰۰ مگابیت در ثانیه است. این کار را با اجرای فن آوری‌های چندین کاربره، چندین ورودی چندین خروجی (MU MIMO) ارائه می‌دهد که در آن نقاط دسترسی وایرلس چندین آنتن دارند.

802.11 ac سریعتر و مقیاس پذیر تر از 802.11 n است.

802.11b

اصلاحات 802.11b پشتیبانی از FHSS را کاهش داده و سرعت را تا ۱۱ مگابیت در ثانیه افزایش می‌دهد. به طور گسترده پذیرفته شده زیرا هر دو در یک فرکانس مشابه 802.11 عمل می‌کنند و سازگاری رو به عقب داشته و می‌توانند در همان WLAN کار کنند.

802.11f

اصلاحیه 802.11 f مشکلاتی را معرفی می‌کند زمانی که مشتریان بی سیم از یک AP به AP دیگر پرسه می‌زنند. این امر باعث می‌شود تا ایستگاه مجدداً با AP جدید احراز هویت شود، که در برخی موارد تأخیری را ایجاد می‌کند که اتصال اپلیکیشن را خراب می‌کند. این اصلاح به اشتراک گذاری اطلاعات احراز هویت بین APها را بهبود می‌بخشد.

802.11g

اصلاحیه 802.11 g پشتیبانی OFDM را افزایش داده و باعث شده است تا توان ۵۴ مگابیت بر ثانیه را داشته باشد. همچنین در فرکانس ۲,۴ گیگاهرتز عمل می‌کند بنابراین با هر دو 802.11 b و 802.11 سازگار است. در حالی که با همان سرعت 802.11 a، یکی از دلایلی که بسیاری به 802.11 روی آورده اند این است که باند ۵ گیگاهرتزی نسبت به باند ۲,۴ گیگاهرتز بسیار شلوغی کمتری دارد.

802.11n

استاندارد 802.11 n برای دستیابی به حداکثر ۶۵۰ Mbps، از چندین مفهوم جدید استفاده می‌کند. این کار را با استفاده از کانالهایی به پهنای ۴۰ مگاهرتز انجام می‌دهد، با استفاده از آنتن‌های متعدد که حداکثر چهار جریان مکانی را در یک زمان امکان پذیر می‌کنند (ویژگی‌ای به نام ورودی چندگانه، خروجی چندگانه [MIMO]) می‌توان از آن در هر دو باند 2,4 گیگاهرتز و 5,0 گیگاهرتز استفاده کرد اما در یک شبکه خالص 5,0 گیگاهرتز بهترین عملکرد را دارد زیرا در این حالت نیازی به اجرای مکانیزم‌هایی ندارد که بتواند با دستگاه‌های 802.11b و 802.11g فعالیت کند. این مکانیزم عملکرد را کند می‌کند.

بلوتوث Bluetooth

بلوتوث یک فناوری بی سیم است که برای ایجاد شبکه‌های منطقه شخصی (PAN) استفاده می‌شود. این شبکه‌ها، اتصال ساده با برد کوتاه هستند که بین دستگاه‌ها و لوازم جانبی، مانند هدفون وجود دارد. بلوتوث نسخه 1,0 – 2,0 در فرکانس 2,4 گیگاهرتز با سرعت ۱ Mbps تا ۳ Mbps با فاصله تا ۱۰ متر کار می‌کند. بلوتوث 3,0 و 4,0 می‌توانند با سرعت ۲۴ Mbps کار کنند. چندین حمله می‌تواند از فناوری بلوتوث بهره ببرد. Bluejacking اغلب زمانی است که یک پیام درخواست نشده به منظور اضافه کردن کارت ویزیت در لیست مخاطبین قربانی، به یک دستگاه دارای بلوتوث ارسال می‌شود.

با قرار دادن دستگاه در حالت غیر قابل کشف Non-discoverable mode می‌توان از این کار جلوگیری کرد.

Bluesnarfing دسترسی غیرمجاز به دستگاه با استفاده از اتصال بلوتوث است. در این حالت مهاجم به جای ارسال پیام به دستگاه، سعی در دسترسی به اطلاعات دستگاه را دارد.

مادون قرمز Infrared

در پایان، مادون قرمز یک فرایند بی سیم از راه کوتاه است که از نور به جای امواج رادیویی استفاده شده، در این حالت از نور مادون قرمز استفاده می‌شود. برای اتصالات کوتاه بین دستگاه‌هایی که هر دو دارای پورت مادون قرمز هستند استفاده می‌شود. این دستگاه با سرعت حداکثر ۵ مگابیت در ثانیه کار می‌کند و به چشمی مستقیم بین دستگاه‌ها نیاز دارد. یک پروتکل مادون قرمز یا پروتکلی وجود دارد که می‌تواند مسائل امنیتی را معرفی کند. پروتکل IrTran-P (انتقال

تصویر) در دوربین‌های دیجیتال و سایر دستگاه‌های ضبط تصویر دیجیتال استفاده می‌شود. کلیه فایل‌های دریافتی ارسال شده از طریق IrTran-P بطور خودکار پذیرفته می‌شوند. از آنجا که فایل‌های دریافتی ممکن است حاوی برنامه‌های مضر باشند، کاربران باید مطمئن شوند که این فایل‌ها از یک منبع قابل اعتماد سرچشمه گرفته اند.

ارتباط میدانی نزدیک (Near Field Communication (NFC

ارتباطات میدانی نزدیک یا NFC مجموعه‌ای از پروتکل‌های ارتباطی است که به دو دستگاه الکترونیکی که یکی از آنها معمولاً یک دستگاه سیار است، اجازه می‌دهد با آوردن آنها در ۲ اینچ از یکدیگر، ارتباط برقرار کنند. دستگاه‌های دارای قابلیت NFC با اپلیکیشن‌هایی تعبیه شده اند که می‌توانند برای خواندن برچسب‌های الکترونیکی یا پرداخت در هنگام اتصال به یک دستگاه سازگار با NFC، استفاده شوند.

WLAN Security

برای پیاده سازی امن فن آوری‌های بی سیم 802,11، باید تمام روش‌های استفاده شده برای ایمن سازی WLAN را درک کنید. در این بخش، مهمترین اقدامات از جمله برخی اقدامات مورد بحث قرار می‌گیرد که اغلب از آنها به عنوان اقدامات امنیتی یاد می‌شود، اما هرگز امنیت واقعی را ارائه نمی‌دهد.

احراز هویت سیستم باز Open System Authentication

احراز هویت پیش فرض اصلی است که در 802,11 استفاده می‌شود. درخواست احراز هویت فقط شامل ID ایستگاه و پاسخ تأیید احراز هویت است. در حالی که می‌توان همراه با WEP استفاده شود، فریم‌های مدیریت احراز هویت به صورت متن ساده Cleartext ارسال می‌شوند زیرا WEP فقط داده‌ها را رمزگذاری می‌کند.

احراز هویت کلید مشترک Shared Key Authentication

احراز هویت کلید مشترک از WEP و یک کلید مخفی مشترک برای احراز هویت استفاده می‌کند. متن چالش همراه با WEP با استفاده از کلید مخفی مشترک رمزگذاری می‌شود. مشتری متن چالش رمزگذاری شده را به نقطه دسترسی بی سیم برمی گرداند.

WEP

محرمانگی همسان سیمی (Wired Equivalent Privacy (WEP اولین اقدام امنیتی است که با استفاده از 802.11 استفاده شد. در مشخصات اصلی به عنوان الگوریتم مشخص شده است و می تواند برای تصدیق اعتبار یک دستگاه و رمزگذاری اطلاعات بین AP و دستگاه استفاده شود. مشکلی که در WEP وجود دارد این است که الگوریتم رمزگذاری RC4 را به روشی پیاده سازی می کند که به هکر امکان رمزگذاری را می دهد. همچنین مشخص شد مکانیسمی که برای تضمین یکپارچگی داده ها طراحی شده است (که داده ها تغییر نکرده اند) ناکافی بوده و امکان تغییر داده ها و کشف این واقعیت فراهم شده است.

WEP با یک کلید مخفی یا گذرواژه که در AP پیکربندی شده است، پیاده سازی می شود و هر ایستگاه برای اتصال، به آن گذرواژه احتیاج دارد. بالاتر و فراتر از مشکلی که در اجرای الگوریتم RC4 وجود دارد، هیچگاه امنیت خوبی برای همه دستگاه ها نیست که با استفاده از این روش، گذرواژه یکسانی را به اشتراک بگذارند.

WPA

برای پرداختن به دغدغه گسترده و عدم کفایت WEP، اتحادیه Wi-Fi، گروهی از تولیدکنندگان که قابلیت همکاری را فراهم کردن، مکانیسمی جایگزین به نام Wi-Fi Protected Access (WPA) دسترسی محافظت شده وای فای که برای بهبود در WEP طراحی شده است، ایجاد کردند. چهار نوع WPA وجود دارد، اما ابتدا اجازه دهید در مورد چگونگی بهبود نسخه اصلی نسبت به WEP بحث کنیم.

در مرحله اول، WPA از پروتکل یکپارچگی کلیدی Temporal Key Integrity Protocol (TKIP) برای رمزگذاری استفاده می کند، که یک کلید جدید برای هر بسته ایجاد می کند. دوم، بررسی یکپارچگی مورد استفاده با WEP قادر به تشخیص هرگونه تغییر در داده ها است WPA. از الگوریتم بررسی یکپارچگی پیام به نام مایکل برای تأیید یکپارچگی بسته ها استفاده می کند. دو نسخه WPA وجود دارد.

برخی از دستگاه های میراثی یا همان ورژن قدیمی تر فقط ممکن است WPA را پشتیبانی کنند. همیشه باید با سازندگان دستگاه بررسی کنید تا دریابید که چه امنیتی آزاد شده Released است که امکان پشتیبانی WPA2 را فراهم کند.

WPA2

WPA2 پیشرفته تر نسبت به WPA است. WPA2 از حالت پیشخوان رمزگذاری

Counter Cipher Mode

با پروتکل کد احراز هویت پیام زنجیره ای

Chaining Message Authentication Code Protocol (CCMP)

بر اساس استاندارد رمزگذاری پیشرفته (AES) Advanced Encryption Standard استفاده

می‌کند، نه براساس TKIP. AES یک روش بسیار قوی تر است و برای انتقال‌های سازگار با

استانداردهای پردازش اطلاعات فدرال (FIPS) ضروری است و همچنین دو نسخه WPA2 وجود

دارد (در قسمت بعدی پوشش داده شده است).

شخصی در مقابل سازمانی Personal Versus Enterprise

WPA و WPA2 نسخه‌های شخصی و سازمانی هستند. نسخه‌های سازمانی با استفاده از یک سرور

احراز هویت که به طور معمول به یک سرور RADIUS نیاز دارند. نسخه‌های شخصی از

گذرواژه‌های تنظیم شده در AP و ایستگاه‌ها استفاده نمی‌کنند. جدول ۴-۴ خلاصه‌ای از WPA

و WPA2 را ارائه می‌دهد.

Variant	Access Control	Encryption	Integrity
WPA Personal	Preshared key	TKIP	Michael
WPA Enterprise	802.1X (RADIUS)	TKIP	Michael
WPA2 Personal	Preshared key	CCMP, AES	CCMP
WPA2 Enterprise	802.1X (RADIUS)	CCMP, AES	CCMP

جدول ۴-۴: WPA و WPA2

پخش SSID

موضوعات مربوط به پخش SSID در بخش "ساختار WLAN" در ابتدای این فصل آمده است.

فیلتر MAC

یکی دیگر از اقدامات امنیتی که معمولاً مورد بحث قرار می‌گیرد، ایجاد لیستی از آدرس‌های

MAC مجاز در AP است. وقتی این کار انجام شد، فقط دستگاه‌هایی که آدرس MAC را در

لیست دارند می توانند با AP ارتباط برقرار کنند. اگرچه در سطح (Surface) قرار دارد، ممکن است این یک معیار امنیتی خوبی به نظر برسد، در حقیقت یک هکر می تواند به راحتی از یک Sniffer برای یادگیری آدرس های MAC دستگاه هایی که با موفقیت تأیید شده اند، استفاده کند. سپس با تغییر آدرس MAC در دستگاه خود به یکی از لیست های موجود، می تواند ورود کند.

فیلترهای MAC همچنین می توانند پیکربندی شوند تا دسترسی به دستگاه های خاص را انکار کنند. عامل محدود کننده در این روش این است که فقط دستگاه هایی که آدرس های MAC را رد کرده اند از دسترسی خاص محروم هستند. همه اتصالات دیگر مجاز خواهد بود.

رمزنگاری ارتباطات Communications Cryptography

رمزگذاری Encryption می تواند بر اساس سطح ارتباطی مورد استفاده، حفاظت متفاوتی را ارائه دهد. دو نوع سطح ارتباط رمزگذاری، رمزگذاری پیوند Link Encryption و رمزگذاری پایان به پایان End-to-End Encryption است.

• رمزگذاری پیوند Link Encryption

رمزگذاری پیوند تمام داده هایی را که از طریق پیوند منتقل می شوند را رمزگذاری می کند. در این نوع ارتباطات، تنها بخشی از بسته که رمزگذاری نشده است، اطلاعات کنترل پیوند داده ها است که برای اطمینان از انتقال صحیح داده ها، لازم است. تمام اطلاعات رمزگذاری می شوند، با هر روتر یا دستگاه دیگر اطلاعات هدر آن رمزگشایی می شود تا بتواند مسیریابی رخ دهد و دوباره قبل از ارسال اطلاعات به دستگاه بعدی رمزگذاری مجدد شود.

اگر طرف فرستنده باید تضمین که امنیت داده و حفظ حریم خصوصی از طریق یک ارتباط عمومی حفظ می شود، باید از رمزگذاری پیوند استفاده شود. این روش اغلب برای محافظت از ارتباطات ایمیلی مورد استفاده قرار می گیرد یا وقتی بانک ها یا موسسات دیگری که داده های محرمانه ای را دارند باید آن داده ها را از طریق اینترنت ارسال کنند.

رمزگذاری پیوند در برابر بسته اسنیفرها و سایر اشکال استراق سمع محافظت می شود و در لایه پیوند داده ها و لایه فیزیکی مدل OSI رخ می دهد. مزایای رمزگذاری پیوند شامل: کلید داده ها رمزگذاری می شوند و هیچ گونه تعامل کاربر برای استفاده، لازم نیست. معایب رمزگذاری پیوند شامل موارد زیر است: هر دستگاهی که داده ها باید از طریق آن منتقل شوند باید کلید را دریافت

کنند، تغییرات کلیدی باید به هر دستگاه در مسیر منتقل شوند و بسته‌ها در هر دستگاه رمزگشایی می‌شوند.

• رمزگذاری پایان به پایان End-to-End Encryption

رمزگذاری پایان به پایان رمزگذاری اطلاعات بسته، کمتر از رمزگذاری پیوند است. در رمزگذاری پایان به پایان، اطلاعات مسیریابی بسته و همچنین هدرها و آدرسهای آنها رمزگذاری نمی‌شوند. این امر به هکرها بالقوه امکان می‌دهد اگر در یک بسته از طریق خراب کردن بسته یا استراق سمع اطلاعات بدست آورند، اطلاعات بیشتری را کسب کنند. رمزگذاری پایان به پایان چندین مزیت دارد. کاربر معمولاً رمزگذاری پایان به پایان را آغاز می‌کند، به کاربر اجازه می‌دهد که دقیقاً چی رمزگذاری شده و چگونه رمزگذاری شده را انتخاب کند. این روش عملکرد هر دستگاه را در طول مسیر تأثیر کمتری از رمزگذاری پیوند می‌گذارد زیرا هر دستگاه برای تعیین نحوه مسیریابی بسته لازم نیست رمزگذاری / رمزگشایی انجام دهد. نمونه‌ای از رمزگذاری پایان به پایان، IPsec است.

امنیت ایمیل Email Security

نامه الکترونیکی به بخشی جدایی ناپذیر از زندگی تقریباً هر شخص تبدیل شده است، به خصوص که مربوط به ارتباطات کسب و کار آنها است. اما بسیاری از پیاده سازی‌های ایمیل بدون امنیت سیستم رمزگذاری، امضاهای دیجیتالی یا کلیدها، امنیت بسیار کمی را ارائه می‌دهند. به عنوان مثال، صحت ایمیل و محرمانه بودن با امضای پیام با استفاده از کلید خصوصی فرستنده و رمزگذاری پیام با کلید عمومی گیرنده ارائه می‌شود. در بخش‌های بعدی، به طور مختصر درباره استانداردهای ایمیل PGP، MIME و S / MIME که در دنیای امروز رایج هستند صحبت می‌کنیم و همچنین مختصراً از رمزنگاری کوانتومی توضیح می‌دهیم.

PGP

حریم بسیار خصوصی Pretty Good Privacy (PGP) رمزگذاری ایمیل را از طریق اینترنت فراهم می‌کند و از فن آوری‌های مختلف رمزگذاری بر اساس نیاز سازمان استفاده می‌کند. PGP می‌تواند محرمانه، یکپارچگی و احراز هویت را مبتنی بر روش‌های رمزگذاری بکارگیرد.

PGP مدیریت کلید را با استفاده از RSA فراهم می کند، PGP از وب اعتماد Web of Trust برای مدیریت کلیدها استفاده می کند. با به اشتراک گذاشتن کلیدهای عمومی، کاربران به جای اتکا به CA، وب اعتماد را ایجاد می کنند. کلیدهای عمومی کلید کاربران در یک حلقه کلید فایل در رایانه هر کاربر ذخیره می شوند. در داخل آن فایل، به هر کاربر سطح اعتماد داده می شود. کاربران درون وب برای یکدیگر ضمانت می دهند. بنابراین اگر کاربر ۱ و کاربر ۲ رابطه اعتماد Trust دارند و کاربر ۱ و کاربر ۳ رابطه اعتماد Trust دارند، کاربر ۱ می تواند دو کاربر دیگر را به یکدیگر توصیه کند. کاربران می توانند سطح اعتماد را در ابتدا به کاربر اختصاص دهند اما در صورت ضمانت تغییر شرایط می توانند بعداً آن سطح را تغییر دهند. اما به خطر انداختن کلید عمومی کاربر در سیستم PGP بدین معنی است که کاربر باید با هر کسی که کلید خود را به اشتراک گذاشته است تماس گرفته تا مطمئن شود که این کلید از فایل حلقه کلید حذف شده است.

PGP رمزگذاری داده ها را برای محرمانه بودن با استفاده از IDEA فراهم می کند. با این حال، الگوریتم های رمزگذاری دیگر قابل استفاده هستند. اجرای PGP با MD5 یکپارچگی داده ها را فراهم می کند. گواهی نامه های عمومی با PGP تأیید اعتبار (احراز هویت) می کنند.

MIME , S/MIME

برنامه افزودنی ایمیل چند منظوره (MIME) Multipurpose Internet Mail Extension یک استاندارد اینترنتی است که به ایمیل امکان می دهد پیوست های غیر متنی، مجموعه کاراکترهای غیر ASCII، بدنه پیام چند قسمت، اطلاعات مربوط به هدر غیر ASCII را در اختیار شما قرار دهد. در دنیای امروز، SMTP با فرمت MIME بیشتر ایمیل را منتقل می کند.

MIME به ایمیل مشتری اجازه می دهد تا یک پیوست را با یک هدر برای توصیف نوع فایل ارسال کند. سیستم دریافت کننده از این هدر و پسوند فایل موجود در آن برای شناسایی نوع پیوست و باز کردن اپلیکیشن مرتبط استفاده می کند و اجازه می دهد تا رایانه هنگامی که کاربر دوبار کلیک روی پیوست می کند، اپلیکیشن مناسب را راه اندازی کند. اگر هیچ اپلیکیشنی با آن نوع فایل مرتبط نباشد، کاربر می تواند اپلیکیشن را با استفاده از گزینه Open With یا وب سایت ممکن است اپلیکیشن لازم را انتخاب کند.

امنیت (S / MIME) MIME به MIME اجازه می دهد تا پیام های ایمیل رمزگذاری کرده و پیوست های دیجیتالی را نیز رمزگذاری و به صورت دیجیتالی انجام دهد. این استاندارد به استانداردهای رمزنگاری کلید عمومی (PKCS)، که مجموعه ای از استانداردهای رمزنگاری کلید

عمومی که توسط صاحبان الگوریتم RSA طراحی شده است، پایبند می‌باشد. S / MIME از رمزگذاری برای تأمین محرمانگی، هوشیاری برای تهیه یکپارچگی، گواهی نامه کلید عمومی برای احراز هویت و خلاصه کردن پیام برای تهیه عدم تکذیب استفاده می‌کند.

رمزنگاری کوانتومی Quantum Cryptography

رمزنگاری کوانتومی روشی برای رمزگذاری است که فیزیک کوانتومی و رمزنگاری را در هم می‌آمیزد و امکان فاکتورگیری محصولات با شماره‌های بزرگ اول را ارائه می‌دهد. رمزنگاری کوانتومی رمزگذاری قوی و تشخیص استراق سمع را فراهم می‌کند. این یک انتخاب عالی برای هر سازمانی است که داده‌های مخفی برتر، مثلاً داده‌های دولت ایالات متحده را منتقل کند.

امنیت اینترنت Internet Security

شبکه جهانی وب مجموعه‌ای از سرورهای HTTP است که وب سایت‌ها و خدمات آنها را مدیریت می‌کنند. اینترنت شبکه‌ای است که شامل کلیه دستگاه‌های فیزیکی و پروتکل‌هایی است که از طریق آن ترافیک وب منتقل می‌شود. مرورگر وب استفاده شده به کاربران اجازه می‌دهد صفحات وب را از طریق HTTP بخوانند. مرورگرها می‌توانند پروتکل‌های زیادی را بخوانند. هر پروتکل که محلی نیست توسط مرورگر وب پشتیبانی نمی‌شود، فقط با نصب یک افزونه یا اپلیکیشن ناظر، قابل خواندن است، در نتیجه نقش مرورگر گسترش می‌یابد. در بحث امنیت اینترنت، موضوعات زیر را شامل می‌شود:

- Remote access -
- SSL/TLS -
- HTTP, HTTPS, and SHTTP -
- SET -
- Cookies -
- SSH -
- IPsec -

دسترسی از راه دور Remote access

اپلیکیشن های دسترسی از راه دور به کاربران این امکان را می دهد تا از یک اتصال از راه دور به منابع یک سازمان دسترسی پیدا کنند. این اتصالات از راه دور می توانند ارتباط مستقیم با شماره گیری dial-in داشته باشند اما به طور فزاینده ای از اینترنت به عنوان شبکه ای که داده ها از آنها انتقال می یابد، استفاده می کنند. اگر یک سازمان امکان دسترسی از راه دور به منابع داخلی را فراهم کند، هنگام انتقال داده ها بین سرویس مشتری (Client) دسترسی از راه دور و سرور دسترسی از راه دور، سازمان باید تضمین کند که داده ها با استفاده از رمزگذاری حفاظت می شوند. سرورهای دسترسی از راه دور می توانند به اتصالات رمزگذاری شده با کلاینت های دسترسی از راه دور احتیاج داشته باشند، به این معنی که هرگونه تلاش اتصال که از رمزگذاری استفاده نمی کند، رد خواهد شد.

SSL / TLS

لایه های سوکت امن (Secure Sockets Layer (SSL یک پروتکل لایه انتقال است که رمزگذاری، احراز هویت سرور / مشتری و یکپارچگی پیام را فراهم می کند. SSL توسط Netscape برای انتقال اسناد خصوصی از طریق اینترنت ساخته شده است. در حالی که SSL رمزگذاری ۴۰ بیتی (SSL 2.0) یا رمزگذاری ۱۲۸ بیتی (SSL 3.0) اجرا می کند، نسخه ۴۰ بیتی به دلیل اندازه کلید محدود، مستعد حمله است. SSL به یک اپلیکیشن اجازه می دهد تا ارتباطات رمزگذاری شده و تأیید شده را در سراسر شبکه داشته باشد.

امنیت لایه انتقال (Transport Layer Security (TLS یک استاندارد جامعه باز است که بسیاری از خدمات مشابه SSL را ارائه می دهد. TLS 1.0 مبتنی بر SSL 3.0 است اما قابل گسترش می باشد. هدف اصلی TLS حفظ حریم خصوصی و یکپارچگی داده ها بین دو اپلیکیشن ارتباطی است.

TLS 1.1 بروزرسانی TLS 1.0 بود که محافظت در برابر حملات زنجیره رمزگذاری -Cipher block chaining (CBC) را انجام می داد. TLS 1.2 از MDS-SHA-1 به کمک توابع شبه تصادفی PRF استفاده می کند. TLS 1.3، هنوز هم به شکل پیش نویس (Draft) این نوشتار، باید حمایت از منحنی های بیضوی ضعیف تر را حذف کند.

SSL و TLS معمولاً هنگام استفاده از رمزگذاری داده ها هنگام انتقال از طریق یک رسانه از یک سیستم به سیستم دیگر، مورد استفاده قرار می گیرند.

HTTP, HTTPS, S-HTTP

پروتکل انتقال (HTTP) Hypertext پروتکل مورد استفاده در وب برای انتقال داده‌های وب سایت بین وب سرور و یک مشتری (کلاینت) وب است. با هر آدرس جدیدی که به مرورگر وب وارد شود، خواه از ورود کاربر اولیه و یا با کلیک روی پیوندی روی صفحه نمایش داده شده، اتصال جدیدی برقرار می‌شود زیرا HTTP یک پروتکل بدون تابعیت است.

HTTP Secure (HTTPS) اجرای HTTP در حال اجرا بر روی پروتکل SSL / TLS است که با استفاده از گواهینامه دیجیتال سرور یک جلسه امن ایجاد می‌کند. SSL / TLS جلسه را با استفاده از یک کانال امن نگه می‌دارد. وب سایت‌های HTTPS همیشه در ابتدای آدرس شامل https:// می‌باشد.

اگرچه به نظر بسیار مشابه می‌رسد، اما امنیت (S-HTTP) HTTP از ارتباط HTTP به روشی متفاوت محافظت می‌کند. S-HTTP فقط یک پیام ارتباطی را رمزگذاری می‌کند، نه یک جلسه کامل (یا مکالمه).

S-HTTP به اندازه HTTPS مرسوم نیست.

تنظیم SET

تراکنش الکترونیکی امن (SET) Secure Electronic Transaction، که توسط ویزا و مستر کارت ارائه شده است، اطلاعات تراکنش کارت اعتباری را از طریق اینترنت تضمین می‌کرد و مبتنی بر گواهینامه‌های X.509 و کلیدهای نامتقارن بود. برای ارسال اطلاعات کارت اعتباری رمزگذاری شده از یک کیف پول الکترونیکی در رایانه کاربر استفاده می‌کرد. اما برای اجرای کامل، این مجموعه نیاز به همکاری کامل موسسات مالی، کاربران کارتهای اعتباری، مؤسسات عمده فروشی و خرده فروشی و دروازه پرداخت داشت و هرگز به طور کامل تصویب نشد.

ویزا اکنون پروتکل Secure 3-D را تبلیغ می‌کند. در سال‌های اخیر، تکنولوژی پردازش کارت اعتباری / بدهی Credit/Debit card دستگاه سیار، از جمله Apple Pay و Samsung Pay، گزینه‌های رایج هستند.

Cookies

کوکی‌ها فایل‌های متنی هستند که در هارد دیسک یا حافظه کاربر ذخیره می‌شوند. این فایل‌ها اطلاعات را درمورد عادات اینترنت کاربر، از جمله مرور و فرستادن اطلاعات ذخیره می‌کنند. از

آنجا که وب سرورهای سایت نحوه استفاده از کوکی ها را تعیین می کنند، سایت های مخرب می توانند از کوکی ها برای کشف مقدار زیادی از اطلاعات در مورد یک کاربر استفاده کنند. اگرچه اطلاعات موجود در کوکی ها در هارد دیسک معمولاً هیچگونه اطلاعات محرمانه ای را شامل نمی شود، اما می توان از آن استفاده کرد برای بدست آوردن اطلاعاتی در مورد یک کاربر که می تواند به یک مهاجم کمک کند تا یک حمله هدفمند بهتر را ترتیب دهد. به عنوان مثال، اگر کوکی ها برای مهاجمان فاش کردند که کاربر به طور روزانه به وب سایت عمومی بانک خاص دسترسی پیدا می کند، این اقدام می تواند نشان دهد که کاربر در آن بانک یک حساب کاربری دارد، در نتیجه حمله کننده با استفاده از یک ایمیل اقدام به حمله فیشینگ می کند که به نظر می رسد از کاربر قانونی در بانک می باشد.

بسیاری از برنامه های آنتی ویروس یا ضد بدافزار شامل عملکردی هستند که به شما امکان می دهد نوع کوکی های دانلود شده را محدود کنید و اطلاعات شناسایی شخصی PII مانند آدرس های ایمیل را مخفی کنید. اغلب این نوع تضمین ها بیش از آنچه ارزششان را دارد، مشکلاتی ایجاد می کنند، زیرا اغلب بر ارتباطات قانونی اینترنتی تأثیر می گذارند.

SSH

پوسته امن (SSH) Secure Shell یک اپلیکیشن و پروتکل است که برای ورود به سیستم از راه دور به یک رایانه دیگر با استفاده از یک تونل امن صورت می گیرد. بعد از برقراری کانال امن پس از تعویض کلید جلسه، کلیه ارتباطات بین دو رایانه از طریق کانال امن رمزگذاری می شود.

IPsec

امنیت پروتکل اینترنت (IPsec) Internet Protocol Security مجموعه ای از پروتکل ها است که یک کانال امن بین دو دستگاه برقرار می کند. IPsec معمولاً از طریق VPN ها پیاده سازی می شود. IPsec با تعیین الگوریتم های استفاده شده و اجرای کلیدهای رمزنگاری مورد نیاز IPsec، از تجزیه و تحلیل ترافیک محافظت می کند.

IPsec شامل هدر احراز هویت (AH)، بار امنیتی کپسوله کردن Encapsulating Security Payload (ESP) و انجمن های امنیتی است. AH احراز هویت و یکپارچگی را فراهم می کند، در حالی که ESP احراز هویت، یکپارچگی و رمزگذاری (محرمانه بودن) را فراهم می کند. یک انجمن امنیتی (SA) Security Association سابقه ای از پیکربندی دستگاه است که نیاز به مشارکت در

ارتباطات IPsec دارد. شاخص پارامتر امنیتی (SPI) Security parameter index نوعی جدول است که SAهای مختلف مورد استفاده را ردیابی می‌کند و اطمینان می‌دهد که یک وسیله از SA مناسب برای ارتباط با دستگاه دیگر استفاده می‌کند. هر دستگاه SPI مخصوص به خود را دارد.

IPsec در یکی از دو حالت اجرا می‌شود: حالت انتقال یا حالت تونل. حالت انتقال فقط از بار پیام محافظت می‌کند، در حالی که حالت تونل از بار، مسیریابی و اطلاعات هدر محافظت می‌کند. هر دوی این حالت‌ها می‌توانند برای ارتباطات IPsec از دروازه به دروازه یا میزبان به دروازه (Gateway-to-Gateway, Host-to-Gateway) استفاده کنند.

IPsec تعیین نمی‌کند که الگوریتم رمزگذاری یا هشینگ استفاده می‌شود. تبادل کلید اینترنتی IKE (Internet Key Exchange) که ترکیبی از OAKLEY و انجمن امنیت اینترنت و پروتکل مدیریت کلید ISAKMP است، یک روش تبادل کلیدی است که بیشتر توسط IPsec استفاده می‌شود. اوکلی یک پروتکل تأسیس کلیدی مبتنی بر دیفی هلمن است که توسط IKE کنار گذاشته شد. ISAKMP برای راه اندازی و مدیریت انجمنهای امنیتی (SA)ها تأسیس شد. IKE با IPsec احراز هویت و تبادل کلید را ارائه می‌دهد.

روش احراز هویت استفاده شده توسط IKE با IPsec شامل کلیدهای از قبل مشترک، گواهی نامه‌ها و احراز هویت کلید عمومی است. امن ترین پیاده سازی کلیدهای از پیش اشتراکی به یک PKI نیاز دارد. اما اگر یک کلید از قبل به اشتراک گذاشته شده مبتنی بر رمزهای ساده باشد، یک PKI ضروری نیست.

مؤلفه‌های شبکه امن

یک سازمان می‌تواند اجزای شبکه را تضمین کند تا از دارایی‌های شبکه آن محافظت شود. اگر یک سازمان نتواند به درستی این مؤلفه‌ها را تأمین کند، تمام ترافیک موجود در شبکه به خطر می‌افتد. اجزای شبکه شامل سخت افزار، رسانه انتقال، دستگاه‌های کنترل دسترسی به شبکه، امنیت نقطه انتهایی Endpoint و شبکه‌های توزیع محتوا Content-distribution networks هستند.

سخت افزار Hardware

در هنگام تأمین امنیت اجزای شبکه، متخصصان امنیت باید کلیه دستگاههای شبکه را به عنوان بخشی از یک راه حل امنیتی جامع در نظر بگیرند. این دستگاهها شامل پیچ پانل ها، مالتی پلکسرها، هاب ها، سوئیچ ها و VLAN ها، روترها، دروازه ها، فایروال ها، سرورهای پروکسی، PBX ها، Honeypot ها، IDS ها و IPS ها هستند. درک مسیریابی شبکه، از جمله کلیه پروتکل های مسیریابی، نیز بسیار اهمیت دارد. در این بخش در مورد همه این مؤلفه ها بحث شده است.

دستگاه های شبکه Network Devices

دستگاه های شبکه در تمام لایه های مدل OSI فعالیت می کنند. لایه ای که در آن فعالیت می کنند درباره سطح هوشمندی آنها و انواع اطلاعات مورد استفاده هر دستگاه، به طور کامل آشکار است. در این بخش دستگاه های رایج و نقش های مربوط به آنها در تصویر کلی ارائه شده است.

Patch Panel

پیچ پانل های در لایه Physical لایه ۱ مدل OSI کار می کنند و به سادگی به عنوان یک نقطه خاتمه مرکزی برای کلیه کابل هایی که از دیوارها عبور می کنند، فعالیت می کنند، که به نوبه خود به رایانه هایی با کابل وصل می شوند. کابل های در حال عبور از دیوارها به صفحه پیچ به طور دائم به پانل وصل می شوند. سپس از کابل های کوتاه به نام کابل های پیچ برای اتصال هر پورت پانل به یک سوئیچ یا هاب استفاده می شود. نکته اصلی که باید در مورد پیچ پانل ها نگران کننده است، امنیت فیزیکی آنها است. آنها باید در یک اتاق قفل دار یا کمد قرار گیرند.

مولتی پلکسر Multiplexer

مولتی پلکسر یک وسیله در لایه فیزیکی (لایه ۱) است که چندین سیگنال اطلاعات ورودی را با استفاده از برخی تکنیک های مولتی پلکسر، در یک سیگنال خروجی، که حامل چندین کانال ارتباطی است، قرار می دهد. در مقابل، یک Demultiplexer یک سیگنال ورودی واحد را حمل می کند که کانال های زیادی را حمل و آن ها را از سیگنال های خروجی چندگانه جدا می کند. به اشتراک گذاشتن یک محیط فیزیکی یکسان می تواند به چند روش مختلف انجام شود: بر اساس فرکانس های مورد استفاده (تقسیم فرکانس چند برابر یا FDM) یا با استفاده از اسلات های زمانی (تقسیم زمان چند برابر یا TDM)

Telco Concentrator

نوعی مولتی پلکسر است که چندین کانال را بر روی یک رسانه انتقال منفرد ترکیب می‌کند تا همه کانال‌های فردی به طور همزمان فعال باشند. به عنوان مثال، ISPها از آنها برای ترکیب چندین اتصال dial-up در خطوط سریعتر T-1 استفاده می‌کنند. کنسانتره‌ها همچنین در شبکه‌های LAN برای ترکیب انتقال از یک خوشه نود استفاده می‌کنند. Telco Concentrator از دستگاه‌های لایه ۱ هستند.

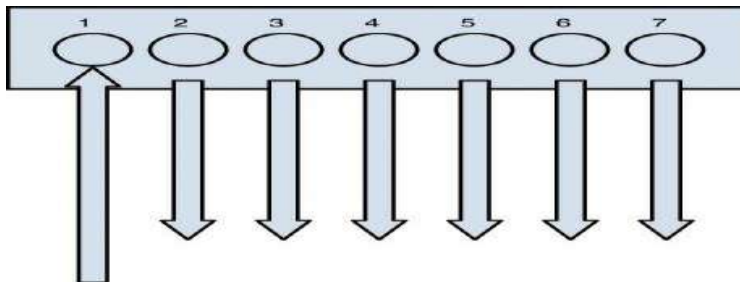
VPN Concentrator

یک کنسانتره شبکه خصوصی مجازی (VPN) ایجاد اتصالات امن VPN و ارسال پیام بین نودهای VPN را فراهم می‌کند. نوعی دستگاه روتر می‌باشد که به طور خاص برای ایجاد و مدیریت زیرساخت‌های ارتباطی VPN ساخته شده است. در لایه Network لایه ۳ کار می‌کند.

هاب Hub

هاب یک دستگاه لایه فیزیکی (لایه ۱) است که به عنوان نقطه اتصال دستگاه‌های توپولوژی ستاره عمل می‌کند. هاب یک دستگاه لایه فیزیکی محسوب می‌شود زیرا هیچگونه هوشمندی ندارد. هنگامی که یک مرکز ترافیک دریافت می‌کند، آن ترافیک را از هر پورت پخش می‌کند زیرا اطلاعاتی برای تصمیم‌گیری در مورد مقصد مورد نظر ندارد.

اگرچه این عمل منجر به برخورد بیشتر و عملکرد ضعیف می‌شود، اما از دیدگاه امنیتی مشکل این است که تمام ترافیک را به کلیه پورت‌ها پخش می‌کند. Sniffer متصل به هر پورت قادر خواهد بود تا همه ترافیک را گوش کند. عملکرد یک هاب در شکل ۴-۱۴ نشان داده شده است. هنگامی که سوئیچ استفاده می‌شود، این مشکل وجود ندارد (بیشتر در مورد بعدی).



شکل ۴-۱۴: هاب

Repeater

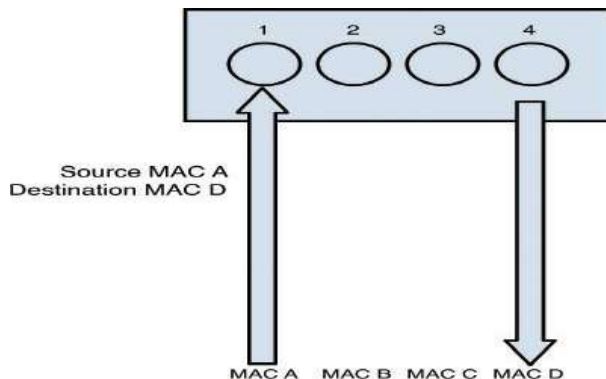
دستگاهی است که برای افزایش فاصله یک شبکه استفاده می شود. از آنجا که قدرت سیگنال با زیاد شدن فاصله کم می شود، در صورت نیاز به گسترش فاصله شبکه که بیشتر از حد مجاز از نوع کابل است، باید از Repeater استفاده شود.

پل یا Bridge

دستگاه هایی در لایه ۲ هستند که ترافیک بین بخش های شبکه را بر اساس آدرس های MAC فیلتر می کنند. Bridge ها از انتقال فریم ها از شبکه محلی به خارج از شبکه محلی منتقل می شوند جلوگیری می کنند، اما آنها همه پخش های (Broadcast) شبکه را به جلو هدایت می کنند. پلها می توانند LAN هایی را که از رسانه های مختلفی استفاده می کنند، مانند اتصال شبکه UTP به شبکه فیبر نوری متصل کنند. برای تأمین امنیت، Bridge ها باید نوعی رمزگذاری لایه پیوند را پیاده سازی کرد.

سوئیچ Switch

سوئیچ ها بسیار شبیه Bridge ها هستند. آنها هوشمند هستند و در لایه ۲ مدل OSI کار می کنند. ما می گوییم که آنها در این لایه برنامه ریزی می کنند زیرا تصمیم گیری های سوئیچینگ را بر اساس آدرس های MAC انجام می دهند، که در لایه ۲ ساکن هستند. شکل ۴-۱۵ این روند را نشان می دهد.



شکل ۴-۱۵

سوئیچ‌ها عملکرد را نسبت به هاب‌ها بهبود می‌بخشند زیرا تصادم Collisions را از بین می‌برند. هر پورت سوئیچ، دامنه تصادم مخصوص به خود قرار دارد، در حالی که تمام پورت‌های یک هاب در یک دامنه دارای تصادم یکسان هستند. از دیدگاه امنیتی، سوئیچ‌ها از این نظر امن تر هستند که یک Sniffer متصل به هر پورت تنها قادر به ضبط ترافیکی است که برای آن پورت در نظر گرفته شده است.

سوئیچ‌ها نسبت به Bridgeها و هاب‌ها بسیار گران تر، سریع تر و سخت تر هستند. Bridge و سوئیچ هر دو عملکرد بهتری نسبت به هاب‌ها دارند. با این حال برخی سوئیچ‌ها هم روتر و هم سوئیچ هستند و در این حالت ما آنها را جز لایه ۳ سوئیچ می‌نامیم زیرا عملیات مسیره‌ی و سوئیچ کردن را انجام می‌دهند.

سوئیچ لایه ۳ در مقابل لایه ۴

به طور معمول فرآیند سویچینگ در لایه ۲ مدل OSI ترسیم می‌شود زیرا از آدرس‌های لایه ۲ برای تصمیم گیری در مورد ارسال فریم استفاده می‌شود. این بدان معنا نیست که یک دستگاه فیزیکی منفرد قادر به انجام هر دو عملکرد نیست. سوئیچ لایه ۳ دستگاهی است که عملکرد مسیریابی نیز در آن ساخته شده است. هم می‌تواند مسیر را تغییر دهد و هم سوئیچ کند و هم می‌تواند دو عملکرد را به صورت یکپارچه ترکیب کند به گونه‌ای که با ورود اولین بسته و سپس بقیه بسته‌ها می‌تواند یک جریان داده را مسیریابی کند و همین‌طور جریان را می‌تواند سریع تغییر داده و در نتیجه عملکرد بهتری حاصل شود.

سوئیچ‌های لایه ۴ با ارائه مسیریابی اضافی در بالای لایه ۳ با استفاده از شماره‌های پورت موجود در هدر لایه انتقال، برای تصمیم گیری‌های مسیریابی، قدم را فراتر می‌گذارند. بزرگترین فواید سوئیچ لایه ۴ امکان اولویت بندی ترافیک داده با استفاده از اپلیکیشن است، به این معنی که کیفیت خدمات (QoS) را می‌توان برای هر کاربر تعریف کرد.

VLANها

سوئیچ‌های سطح سازمانی قابلیت عملکرد دیگری به نام شبکه‌های محلی مجازی (VLAN) را نیز دارند. آنها زیرمجموعه‌های منطقی سوئیچ هستند که پورت‌ها را از یکدیگر جدا می‌کنند مثل اینکه در LANهای مختلف قرار دارد. این VLANها همچنین می‌توانند چندین سوئیچ را داشته

باشند، به این معنی که دستگاه های متصل به سوئیچ ها در قسمت های مختلف شبکه می توانند بدون در نظر گرفتن موقعیت فیزیکی در همان VLAN قرار بگیرند. VLAN روش دیگری برای اضافه کردن لایه جداسازی بین دستگاه های حساس و بقیه شبکه ارائه می دهد. به عنوان مثال، اگر فقط دو دستگاه قادر به اتصال به سرور HR باشند، این دو دستگاه و سرور HR می توانند در یک VLAN، جدا از سایر VLAN ها قرار بگیرند. ترافیک بین VLAN فقط از طریق روتر امکان پذیر است. از روترها می توان برای اجرای ACL های استفاده کرد که کنترل ترافیک مجاز بین VLAN ها را کنترل می کنند.

مسیریاب (روتر) Router

روترها در لایه ۳ (لایه شبکه) فعالیت می کنند وقتی که ما در مورد عملکرد مسیریابی ایزوله بحث می کنیم. دستگاه های خاص می توانند عملکرد مسیریابی را با سوئیچینگ و فیلتر لایه ۴ ترکیب کنند. اما، از آنجا که مسیریابی برای تصمیم گیری از اطلاعات لایه ۳ (آدرس IP) استفاده می کند، یک عملکرد لایه ۳ است.

روترها از یک جدول مسیریابی استفاده می کنند که به روتر می گوید برای هدایت ترافیک برای یک شبکه خاص، از کدام جهت حرکت کند. اگرچه روترها را می توان با مسیرها به رایانه های شخصی پیگیربندی کرد، اما به طور معمول آنها به سمت شبکه ها حرکت می کنند، نه به رایانه های جداگانه. هنگامی که بسته وارد روتر شد که به طور مستقیم به شبکه مقصد وصل شده است، آن روتر خاص پخش ARP را انجام می دهد تا آدرس MAC رایانه را یاد بگیرد و بسته ها را به صورت فریم در لایه ۲ ارسال کند.

روترها یک عملکرد مهم امنیتی را انجام می دهند، زیرا ACL ها بر روی آنها به صورت رایج تنظیم شده اند. این مجموعه قوانین تنظیم شده که باعث کنترل ترافیک مجاز یا عدم استفاده از یک مسیر از طریق روتر می شود. این قوانین می توانند در لایه ۳ عمل کنند که این تصمیمات را براساس آدرس های IP یا در لایه ۴ در صورت مجاز بودن انواع خاصی از ترافیک انجام دهد. هنگامی که این کار انجام شد، ACL به طور معمول به تعداد پورت سرویس یا اپلیکیشنی که مجاز یا رد شده است Denied، Allowed مراجعه می کند.

روترهای مرزی با میزبانهای خارجی (External Hosts) ارتباط برقرار می کنند تا میزبانهای خارجی بتوانند به میزبان داخلی متصل شوند. روترهای داخلی با میزبان داخلی ارتباط برقرار می کنند تا بتوانند به میزبان داخلی دیگر متصل شوند. تنظیمات امنیتی روترهای مرزی بسیار

حیاتی است زیرا آنها باید از ترافیک خارجی فیلتر شوند تا از دسترسی ناخواسته به شبکه داخلی جلوگیری شود.

دروازه Gateway

اصطلاح Gateway به دستگاه خاصی اطلاق نمی‌شود بلکه به هر دستگاهی که نوعی ترجمه را انجام دهد یا به عنوان یک نقطه کنترل برای ورود و خروج عمل کند. یک نمونه از دستگاه‌هایی که به عنوان یک دروازه کار می‌کنند یک سرور ایمیل خواهد بود که همه نوع سرورهای ایمیل (Exchange, IBM Notes, Novell GroupWise)، ایمیل دریافت می‌کند و ترجمه‌ای از فرمت‌های لازم را بین این اجراهای مختلف انجام می‌دهد. مثال دیگر سرور دسترسی به شبکه یا (NAS) Network Access Server است که دسترسی به یک شبکه را کنترل می‌کند. این یک دروازه در نظر گرفته می‌شود که ممکن است نیاز داشته باشد تا قبل از اجازه ورود، همه ترافیک را احراز هویت کند. این نوع سرورها حتی ممکن است خود رایانه‌ها را برای آخرین نسخه‌های امنیتی و بروزرسانی‌ها قبل از ورود بررسی کنند.

فایروال‌ها

دستگاه شبکه‌ای که شاید بیشترین ارتباط را با ایده امنیت داشته باشد، فایروال است. فایروال‌ها می‌توانند برنامه‌های نرم افزاری باشند که بر روی سیستم عامل‌های سرور نصب شده اند یا می‌توانند تجهیزاتی باشند که سیستم عامل خاص خود را دارند. در هر دو صورت کار آنها بازرسی و کنترل نوع ترافیک مجاز است. فایروال‌ها را می‌توان براساس نوع و نوع معماری آنها مورد بحث قرار داد. آنها همچنین می‌توانند وسیله‌ای فیزیکی باشند یا در یک محیط مجازی وجود داشته باشند. در این بخش از همه زوایا به آنها نگاه می‌شود.

انواع فایروال

وقتی در مورد انواع فایروال‌ها بحث می‌کنیم، بر تفاوت در نحوه عملکرد آنها تمرکز می‌کنیم. برخی از فایروال‌ها نسبت به بقیه، ترافیک کامل تری دارند. معمولاً در عملکرد فایروال و نوع بازرسی که انجام می‌شود، مبادله‌ای وجود دارد. بازرسی عمیق از محتویات هر بسته باعث می‌شود که فایروال تأثیر مخربی بر کارایی داشته باشد و با یک نگاه اجمالی تر به هر بسته تا حدودی

کمتر از عملکردش تأثیر می‌گذارد. به همین دلیل انتخاب خود را از آنچه ترافیک برای بازرسی عاقلانه انجام می‌دهد، با در نظر داشتن این مبادله عنوان می‌کنیم.

فایروال‌های فیلتر بسته بندی Packet filtering firewalls کمترین ضرر را برای کارایی دارند زیرا تنها هدر بسته را برای آدرس‌های IP مجاز یا شماره پورت بازرسی می‌کنند. اگرچه انجام این عملکرد ترافیک را کندتر می‌کند، این کار تنها با نگاه کردن به ابتدای بسته و تصمیم‌گیری سریع مجاز یا غیر مجاز می‌باشد.

اگرچه Packet filtering firewalls عملکرد مهمی دارند، اما نمی‌توانند از انواع بسیاری حملات جلوگیری کنند. آنها نمی‌توانند از Spoofing IP، حملات خاص برای یک اپلیکیشن، حملات وابسته به قطعه قطعه کردن بسته Packet fragmentation یا حمله‌هایی که از TCP دستی استفاده می‌کنند، جلوگیری کنند. برای متوقف کردن این حملات، انواع فایروال پیشرفته‌تری لازم است.

فایروال‌های برجسته Stateful firewalls آنهایی هستند که از عملکرد صحیح دستی TCP (TCP handshake) آگاه هستند، وضعیت همه اتصالات را با توجه به این فرایند پیگیری می‌کنند و می‌توانند تشخیص دهند که چه زمانی بسته‌ها در حال ورود به شبکه هستند که منطقی در رابطه با عملکرد دستی TCP نیست.

برای بازبینی این فرآیند، هرگز نباید بسته‌ای را برای تحویل که دارای پرچم SYN و مجموعه پرچم ACK باشد، بدست آورد، مگر آنکه بخشی از فرآیند Handshake موجود باشد و در پاسخ به بسته‌ای باشد که از داخل شبکه با مجموعه پرچم SYN ارسال می‌شود. این نوع، بسته‌ای است که فایروال برجسته را مجاز نمی‌کند. همچنین این قابلیت را دارد که انواع دیگر حمله را که سعی در سوء استفاده از این فرآیند دارند، تشخیص دهد. این کار را با نگه داشتن یک جدول در مورد کلیه اتصالات فعلی و وضعیت هر فرآیند اتصال انجام می‌دهد و به ما امکان می‌دهد هرگونه ترافیکی را که با وضعیت فعلی اتصال معنا ندارد، تشخیص دهیم. البته حفظ این جدول و مراجعه به جدول باعث می‌شود تا این نوع فایروال تأثیر بیشتری نسبت به یک فایروال فیلتر بسته بندی Packet Filtering Firewall بر عملکرد داشته باشد.

فایروال‌های پروکسی در حقیقت بین هر اتصال از خارج به داخل قرار گرفته و از سمت نقاط انتهایی Endpoints اتصال را برقرار می‌کنند. بنابراین هیچ ارتباط مستقیمی وجود ندارد. فایروال پروکسی به عنوان رله بین دو نقطه انتهایی عمل می‌کند. فایروال‌های پروکسی می‌توانند در دو لایه مختلف مدل OSI کار کنند.

پروکسی‌های سطح مدار Circuit-level proxies در لایه Session همان لایه ۵ مدل OSI کار می‌کنند. آنها تصمیماتی را براساس اطلاعات مربوط به هدر پروتکل و لایه جلسه Session دریافت می‌کنند. از آنجا که آنها بازرسی عمیق بسته را انجام نمی‌دهند در لایه ۷ همان لایه Application، آنها مستقل از اپلیکیشن در نظر گرفته می‌شوند و می‌توانند برای طیف گسترده‌ای از انواع پروتکل لایه ۷ استفاده شوند.

فایروال Socket Secure (SOCKS) نمونه‌ای از فایروال سطح مدار است و نیاز به یک مشتری SOCKS در رایانه‌ها دارد. بسیاری از فروشندگان، نرم افزار خود را با SOCKS ادغام کرده اند تا استفاده از این نوع فایروال آسان تر شود. SOCKS بسته‌های شبکه را از طریق یک سرور پروکسی هدایت می‌کند. SOCKS v5 احراز هویت را به این فرآیند اضافه کرده است. فایروال SOCKS در لایه Session یا لایه ۵ کار می‌کند.

پروکسی‌های سطح اپلیکیشن، بازرسی عمیق بسته را انجام می‌دهند. این نوع فایروال جزئیات فرآیند ارتباطات در لایه ۷ را برای اپلیکیشن قابل درک می‌کند. یک فایروال در سطح اپلیکیشن عملکردی متفاوت برای هر پروتکل دارد. به عنوان مثال، برای HTTP پروکسی قادر خواهد بود ترافیک را بر اساس دستورات خاص HTTP بخواند و فیلتر کند. کار با این لایه مستلزم باز و بسته شدن هر بسته است و این فایروال بیشترین تأثیر را در عملکرد دارد.

فیلتر بسته بندی پویا Dynamic packet filtering بجای توصیف نوع دیگری از فایروال، عملکردی را که یک فایروال ممکن است داشته باشد یا ممکن است در اختیار نداشته باشد را توصیف می‌کند. هنگامی که رایانه‌های داخلی سعی می‌کنند با یک رایانه راه دور جلسه‌ای برقرار کنند، هر دو شماره منبع و مقصد را در بسته قرار می‌دهد. به عنوان مثال، اگر رایانه از وب سرور درخواست کند، مقصد پورت ۸۰ خواهد بود، به خاطر اینکه HTTP از پورت ۸۰ استفاده می‌کند. رایانه مبدا پورت منبع را بطور تصادفی از اعداد موجود در بالای شماره پورت‌های مشهور یا بالاتر از ۱۰۲۳ انتخاب می‌کند. از آنجا که پیش بینی این عدد تصادفی غیرممکن خواهد بود، ایجاد یک قانون فایروال که پیش بینی می‌کند و امکان عبور و مرور از فایروال را در آن پورت تصادفی، غیرممکن خواهد کرد. یک فایروال فیلتر بسته بندی، آن پورت منبع را ردیابی می‌کند و به صورت پویا یک قاعده (Rule) را به لیست اضافه می‌کند تا امکان بازگشت به آن پورت فراهم شود.

هسته پروکسی فایروال نمونه‌ای از فایروال نسل پنجم است. این بسته را در هر لایه از مدل OSI بازرسی می‌کند اما عملکردی را که یک فایروال لایه Application وجود دارد معرفی نمی‌کند

زیرا این کار را در لایه هسته (Kernel) انجام می دهد. همچنین از مدل پروکسی پیروی می کند که بین این دو سیستم قرار گرفته و از طرف آنها اتصالات را ایجاد می کند.

معماری فایروال Firewall Architecture

اگرچه نوع فایروال با عملکرد داخلی فایروال ارتباط برقرار می کند، اما معماری به روشی که فایروال یا فایروال ها در شبکه مستقر شده اند، شکل می گیرد تا یک سیستم حفاظتی ایجاد شود. در این بخش به روشهای مختلفی که می توان دیوار آتش نصب کرد و همچنین نام پیکربندی های مختلف، می پردازیم.

گرچه باستیون هاست ها Bastion hosts در رابطه با دیوارهای آتش در این بحث گنجانده شده اند، اما یک باستیون هاست ممکن است یک فایروال نباشد. این اصطلاح در واقع به موقعیت یک دستگاه اشاره دارد، اگر مستقیماً در معرض اینترنت یا هر شبکه غیرقابل اعتماد قرار بگیرد، ما آن را باستیون هاست می نامیم. کلیه رویه های سخت استاندارد برای این دستگاههای اهمیت ویژه ای دارند. هرگونه خدمات غیر ضروری باید متوقف شود، پورت های غیر ضروری باید بسته شوند و کلیه پچ های امنیتی باید به روز باشند. گفته می شود این رویه ها سطح حمله را کاهش می دهد. اگر یک باستیون هاست مستقر شود، تنها هاست شبکه داخلی است که در معرض شبکه های غیر قابل اعتماد یا اینترنت است. اگر باستیون هاست به طور جداگانه از فایروال مستقر شود، در خارج از فایروال یا در قسمت عمومی ناحیه تقلیل یافته DMZ قرار می گیرد. باستیون هاست همه ترافیک ورودی را فیلتر می کند. فایروال ها و روترها می توانند به صورت باستیون هاست تنظیم شوند.

یک فایروال دوجداره Dual-homed Firewall، که به آن هاست دوگانه Dual-homed Host نیز گفته می شود، از طریق نصب دو کارت واسط شبکه یا NIC، هر دو در یک شبکه مجزا دارای دو واسط شبکه هستند. در بسیاری موارد مسیریابی خودکار بین این واسط ها خاموش است. نرم افزار فایروال ترافیک بین دو واسط را بر اساس قوانین فایروال تنظیم شده توسط ادمین امکان پذیر یا رد می کند. خطر تکیه بر یک فایروال دوگانه منفرد این است که یک نقطه شکست وجود دارد. اگر این دستگاه بخطر بیفتد، شبکه نیز بخطر می افتد. در صورت بروز حمله Denial-of-Service (DoS)، هیچ ترافیکی عبور نخواهد کرد که وضعیت خوبی نیست.

در بعضی موارد ممکن است فایروال چند خانه‌ای باشد. یکی از انواع رایج، فایروال سه پا Three-legged Firewall است. این تنظیمات دارای سه واسط می‌باشد یکی به شبکه غیر قابل اعتماد Untrusted Network، یکی به شبکه داخلی و دیگری به DMZ.

یک DMZ، همچنین به عنوان زیر شبکه نمایش داده می‌شود، بخشی از شبکه‌ای است که سیستم‌هایی در آن قرار می‌گیرند که به طور مرتب از شبکه غیر قابل اعتماد به آنها دسترسی پیدا می‌کنند. پس از آن می‌توان فایروال را کنترل کرد تا بتوان ترافیکی که بین این سه شبکه جریان دارد را کنترل کرد، تا حدودی به ترافیکی که برای DMZ در نظر گرفته شده است دقت داشته باشید و سپس با ظن بیشتری به ترافیک شبکه داخلی بپردازید.

اگرچه فایروال‌هایی که تاکنون مورد بحث قرار گرفته است، به طور مستقیم به شبکه غیر قابل اعتماد متصل می‌شوند (حداقل یک واسط interface انجام می‌دهد)، میزبان نمایش داده شده یک فایروال است که بین روتر نهایی و شبکه داخلی قرار دارد. وقتی ترافیک وارد روتر شود و به فایروال منتقل شود، قبل از ورود به شبکه داخلی، بازرسی خواهد شد.

باتوجه به این مفهوم، یک زیر شبکه نمایش داده شده است. در این حالت از دو فایروال استفاده می‌شود و برای ورود به شبکه داخلی باید ترافیک در هر دو فایروال بازرسی شود. به این منظور زیر شبکه نمایش داده می‌شود زیرا بین دو فایروال زیر شبکه وجود خواهد داشت که می‌تواند به عنوان DMZ برای منابع خارجی جهان عمل کند.

در دنیای واقعی، این رویکردهای مختلف برای برآورده کردن الزامات با یکدیگر ترکیب شده و مطابقت دارند، بنابراین ممکن است عناصری از این مفاهیم معماری را پیدا کرده که در یک موقعیت خاص کاربرد دارند.

پروکسی سرورها Proxy Server

پروکسی سرورها می‌توانند لوازم خانگی باشند یا می‌توانند نرم افزاری باشند که روی سیستم عامل سرور نصب شده باشند. این سرورها مانند یک فایروال پروکسی عمل می‌کنند به این دلیل که اتصال وب بین سیستم‌ها را از سمت آنها ایجاد می‌شود، اما به طور معمول می‌توانند ترافیک مجاز و غیرمجاز را براساس دانه دانه Granular basis جلوه دهند. به عنوان مثال، یک پروکسی سرور ممکن است اجازه دهد گروه فروش به وب سایتهای خاصی مراجعه کنند در حالی که اجازه نمی‌دهد گروه ورود داده‌ها به همان سایتهای دسترسی پیدا کند. قابلیت‌های فراتر از HTTP به انواع دیگری ترافیک، مانند FTP و دیگران گسترش یافته است.

پروکسی سرورها می توانند یک عملکرد مفید اضافی به نام Caching web ارائه دهند. هنگامی که یک پروکسی سرور برای ارائه حافظه کش وب پیکربندی شده است، یک نسخه از تمام صفحات وب را که در یک حافظه کش وب به رایانه های داخلی تحویل داده و ذخیره می کند. اگر هر کاربر بعداً همان صفحه را درخواست کند، پروکسی سرور یک نسخه محلی دارد و برای بازیابی آن از اینترنت، وقت و تلاش صرف نمی کند. این تا حد زیادی باعث بهبود عملکرد وب برای صفحات متقاضی می شود.

PBX

تبادل شاخه خصوصی (PBX) private branch exchange یک سوئیچ تلفن خصوصی است که در محل مشتری ساکن است و ارتباط مستقیم با سوئیچ ارائه دهنده ارتباط از راه دور دارد. PBX هدایت مسیریابی تماس را در سیستم تلفن داخلی انجام می دهد. اینگونه است که یک شرکت می تواند دو خط "خارج" اما ۵۰ تلفن داخلی داشته باشد. این تماس در یکی از دو خط بیرونی انجام می شود و PBX آن را به سمت بسط مناسب هدایت می کند. گاهی اوقات سیستم آنالوگ را به دیجیتال تبدیل می کند اما همیشه این فعالیت را انجام نمی دهد.

ملاحظات امنیتی با این دستگاهها حول تنظیمات پیش فرض آنها می چرخد. آنها به طور معمول با گذرواژه پیش فرض مدیر تنظیم می شوند که باید تغییر کنند، و اغلب حاوی اتصالات درپشتی هستند که توسط پرسنل پشتیبانی فروشنده می توانند برای اتصال و کمک به مشکلات استفاده شوند. این درب های پشتی معمولاً شناخته شده بوده و تا زمانی که لازم باشد باید غیرفعال باشند.

هانیپات ها Honey-pot

سیستم هایی هستند که برای هکرها تنظیم شده اند و در هنگام جمع آوری اطلاعات در مورد حمله، هکرها را برای گذراندن زمان حمله فریب می دهند. در بعضی موارد، شبکه های کامل به نام هانی پات ها برای این منظور جذاب تنظیم شده اند. این نوع رویکردها فقط باید توسط شرکت هایی با مهارت استقرار و نظارت صحیح بر روی آنها انجام شود.

باید دقت کرد که هانی پات ها ارتباط مستقیمی با هیچ سیستم مهمی ندارند و مانع از ایجاد یک نقطه پرش به سایر مناطق شبکه می شود. هدف نهایی این سیستم ها منحرف کردن توجه از منابع با ارزش تر و جمع آوری هرچه بیشتر اطلاعات در مورد حمله است. Tarpit نوعی از هانی پات

می‌باشد که به منظور ایجاد ارتباط بسیار کند با هکر طراحی شده است تا حمله مورد بررسی قرار گیرد.

سیستم تشخیص نفوذ IDS

سیستمی است که وظیفه تشخیص دسترسی غیرمجاز یا حمله به سیستم‌ها و شبکه‌ها را دارد. این سیستم می‌تواند تهدیدات، خارج سازی و مشخص کردن تهدیدات از خارج و داخل شبکه را تأیید کند. بیشتر IDSها برای واکنش به روش‌های خاص در موقعیت‌های خاص برنامه ریزی شده‌اند. اطلاع رسانی رخداد و هشدارها برای IDS بسیار مهم است. آنها به ادمین‌ها و متخصصان امنیت اطلاع می‌دهند که چه زمانی و کجا حملات شناسایی شده‌اند.

متداول ترین روش برای طبقه بندی IDS مبتنی بر منبع اطلاعات است که شامل: مبتنی بر شبکه یا مبتنی بر میزبان.

IDS مبتنی بر شبکه یا NIDS رایج ترین IDS است و بر ترافیک شبکه در یک بخش شبکه محلی نظارت می‌کند. برای نظارت بر ترافیک در بخش شبکه، کارت واسط شبکه باید در حالت بی قاعده Promiscuous تنظیم شده باشد. NIDS فقط می‌تواند بر ترافیک شبکه نظارت کند. این امر نمی‌تواند فعالیت داخلی را که در یک سیستم اتفاق می‌افتد، نظیر حمله به سیستمی که با ورود به سیستم به ترمینال محلی سیستم انجام می‌شود، نظارت کند. NIDS تحت تأثیر یک شبکه تغییر یافته قرار دارد زیرا به طور کلی NIDS فقط یک بخش شبکه را کنترل می‌کند.

IDS مبتنی بر میزبان یا HIDS بر ترافیک در یک سیستم واحد نظارت می‌کند. مسئولیت اصلی آن محافظت از سیستمی است که بر روی آن نصب شده است. HIDS از اطلاعات موجود در مسیرهای ممیزی سیستم عامل و Logهای مربوط به سیستم استفاده می‌کند. قابلیت‌های شناسایی HIDS محدود به چگونگی کامل بودن Logهای ممیزی و Logهای سیستم است. پیاده سازی‌های IDS بیشتر به دسته‌های زیر تقسیم می‌شوند:

- **مبتنی بر امضا Signature-based:** این نوع IDS ترافیک را تجزیه و تحلیل

می‌کند و آن را برای حمله یا الگوهای حالت، با نام امضاها، که در پایگاه داده IDS ساکن هستند، مقایسه می‌کند. همچنین از آن به عنوان سیستم تشخیص سوء استفاده یاد می‌شود. اگرچه این نوع از IDS بسیار رایج است، اما تنها می‌تواند حملات را در مقایسه با پایگاه داده خود تشخیص دهد و فقط به اندازه امضاها ارائه شده مؤثر است و بروزرسانی‌های مکرر ضروری می‌باشد.

دو نوع اصلی IDS مبتنی بر امضا هستند

✓ **تطبیق الگو** *Pattern-matching IDS*: ترافیک را با پایگاه داده الگوهای حمله مقایسه می کند. IDS هنگام شناسایی ترافیک منطبق با الگوی حمله، مراحل خاصی را انجام می دهد.

✓ **تطبیق رسمی** *Stateful-matching IDS*: حالت اولیه سیستم عامل را ضبط می کند. هرگونه تغییر درحالت سیستم که بطور خاص قوانین تعریف شده را نقض کند منجر به ارسال هشدار یا اطلاع رسانی می شود.

• **مبتنی بر ناهنجاری** *Anomaly-based*: این نوع IDS ترافیک را تجزیه و تحلیل می کند و آن را با ترافیک عادی مقایسه می کند تا تعیین کند که آیا ترافیک مذکور یک تهدید محسوب می شود یا خیر. همچنین از آن به عنوان یک سیستم مبتنی بر رفتار یا پروفایل استفاده می شود. مشکلی که در این نوع سیستم وجود دارد این است که هرگونه ترافیکی خارج از هنجارهای مورد انتظار گزارش شده، نتیجه مثبت غلط *false positives* نسبت به سیستم های مبتنی بر امضا بیشتر است. سه نوع IDS مبتنی بر ناهنجاری وجود دارد:

✓ **مبتنی بر ناهنجاری آماری** *Statistical anomaly-based IDS*: از محیط زنده *LIVE* برای ثبت فعالیت ها، نمونه می گیرد. هرچه مدت زمان کار IDS بیشتر باشد، پروفایلی که ساخته خواهد شد دقیق تر است. با این حال، ایجاد پروفایلی که تعداد زیادی از موارد مثبت کاذب *false positives* نداشته باشد می تواند دشوار و وقت گیر باشد. آستانه یا *Threshold* انحراف فعالیت در این نوع IDS مهم است. آستانه بیش از حد پایین منجر به مثبت کاذب می شود، در حالی که آستانه بیش از حد بالا منجر به منفی غلط *false negatives* می شود.

✓ **پروتکل مبتنی بر ناهنجاری** *Protocol anomaly-based IDS*: از پروتکل هایی که نظارت خواهد کرد آگاهی دارد. یک پروفایل به صورت کاربرد عادی ساخته شده با فعالیت مقایسه می شود.

✓ **مبتنی بر ناهنجاری ترافیکی** *Traffic anomaly-based IDS*: تغییرات الگوی ترافیکی را ردیابی می کند. کلیه الگوهای ترافیک آینده با نمونه مقایسه می شوند. تغییر آستانه باعث کاهش تعداد مثبت کاذب یا منفی غلط خواهد شد. این نوع فیلتر برای تشخیص

حملات ناشناخته بسیار عالی است، اما ممکن است فعالیت کاربر به اندازه کافی ثابت نباشد تا بتواند به طور مؤثر این سیستم را پیاده سازی کند.

• **مبتنی بر قانون یا مبتنی بر اکتشاف Rule- or heuristic-based:** این نوع از IDS

یک سیستم خبره است که از یک پایه دانش، موتور استنتاج و برنامه نویسی مبتنی بر قانون استفاده می کند. دانش به عنوان قوانین پیکربندی شده است. داده ها و ترافیک مورد تجزیه و تحلیل قرار می گیرند و قوانین مربوط به ترافیک تحلیل شده اعمال می شوند. موتور استنتاج از نرم افزار هوشمند خود برای "یادگیری" استفاده می کند. در صورت رعایت ویژگی های حمله، هشدارها یا اعلان ها شروع می شوند و اغلب به آن سیستم IF / THEN یا سیستم خبره گفته می شود.

IDS مبتنی بر اپلیکیشن یک IDS تخصصی است که فایل های Log تراکنش ها را برای یک اپلیکیشن واحد تجزیه و تحلیل می کند. این نوع IDS معمولاً به عنوان بخشی از اپلیکیشن ارائه می شود یا می توان آن را به عنوان افزودنی add-on خریداری کرد.

ابزارهایی که می توانند یک IDS را تکمیل کنند شامل سیستم های تجزیه و تحلیل آسیب پذیری، هانی پات ها و سلولهای پر شده است. همانطور که قبلاً توضیح داده شد، Honeypot ها سیستمهایی هستند که با کاهش امنیت برای جذب مهاجمین پیکربندی شده اند تا ادمین ها بتوانند در مورد فنون حمله اطلاعات کسب کنند. سلولهای بسته بندی شده Padded cells میزبان های خاصی هستند که یک مهاجم هنگام حمله منتقل می کند.

IPS

یک سیستم پیشگیری از نفوذ یا Intrusion prevention system (IPS) سیستمی است که وظیفه جلوگیری از حملات را بر عهده دارد. با شروع حمله، IPS اقدامات لازم را برای جلوگیری و مهار حمله انجام می دهد. IPS می تواند مانند IDS مبتنی بر شبکه یا میزبان باشد. اگرچه IPS می تواند مبتنی بر امضا یا ناهنجاری باشد، اما می تواند از یک نرخ مبتنی بر متر (معیار) Rate-based Metric استفاده کند که حجم ترافیک و همچنین نوع ترافیک را تحلیل می کند. در بیشتر موارد، اجرای IPS به دلیل امنیت اضافه شده برای جلوگیری از حمله در مقابل تشخیص سادگی، هزینه بیشتری نسبت به IDS دارد. علاوه بر این، اجرای یک IPS کارایی بارگزاری (Load) بیشتری از یک اجرای IDS دارد.

نقطه دسترسی بی سیم Wireless Access Point

یک نقطه دسترسی بی سیم یا AP به دستگاههای بی سیم اجازه می دهد تا با استفاده از Wi-Fi یا استانداردهای مربوطه به یک شبکه سیمی متصل شوند. در لایه های Physical , Data Link , و لایه های ۱ و ۲ کار می کنند.

دستگاههای سیار Mobile Devices

دستگاههای سیار - از جمله لپ تاپ، تبلت، تلفنهای هوشمند، کتابخوان الکترونیکی و دستگاههای پوشش فناوری - به سرعت تبدیل به پرکاربردترین دستگاهها شده اند. در صورت مجاز بودن دستگاههای شخصی، یک سازمان باید سیاست امنیتی رسمی دستگاه سیار را اتخاذ کند و سیاست امنیتی یا Bring-your-own-device (BYOD) را برای سازمان به ارمغان آورد. سازمان همچنین ممکن است بخواهد راه اندازی سرور کنترل دسترسی به شبکه NAC را در نظر بگیرد تا مطمئن شود که هر دستگاهی که به شبکه می پیوندد حداقل شرایط امنیتی را برآورده می کند و هر دستگاهی که حداقل شرایط امنیتی را برآورده نکند، قرنطینه می شود.

مسیریابی شبکه Network Routing

مسیریابی در لایه ۳ مدل OSI اتفاق می افتد، این همان لایه ای است که IP در آن کار می کند و آدرس های IP مبدا و مقصد در بسته قرار می گیرند. روترها دستگاه هایی هستند که باعث انتقال ترافیک بین سیستمها در شبکه های مختلف IP می شوند. هنگامی که رایانه ها در شبکه های IP مختلف هستند، نمی توانند ارتباط برقرار کنند مگر اینکه به روتر دسترسی داشته باشند تا بتواند بسته ها را به شبکه های دیگر منتقل کنند.

روترها اطلاعات مربوط به مسیرهای شبکه های دیگر را در یک جدول مسیریابی نگه می دارند. این جداول می توانند به چندین روش جمع شوند. Administrator ها بصورت دستی وارد این مسیرها می شوند، یا پروتکل های مسیریابی پویا به روترهایی که با همان پروتکل در حال اجرا هستند اجازه می دهند تا جداول مسیریابی و اطلاعات مسیریابی را تبادل کنند. تنظیمات دستی، همچنین مسیریابی ایستا نامیده می شود، این مزیت را دارد که از ترافیک اضافی ایجاد شده توسط پروتکل های مسیریابی پویا جلوگیری کند و امکان کنترل دقیق رفتار مسیریابی را فراهم می آورد، اما در صورت بروز خرابی در لینک (Link Failure)، به مداخله دستی Manual Intervention

نیاز دارد. پروتکل‌های مسیریابی پویا باعث ایجاد ترافیک می‌شوند اما قادر به واکنش در ارتباط با قطع ارتباط و بازگرداندن ترافیک بدون مداخله دستی هستند.

از دیدگاه امنیتی، پروتکل‌های مسیریابی این امکان را به وجود می‌آورند که بتواند ترافیک بروزرسانی مسیریابی را بگیرد و به هکر این امکان را می‌دهد تا اطلاعات ارزشمندی درباره چیدمان شبکه کسب کند.

علاوه بر این، دستگاه‌های سیسکو (شاید بیشتر مورد استفاده قرار می‌گیرد) از پروتکل اختصاصی لایه ۲ به طور پیش فرض به نام Cisco Discovery Protocol (CDP) استفاده می‌کنند تا در مورد قابلیت‌های خود به یکدیگر اطلاع دهند. در صورت ضبط بسته‌های CDP، می‌توان اطلاعات اضافی بدست آورد که می‌تواند برای نقشه برداری از شبکه قبل از حمله مفید باشد. در این بخش مقایسه و متضاد پروتکل‌های مسیریابی بررسی می‌شود.

بردار مسافت، حالت پیوند، یا مسیریابی هیبریدی

Distance Vector, Link State, or Hybrid Routing

پروتکل‌های مسیریابی قابلیت‌ها و خصوصیات عملیاتی متفاوتی دارند که هنگام استفاده از آنها تأثیر می‌گذارد. پروتکل‌های مسیریابی در دو نوع اساسی وجود دارد: داخلی و خارجی. پروتکل‌های مسیریابی داخلی در یک سیستم خودمختار استفاده می‌شود، یک شبکه که توسط یک مجموعه از ادمین‌ها، به طور معمول یک شرکت واحد اداره می‌شود. پروتکل‌های مسیریابی بیرونی مسیر ترافیک بین سیستم‌ها یا شبکه‌های شرکت را طی می‌کنند. نمونه‌ای از این نوع مسیریابی اتفاقاتی است که در اینترنت رخ می‌دهد.

پروتکل‌های مسیریابی همچنین می‌توانند در سه دسته قرار بگیرند که عملکرد آنها را بیش از محدوده خود توصیف می‌کنند: بردار مسافت، حالت پیوند و هیبریدی (یا بردار مسافت پیشرفته). تفاوت بیشتر مربوط به میزان ایجاد شده در ترافیک و روشی است که برای تعیین بهترین مسیر از مسیرهای ممکن به یک شبکه استفاده می‌شود. به مقدار استفاده شده برای تصمیم‌گیری، متریک Metric گفته می‌شود و هر کدام برای محاسبه متریک و در نتیجه تعیین بهترین مسیر، روش متفاوتی دارند.

پروتکل‌های بردار مسافت کل جدول مسیریابی خود را با روترهای همسایه خود در یک زمان به اشتراک می‌گذارند، در نتیجه بیشترین ترافیک را در سه دسته ایجاد می‌کنند. آنها همچنین از

متریک به نام Hop Count استفاده می کنند. تعداد هاپ به سادگی تعداد روترهایی است که برای رسیدن به یک شبکه طی شده است.

پروتکل های حالت پیوند فقط تغییرات شبکه (قطع ارتباط و بازیابی) را با همسایگان به اشتراک می گذارند، در نتیجه میزان ترافیک ایجاد شده را بسیار کاهش می دهند. آنها همچنین از یک متریک بسیار پیچیده تر استفاده می کنند که مبتنی بر فاکتورهای زیادی مانند پهنای باند هر پیوند در مسیر و تراکم در هر پیوند است. بنابراین هنگام استفاده از یکی از این پروتکل ها، ممکن است مسیری به عنوان بهترین مسیر انتخاب شود حتی اگر تعداد بیشتری از هاپ را داشته باشد زیرا مسیر انتخاب شده از پهنای باند بهتری برخوردار است، یعنی تراکم کمتری دارد.

پروتکل های بردار مسافت هیبریدی یا پیشرفته ویژگی های هر دو نوع را نشان می دهند. EIGRP، که بعداً در این بخش مورد بحث قرار می گیرد، تنها نمونه این نوع است. در گذشته به EIGRP به عنوان یک پروتکل هیبریدی گفته می شد اما در چند سال گذشته، سیسکو (که IGRP و EIGRP ایجاد کرد) این پروتکل را بردار مسافت پیشرفته نامیده است، بنابراین ممکن است هر دو اصطلاح مورد استفاده را مشاهده کنید. در بخش های بعدی، چندین مورد از رایجترین پروتکل های مسیریابی به طور خلاصه مورد بحث قرار گرفته است.

RIP

پروتکل اطلاعات مسیریابی Routing Information Protocol (RIP) یک پروتکل بردار مسافت مبتنی بر استاندارد است که دارای دو نسخه است: RIPv1 و RIPv2. این پروتکل در لایه ۳ (لایه شبکه) فعالیت می کند. هر دو از هاپ به عنوان یک متریک استفاده می کنند و هر ۳۰ ثانیه کل جدول های مسیریابی خود را به اشتراک می گذارند. اگرچه RIP ساده ترین راه برای پیکربندی می باشد، اما حداکثر تعداد هاپ ۱۵ عدد می باشد، بنابراین فقط در شبکه های بسیار کوچک مفید است. بزرگترین تفاوت بین این دو نسخه این است که RIPv1 فقط می تواند مسیریابی طبقاتی را انجام دهد در حالی که RIPv2 می تواند در شبکه ای که CIDR در آن پیاده سازی شده است، مسیریابی شود.

بر خلاف RIPv1، RIPv2 یک پوشش یا ماسک زیر شبکه Subnet Mask دارد. این برنامه از امنیت تأیید گذرواژه پشتیبانی می کند و هاپ بعدی را مشخص می کند.

OSPF

Open Shortest Path First (OSPF) یک پروتکل حالت پیوند مبتنی بر استانداردها است. از متریکی (معیاری) با عنوان هزینه Cost استفاده می‌شود که براساس بسیاری از ملاحظات محاسبه می‌شود. OSPF نسبت به پروتکل مسیریابی بردار مسافت مانند RIP تصمیم‌گیری در مسیریابی را پیچیده تر می‌کند. برای بهره‌گیری کامل از OSPF، دانش بسیار عمیق تری از مسیریابی و خود OSPF لازم است و می‌تواند با موفقیت در شبکه‌های با مقیاس بسیار بزرگ موفق بوده زیرا هیچ حداقل تعداد هاپی وجود ندارد.

OSPFv2 به روترها اجازه می‌دهد تا با روترهای دیگر در مورد مسیری که می‌دانند ارتباط برقرار کنند. برای ارتباط مسیرها بین روترها از اعلانات حالت پیوند یا Link state Advertisements (LSAs) استفاده می‌شود.

Interior Gateway Routing Protocol (IGRP)

پروتکل مسیریابی دروازه داخلی یا IGRP یک پروتکل مسیریابی منسوخ Cisco اختصاصی است که احتمالاً در دنیای واقعی به دلیل عدم توانایی آن در کار در محیطی که CIDR در آن پیاده سازی شده است، مشاهده نمی‌شود. این پروتکل با نسخه بدون کلاس پیشرفته IGRP (EIGRP) در بحث بعدی جایگزین شده است.

Enhanced IGRP (EIGRP)

پیشرفته IGRP یک پروتکل مسیریابی اختصاصی بدون سیسکو است که یک پروتکل بردار مسافت یا پیشرفته در نظر گرفته می‌شود. این EIGRP برخی از ویژگی‌های هر دو حالت پیوند و مسافت را نشان می‌دهد. همچنین هیچ محدودیتی در شمارش هاپ وجود ندارد و اجرای آن بسیار ساده تر از OSPF است. با این وجود، لازم است که همه روترها سیسکو باشند.

VRRP

وقتی روتر غیرفعال می‌شود، تمام میزبان‌هایی که از آن روتر برای مسیریابی استفاده می‌کنند، قادر به ارسال ترافیک به شبکه‌های دیگر نخواهند بود.

پروتکل افزونگی روتر مجازی (VRRP) Virtual Router Redundancy Protocol در واقع یک پروتکل مسیریابی نیست بلکه از آن استفاده می‌شود تا در صورت غیرفعال شدن روتر، از چندین دروازه برای مشتری به خاطر تحمل خطا استفاده کند. تمام میزبان‌های یک شبکه با آدرس IP

روتر مجازی به عنوان دروازه پیش فرض آنها تنظیم می شوند. روترهای فیزیکی متعددی براساس این آدرس نقشه برداری می شوند، بنابراین حتی در صورت غیرفعال شدن، روتر در دسترس خواهد بود.

IS-IS

Intermediate System to Intermediate System (IS-IS) یک پروتکل مسیریابی پیچیده داخلی است که بیشتر از IP مبتنی بر پروتکل های OSI است. این یک پروتکل حالت پیوند است. اجرای TCP / IP یکپارچه IS-IS نامیده می شود. OSPF عملکرد بیشتری دارد، اما IS-IS ترافیک کمتری نسبت به OSPF ایجاد می کند و بسیار کمتر از OSPF پیاده سازی می شود.

BGP

پروتکل مسیریابی مرزی (Border Gateway Protocol (BGP) یک پروتکل مسیریابی بیرونی می باشد که یک پروتکل بردار مسیر محسوب می شود. این مسیر بین سیستم های خودمختار Autonomous Systems (AS) یا دروازه میزبان ها Gateway Hosts حرکت می کند و در اینترنت استفاده می شود. BGP مجموعه از ویژگی های غنی ای دارد که می تواند توسط ادمین ها برای کنترل انتخاب مسیر و کنترل روش دقیق ورود ترافیک به AS و کنترل آن دستکاری شود. با این حال، یکی از پیچیده ترین فهم و تنظیمات می باشد. BGP یک پروتکل لایه Application یا برنامه (لایه ۷) است.

رسانه انتقال Transmission Media

رسانه انتقال مورد استفاده در یک شبکه کابلی است که برای انتقال ترافیک شبکه استفاده می شود. هر یک از رسانه های انتقال مختلف دارای حداکثر سرعت، حداکثر فاصله، مسائل امنیتی مختلف و محیط متفاوت هستند. در این بخش ما در مورد کابل کشی، توپولوژی شبکه، فناوری های شبکه و فناوری های WAN که در آزمون CISSP مطرح می شود، بحث می کنیم.

کابل کشی Cabling

کابل کشی در لایه فیزیکی مدل OSI ساکن است و به سادگی واسطه ای را برای انتقال اطلاعات فراهم می کند. اکثریت قریب به اتفاق داده ها به کابل های مختلفی از جمله کواکسیال، فیبر نوری

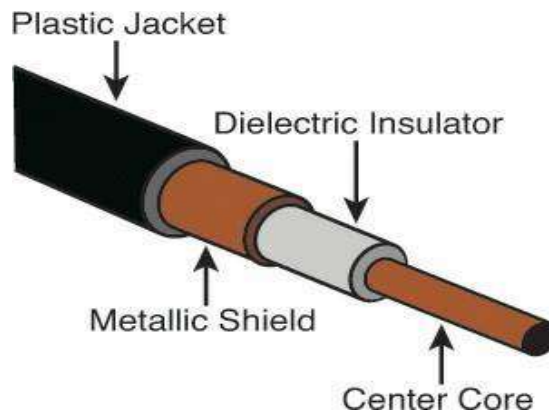
و زوج بهم پیچ خورده منتقل می‌شوند. برخی از این کابل‌ها داده‌ها را از نظر ولتاژ الکتریکی نشان می‌دهند در حالی که کابل‌های فیبر نوری برای نشان دادن داده‌ها، نور را دستکاری می‌کنند. با استفاده از چندین معیار می‌توانید کابل‌ها را با یکدیگر مقایسه کرد. یکی از معیارهایی که در رابطه با شبکه سازی اهمیت دارد، میزان حساسیت کابل برای تضعیف Attenuation می‌باشد. تضعیف در زمان رسیدن سیگنال هنگام عبور از کابل رخ می‌دهد. این سیگنال را تضعیف می‌کند و در برخی از نقاط (در هر نوع کابل متفاوت است) سیگنال دیگر به اندازه کافی قوی نیست که به درستی در مقصد خوانده شود. به همین دلیل، تمام کابل‌ها دارای حداکثر طول هستند. این امر بدون توجه به اینکه کابل فیبر نوری یا الکتریسیته می‌باشد، صادق است. نکته مهم دیگر مقایسه انواع کابل‌ها، میزان داده آنهاست که میزان ارسال داده از طریق کابل در ثانیه را توصیف می‌کند. این منطقه در طی سال‌ها پیشرفت چشم گیری داشته است، از نرخ ۱۰ مگابیت بر ثانیه در یک شبکه LAN به ۱۰۰۰ Mbps و حتی ۱۰ گیگابیت در ثانیه در شبکه‌های امروز (و حتی در data center با سرعت بالاتر) پیشرفت کرده است. نکته دیگر هنگام انتخاب نوع کابل، سهولت نصب است. نصب برخی از انواع کابل آسانتر از سایرین است و کابل کشی فیبر نوری برای نصب نیاز به یک مجموعه مهارت خاص دارد که هزینه نصب آن را بالا می‌برد. سرانجام (و از همه مهمتر برای بحث ما) امنیت کابل است. کابل‌ها می‌توانند اطلاعات را نشت یا پخش کنند. در صورت دسترسی فیزیکی به آنها، هکرها می‌توانند از طریق کابل نفوذ کنند. همانطور که انواع کابل‌ها می‌توانند در طول و ظرفیت مجاز متفاوت باشند، در حساسیت آنها نسبت به این نوع از دست دادن داده‌ها نیز متفاوت هستند.

کواکسیال Coaxial

یکی از اولین نوع کابل‌ها که برای شبکه سازی مورد استفاده قرار می‌گرفت، کواکسیال بود، همان نوع بنیادی کابل که تلویزیون کابلی را به میلیون‌ها خانه منتقل می‌کرد. اگرچه کابل کشی کواکسیال، به دلیل ظرفیت کم و سازگاری کم با انواع دیگر کابل هنوز مورد استفاده قرار می‌گیرد، اما استفاده از آن در LAN‌ها تقریباً منسوخ شده است. کابل کشی کواکسیال در دو نوع یا ضخامت ارائه می‌شود. نوع ضخیم تر با نام Thicknet که نام رسمی 10Base5 را دارد. این سیستم نامگذاری، برای انواع دیگر کابل نیز مورد استفاده قرار می‌گیرد که چندین واقعیت در مورد کابل ارائه می‌دهد. در مورد 10Base5 به این معنی است که

قادر به انتقال ۱۰ مگابیت در ثانیه است و تقریباً ۱۶۴۰ فوت را می تواند طی کند. Thicknet از دو نوع کانکتور استفاده می کند: یک Vampire tap (به این ترتیب نامگذاری شده است زیرا دارای سنبله ای است که کابل را سوراخ می کند) و اتصالات N (N-connectors). Thinnet یا 10Base2 نیز با سرعت ۱۰ مگابیت در ثانیه کار می کند. اگرچه وقتی نامگذاری شد پیش بینی می شد که قادر به طی کردن ۲۰۰ فوت باشد، اما بعداً به ۱۸۵ فوت کاهش یافت. هر دو نوع در توپولوژی باس مورد استفاده قرار می گیرند. Thinnet از دو نوع کانکتور استفاده می کند: اتصالات BNC و اتصالات T.

کواکسیال دارای یک پوشش (عایق) استوانه ای بیرونی است که با یک سیم هسته جامد (Thicknet) یا یک هسته بهم تابیده شده (Thinnet) را احاطه کرده است. به مرور زمان کابل کشی زوج بهم پیچ خورده و کابل کشی فیبر نوری با توان بیشتری جایگزین این نوع کابل کشی شدند. کابل کشی کواکسیال قابل استفاده است، بنابراین دسترسی فیزیکی به این کابل کشی باید در صورت امکان محدود یا جلوگیری شود. اگر از آن استفاده می شود باید دور از چشم باشد. شکل ۴-۱۶ ساختار کابل کواکسیال را نشان می دهد.

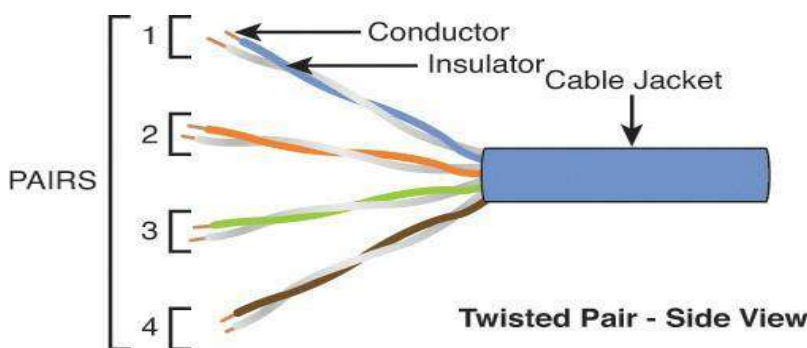


شکل ۴-۱۶: کابل کشی کواکسیال

یکی دیگر از مشکلات امنیتی کواکسیال در یک توپولوژی باس این است که Broadcast-Based است و بدان معناست که یک اسنیفر متصل در هر نقطه از شبکه می تواند همه ترافیک را ضبط کند.

زوج بهم پیچ خورده Twisted Pair

رایجترین نوع کابل کشی شبکه که امروزه یافت می‌شود کابل کشی زوج بهم پیچ خورده نامیده می‌شود. به این دلیل گفته می‌شود زیرا در داخل کابل چهار سیم به حالت زوج کوچکتر وجود دارد که بهم تابیده یا پیچ خورده اند. علت طراحی این پیچش، در صورتی که سیم هایی که داخل کابل هستند با یکدیگر تداخل داشتند برای از بین بردن پدیده‌ای به نام متقاطع Crosstalk می‌باشد. تعداد زوج سیم هایی که استفاده می‌شود بستگی به پیاده سازی آن دارد. در برخی از پیاده سازی‌ها فقط از دو زوج استفاده می‌شود و در برخی دیگر از هر چهار زوج سیم استفاده می‌شود. شکل ۴-۱۷ ساختار کابل زوج بهم پیچ خورده را نشان می‌دهد.



شکل ۴-۱۷: کابل کشی زوج بهم پیچ خورده

کابل کشی زوج بهم پیچ خورده در نسخه‌های محافظ STP و محافظت نشده UTP ارائه می‌شود. چیزی جز محافظت در برابر تداخل رادیویی فرکانس RFI و تداخل الکترومغناطیسی EMI حاصل نمی‌شود. RFI از منابع رادیویی در منطقه تداخل دارد، در حالی که EMI از خطوط برق تداخل دارد. نوع رایج EMI (نویز حالت معمول) نامیده می‌شود که این تداخلی است که در هر دو قسمت سیگنال (بازگشت سیگنال و مدار) یا ترمینال‌های یک مدار اندازه‌گیری و زمین ظاهر می‌شود. اگر EMI و RFI مشکلی نداشته باشند، با استفاده از STP هیچ چیزی حاصل نمی‌شود و هزینه بیشتری نیز دارد.

سیستم نامگذاری که با کواکسیال و فیبر نوری استفاده می‌شود در یک زوج بهم پیچ خورده نیز استفاده می‌شود. در زیر با انواع عمده زوج بهم پیچ خورده روبرو می‌شوید:

10BaseT با سرعت ۱۰ مگابیت بر ثانیه کار می‌کند.

100BaseT همچنین اترنت سریع نیز نامیده می‌شود. با سرعت ۱۰۰ مگابیت بر ثانیه کار می‌کند.

1000BaseT به آن Gigabit Ethernet نیز گفته می شود. با سرعت ۱۰۰۰ Mbps کار می کند.
10GBaseT: با سرعت ۱۰ گیگابیت بر ثانیه کار می کند.

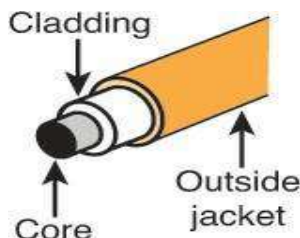
کابل کشی زوج بهم پیچ خورده دارای قابلیت های مختلفی است و در دسته بندی های مختلف رتبه بندی می شود. جدول ۴-۵ انواع عمده و خصوصیات آنها را نشان می دهد. علیرغم دسته بندی، کابل کشی زوج بهم پیچ خورده را می توان حدود ۱۰۰ متر قبل از تضعیف سیگنال اجرا شود.

Name	Maximum Transmission Speed
Cat3	10 Mbps
Cat4	16 Mbps
Cat5	100 Mbps
Cat5e	100 Mbps
Cat6	1 Gbps
Cat6a	10 Gbps
Cat7	10 Gbps
Cat7a	10 Gbps; 40 Gbps (50 meters); 100 Gbps (15 meters)

جدول ۴-۵: دسته های زوج بهم پیچ خورده

فیبر نوری Fiber optic

کابل کشی فیبر نوری از منبع نوری استفاده می کند که دارای زیرشاخه یک شیشه داخلی یا هسته پلاستیکی در کابل می باشد. این هسته توسط روکش پوشانده شده است که باعث می شود نور به هسته فیبر محدود شود. اغلب به عنوان ستون فقرات شبکه Backbone استفاده می شود و حتی ممکن است در اینترنت، تلفن و پیاده سازی تلویزیون کابلی نیز مشاهده شود. شکل ۴-۱۸ ساختار کابل فیبر نوری را نشان می دهد.



شکل ۴-۱۸: کابل کشی فیبر نوری

کابل کشی فیبر نوری، نور را به گونه‌ای دستکاری می‌کند که بتوان آن را به صورت یک و صفر تعبیر کرد. از آنجا که این سیستم بر پایه الکتریکی نیست، در برابر RFI، EMI و Crosstalk کاملاً غیرقابل نفوذ است. علاوه بر این، اگرچه غیرممکن نیست، اما بهره برداری یا استراق سمع بر روی کابل فیبرنوری بسیار مشکل تر است. در بیشتر موارد، با ضربه خوردن منجر به خرابی کابل می‌شود، که در این صورت برای همه کاملاً آشکار می‌شود.

فیبرنوری در یک حالت منفرد Single mode و چند حالت Multi-mode عرضه می‌شود. حالت منفرد از یک پرتو واحد نور که توسط یک لیزر تهیه شده است استفاده می‌کند، از این دو نوع فیبرنوری حالت منفرد برد بیشتری دارد و گرانتزین می‌باشد. فیبرنوری چند حالت همزمان از چندین پرتوی نور استفاده می‌کند، از LED استفاده می‌کند، برد کوتاهتری دارد و ارزانتر است. در هر صورت از هر نوع کابل کشی الکتریکی فراتر می‌رود و همچنین ظرفیت بیشتری را فراهم می‌کند. با این حال، کابل کشی فیبر نوری اشکالاتی دارد. همچنین برای خرید این نوع، علاوه بر گران ترین کابل کشی، پرهزینه ترین نصب را نیز داراست.

جدول ۴-۶ برخی از مشخصات فیبرنوری انتخاب شده و حداکثر فاصله‌های علمی آنها را نشان می‌دهد.

Standard	Distance
100Base-FX	Maximum length is 400 meters for half-duplex connections (to ensure collisions are detected) or 2 kilometers for full-duplex
1000Base-SX	550 meters
1000Base-LX	Multi-mode fiber (up to 550 meters) or single-mode fiber (up to 2 kilometers; can be optimized for longer distances, up to 10 kilometers)
10GBase-LR	10 kilometers
10GBase-ER	40 kilometers

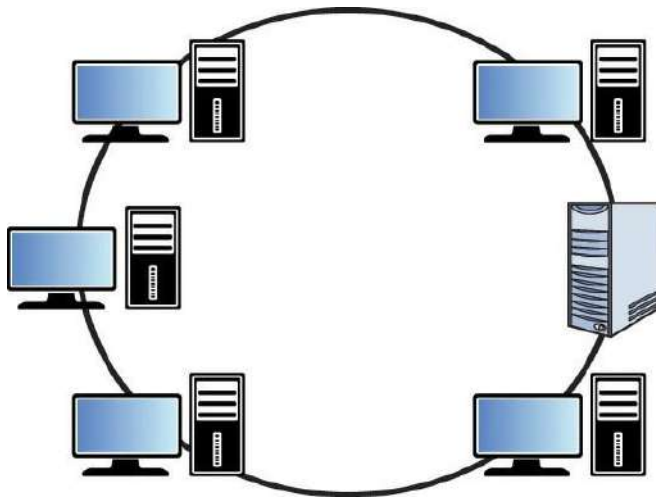
جدول ۴-۶: مشخصات انتخاب شده فیبر

توپولوژی های شبکه

شبکه ها را می توان با توپولوژی منطقی آنها (مسیر داده استفاده شده) و توپولوژی فیزیکی آنها (نحوه اتصال دستگاه ها به یکدیگر) توصیف کرد. در بیشتر موارد، توپولوژی منطقی و توپولوژی فیزیکی یکسان هستند اما به طور کل اینگونه نمی باشد. در این بخش هم توپولوژیهای شبکه منطقی و هم فیزیکی مورد بحث قرار می گیرد.

حلقه Ring

توپولوژی حلقه فیزیکی موضوعی است که در آن دستگاه ها به صورت دایره ای یا حلقه ای زنجیر می شوند. اگر شبکه همچنین یک حلقه منطقی باشد، داده ها حلقه را از یک دستگاه به دستگاه دیگر می چرخانند. دو فناوری از این توپولوژی استفاده می کنند، واسط توزیع کننده داده ها در شبکه فیبرنوری Fiber Distributed Data Interface (FDDI) و Token Ring. هر دو این فناوری ها در بخش "فناوریهای شبکه" با جزئیات مورد بحث قرار گرفته اند. شکل ۴-۱۹ یک توپولوژی حلقه را نشان می دهد.



شکل ۴-۱۹: توپولوژی حلقه Ring Topology

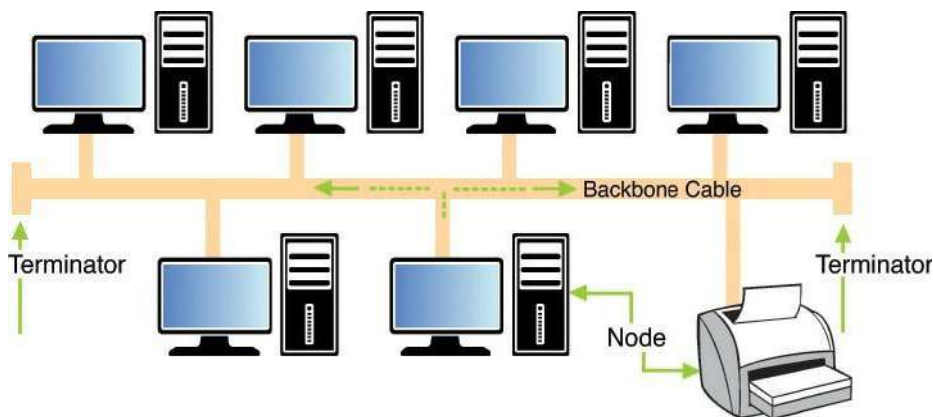
یکی از اشکالات توپولوژی حلقه این است که اگر یک شکست در خط رخ دهد، به دلیل شکسته شدن حلقه، تمام سیستم ها تحت تأثیر قرار می گیرند. همانطور که در بخش "فن آوری های

شبکه "مشاهده خواهید کرد، یک شبکه FDDI با یک حلقه دویل برای تحمل خطا عملیات آدرس دهی را انجام می‌دهد.

Bus

توپولوژی Bus اولین توپولوژی اینترنت مورد استفاده بود. در این توپولوژی تمام دستگاه‌ها به یک خط واحد متصل می‌شوند که دارای دو نقطه پایانی قطعی است. شبکه به عقب باز نمی‌گردد یک حلقه را تشکیل نمی‌دهد. این توپولوژی مبتنی بر پخش است، که می‌تواند یک مسئله امنیتی باشد به این دلیل که یک اسنiffer یا تحلیل کننده پروتکل متصل به هر نقطه از شبکه قادر به ضبط کلیه ترافیک خواهد بود.

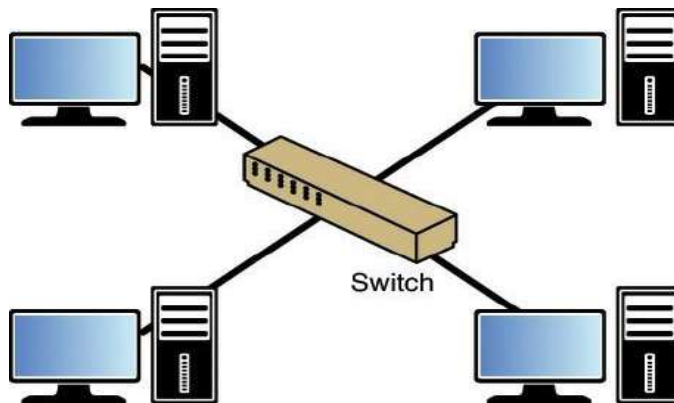
از نقطه نظر تحمل خطا، توپولوژی Bus همان خطر Ring را دارد. اگر یک وقفه در هر نقطه از خط اتفاق بیفتد، تمام دستگاه‌ها تحت تأثیر قرار می‌گیرند. علاوه بر این، یک الزام خاص برای این توپولوژی این است که باید در انتهای Bus خاتمه یابد و مانع برگشت مجدد سیگنال‌ها در خط می‌شود. (در مبحث‌های بعدی در مورد تصادم‌ها Collisions بیشتر بحث می‌شود، در مورد تصادم مجبور است دوباره بسته‌های مورد تصادم قرار گرفته ارسال شوند و بازده کلی را کاهش دهند.) اگر این خاتمه به درستی انجام نشده باشد، شبکه به درستی کار نخواهد کرد. شکل ۴-۲۰ توپولوژی Bus را نشان می‌دهد.



شکل ۴-۲۰: توپولوژی bus

ستاره Star

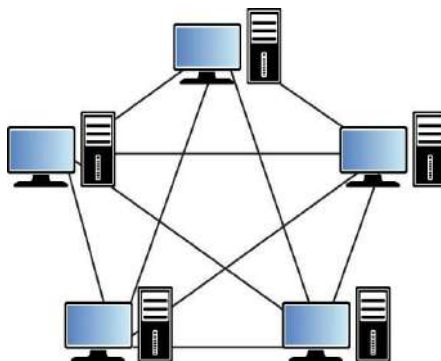
توپولوژی ستاره امروزه رایج ترین کاربرد را دارد. در این توپولوژی، تمام دستگاه ها به یک دستگاه مرکزی متصل می شوند (هاب یا سوئیچ). یکی از مزایای این توپولوژی این است که اگر اتصال به هر دستگاه واحد خراب شود، فقط آن دستگاه تحت تأثیر قرار می گیرد و هیچ دستگاه دیگری تحت تأثیر قرار نمی گیرد. نکته منفی این توپولوژی این است که یک نقطه شکست (هاب یا سوئیچ) وجود دارد. اگر هاب یا سوئیچ خراب شود، تمام دستگاه ها تحت تأثیر قرار می گیرند. شکل ۴-۲۱ توپولوژی ستاره را نشان می دهد.



شکل ۴-۲۱: توپولوژی ستاره

تار عنکبوتی یا Mesh

اگرچه توپولوژی تار عنکبوتی دارای بیشترین تحمل خطا در مورد بحث های موجود است، اما استقرار آن نیز پرهزینه می باشد. در این توپولوژی، تمام دستگاه ها به تمام دستگاه های دیگر متصل هستند. این امر تحمل کامل خطا را فراهم می کند، اما همچنین نیاز به واسطه ها و کابل های مختلف در هر دستگاه دارد. به همین دلیل، فقط در شرایط نادر و جایی که چنین هزینه ای ضروری است، مستقر می شود. شکل ۴-۲۲ توپولوژی مش را نشان می دهد.

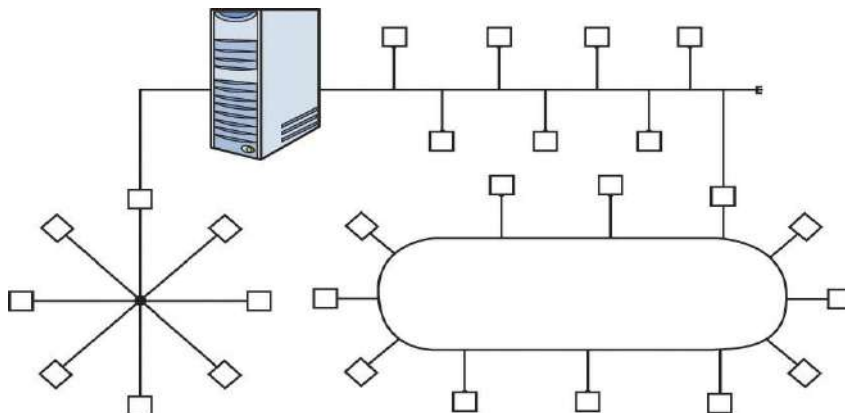


شکل ۴-۲۲: توپولوژی تار عنکبوتی یا Mesh

Hybrid

در بسیاری موارد، شبکه یک سازمان ترکیبی از توپولوژی‌های ذکرشده شبکه یا یک شبکه Hybrid است. به عنوان مثال، یک بخش ممکن است یک ستاره باشد که به یک شبکه bus یا یک شبکه Ring متصل شده است.

شکل ۴-۲۳ نمونه‌ای از شبکه Hybrid را نشان می‌دهد.



شکل ۴-۲۳: توپولوژی Hybrid

فن آوری‌های شبکه Network Technologies

درست همانطور که می‌توان شبکه‌ای را در توپولوژی‌های مختلف به هم متصل کرد، طی سالیان متمادی فناوری‌های مختلفی اجرا شده اند که بیش از آن توپولوژی‌ها را اداره می‌کنند. این فناوری‌ها در لایه ۲ مدل OSI کار می‌کنند و جزئیات عملکرد آنها در استانداردهای مختلف

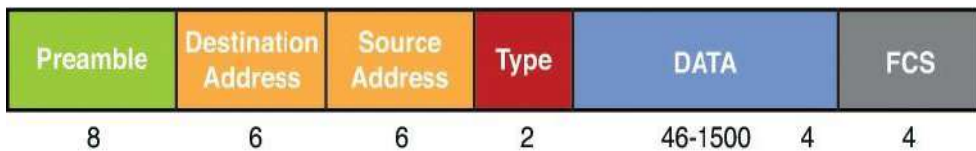
توسط انستیتوی مهندسان برق و الکترونیک IEEE مشخص شده است. برخی از این فن آوری ها برای اپلیکیشن های شبکه محلی LAN طراحی شده اند، در حالی که برخی دیگر در شبکه گسترده WAN مورد استفاده قرار می گیرند. در این بخش به فناوری های اصلی LAN و برخی از فرآیندهای استفاده شده از این فناوری ها برای حکمیت دسترسی به شبکه می پردازیم.

اترنت 802.3

IEEE جزئیات اترنت را در استاندارد 802.3 مشخص کرده است. قبل از این استاندارد سازی، اترنت در چندین شکل اولیه وجود داشته است که رایج ترین آنها Ethernet II یا DIX Ethernet نامیده می شود (DIX مخفف سه شرکت DEC، Intel، Xerox است که در بوجود آوردن آن همکاری داشته اند).

در بخش مربوط به مدل OSI بیان شد که PDU ایجاد شده در لایه ۲ یک فریم نامیده می شود. از آنجا که اترنت یک پروتکل لایه ۲ است، ما به بسته های اترنت فردی فریم می نامیم. در ساختارهای فریم Ethernet II و 802.3 تفاوت های اندکی وجود دارد، اگرچه در همان شبکه سازگار می باشند. شکل ۴-۲۴ مقایسه دو فریم را نشان می دهد. تفاوت قابل توجه در این است که در طی فرآیند استاندارد سازی IEEE، قسمت اترنت در استاندارد 802.3 جدید به فیلد طول (length) داده تغییر یافت. برای شناسایی نوع داده، فیلد دیگری به نام هدر 802.2 درج شده است تا آن اطلاعات را در خود جای دهد.

Ethernet



IEEE 802.3



Field lengths are in bytes

شکل ۴-۲۴: Ethernet II و 802.3

اترنت روی سیم کشی کواکسیال، فیبرنوری و زوج بهم پیچ خورده پیاده سازی می شود. در جدول ۴-۷ برخی از متداول ترین پیاده سازی های اترنت آورده شده است.

Ethernet Type	Cable Type	Speed
10Base2	Coaxial	10 Mbps
10Base5	Coaxial	10 Mbps
10BaseT	Twisted pair	10 Mbps
100BaseTX	Twisted pair	100 Mbps
1000BaseT	Twisted pair	1000 Mbps
1000BaseX	Fiber	1000 Mbps
10GBaseT	Twisted pair	10 Gbps

جدول ۴-۷: پیاده سازی اترنت

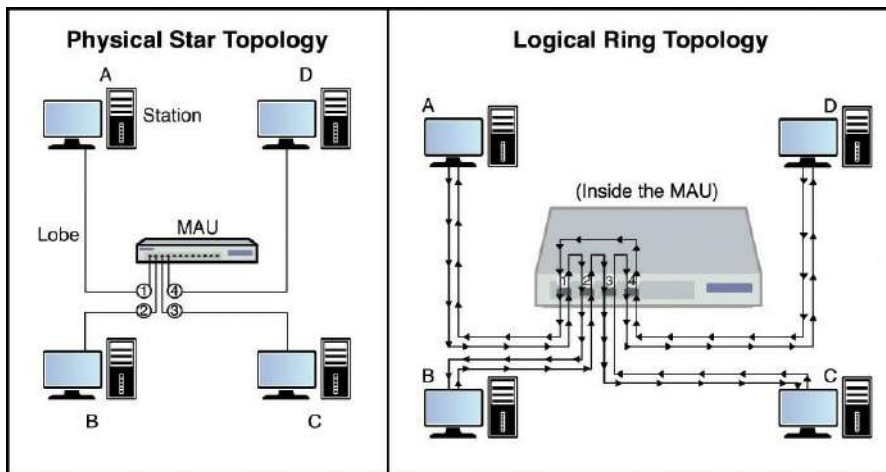
علیرغم اینکه 1000BaseT و 1000BaseX سریعتر هستند، 100BaseTX اترنت سریع Fast Ethernet نامیده می شود. همچنین، هر دو 1000BaseT و 1000BaseX معمولاً به عنوان Gigabit Ethernet نامیده می شوند.

اترنت خواستار دستگاه برای به اشتراک گذاشتن رسانه به صورت فریم به فریم می باشد. این دسترسی به رسانه ها با استفاده از فرآیندی به نام Carrier Sense Multiple Access / Detection (CSMA / CD) Collision می باشد. این فرآیند به تفصیل در بخش "CSMA / CD در مقابل CSMA / CA" مورد بحث قرار می گیرد، جایی که با روش مورد استفاده در شبکه های بی سیم 802.11 در تضاد است.

802.5 Token Ring

اترنت رایج ترین پروتکل لایه ۲ است، اما همیشه اینگونه نبوده است. نمونه ای از پروتکل لایه ۲ اختصاصی که از موفقیت کمی برخوردار بود IBM Token Ring است. این پروتکل با استفاده از دستگاه های کانکتور و کابل های خاص IBM کار می کند و نودها باید دارای کارتهای شبکه Token Ring باشند. این دستگاه می تواند با سرعت ۱۶ مگابیت بر ثانیه کار کند، که زمان انتشارش چشمگیر بود، اما ماهیت اختصاصی تجهیزات و سریع تر شدن اترنت باعث شد Token Ring از دید طرفدارانش افت کند.

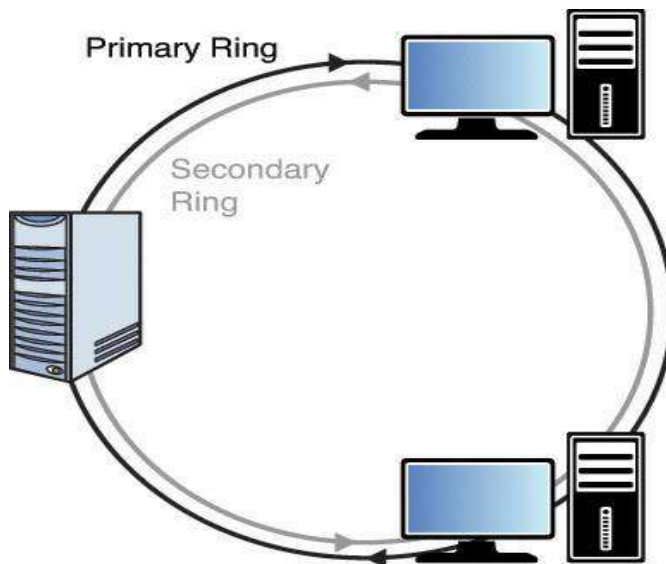
همانطور که قبلاً گفته شد، در بیشتر موارد توپولوژی شبکه فیزیکی همان توپولوژی منطقی است. Token Ring استثناء از آن قاعده کلی است. از منظر منطقی یک شبکه از نوع حلقه و از منظر فیزیکی یک ستاره است. در حالت ستاره همه دستگاه ها به یک دستگاه مرکزی به نام واحد دسترسی رسانه (MAU) وصل می شوند، اما وقتی جریان اطلاعات را بررسی می کنیم حلقه در MAU شکل می گیرد همانطور که در شکل ۴-۲۵ نشان داده شده است، با ورود و خروج از هر پورت MAU، در یک طراحی حلقه Ring از یک دستگاه به دستگاه دیگر می رود.



شکل ۴-۲۵: Token Ring

FDDI

پروتکل لایه ۲ دیگری که از یک توپولوژی حلقه استفاده می کند، واسط توزیع کننده داده ها در شبکه فیبرنوری (FDDI) Fiber Distributed Data Interface است. برخلاف Token Ring، یک حلقه فیزیکی و منطقی است. در واقع یک حلقه دابل است که هر یک در جهت متفاوتی برای تحمل خطا قرار می گیرند. همچنین با کابل کشی فیبر نوری اجرا می شود. در بسیاری موارد از ستون فقرات Backbone شبکه استفاده می شود و سپس به انواع دیگر شبکه مانند اترنت متصل می شود و شبکه هیبریدی را تشکیل می دهد و در شبکه های منطقه شهری Metropolitan area (MANs) مورد استفاده قرار می گیرد زیرا تا ۱۰۰ کیلومتر قابل نصب می باشد. شکل ۴-۲۶ نمونه ای از حلقه FDDI را نشان می دهد.



شکل ۴-۲۶

روشهای بحث

صرف نظر از پروتکل لایه ۲ در حال استفاده، باید روشی برای نتیجه استفاده از رسانه مشترک به کار برده شود. چهار فرایند اساسی برای عمل به عنوان پلیس ترافیک به کار گرفته شده است، به عبارت دیگر:

- CSMA / CD
- CSMA / CA
- Token passing
- Polling

این بخش هر یک را از دید مقایسه و تضاد بررسی کرده و نمونه هایی از فناوری هایی که هر یک استفاده می کنند را ارائه می دهد.

CSMA / CD در مقابل CSMA / CA

برای درک بهتر CSMA / CD و CSMA / CA، باید با مفهوم تصادم و حوزه های تصادم در یک رسانه شبکه مشترک آشنا باشید. تصادم هنگامی اتفاق می افتد که دو دستگاه به طور همزمان فریم را ارسال می کنند و باعث می شوند فریم ها و سیگنال های الکتریکی آنها در سیم به هم

برخورد کنند. هنگامی که این اتفاق می افتد، هر دو سیگنال و فریم هایی که آنها نشان می دهند از بین می روند یا حداقل خراب می شوند به گونه ای که هنگام رسیدن به مقصد دور ریخته می شوند. فساد یا دفع فریم باعث می شود که هر دو دستگاه فریم ها را مجدداً تغییر دهند و در نتیجه باعث کاهش توان کلی شوند.

دامنه های تصادم Collision Domains

دامنه تصادم بخشی از شبکه است که در آن امکان برخورد سیگنال های دو یا چند دستگاه وجود دارد. در یک توپولوژی Bus، کل شبکه را تشکیل می دهد زیرا کل Bus یک رسانه مشترک است. در یک توپولوژی ستاره، دامنه تصادم ها یا دامنه ها به دستگاه اتصال مرکزی بستگی دارد. دستگاه های اتصال مرکزی شامل هاب ها و سویچ ها هستند. اما اختلافات آنها با توجه به دامنه های تصادم، در اینجا مورد بررسی قرار می گیرد.

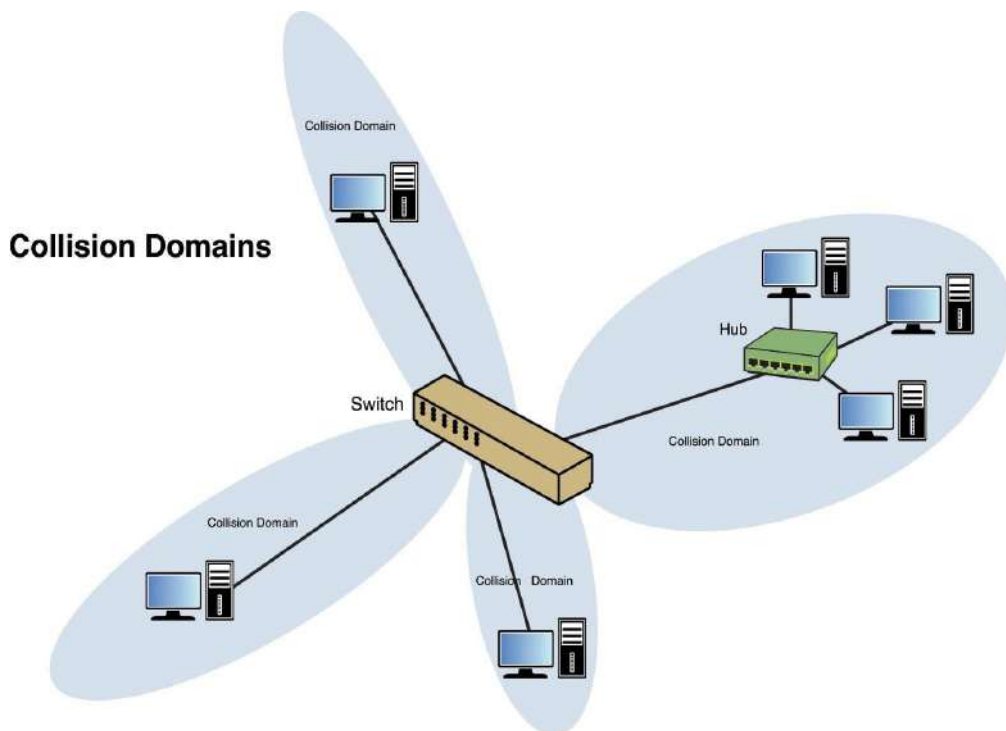
هاب یک جعبه اتصال غیر هوشمند است که تمام دستگاه ها به آن متصل می شوند. تمام پورت های هاب در یک دامنه تصادم یکسان هستند زیرا وقتی یک هاب یک فریم را دریافت می کند، فریم را از تمام پورت ها پخش می کند. بنابراین از نظر منطقی، شبکه هنوز یک bus است.

توپولوژی ستاره ای با سوئیچ در مرکز به این روش کار نمی کند. یک سوئیچ دارای هوشمندی می باشد تا آدرس MAC هر دستگاه را در هر پورت ضبط کند. پس از ثبت تمام آدرس های MAC دستگاه ها، سوئیچ فقط یک فریم را به پورتی که در آن دستگاه مقصد قرار دارد، می فرستد. از آنجا که ترافیک هر دستگاه از ترافیک دستگاه های دیگر جدا شده است، در نظر گرفته می شود که هر دستگاه در دامنه تصادم خاص خود قرار دارد.

این تفکیک ارائه شده توسط سوئیچ ها هم از نظر عملکرد و هم از مزایای امنیتی برخوردار است. از دیدگاه عملکرد، این تعداد تصادم ها را به میزان زیادی کاهش می دهد، در نتیجه باعث افزایش قابل توجه توان کلی در شبکه می شود. از منظر امنیتی، این بدان معنی است که یک اسنیفر متصل به پورت در سوئیچ فقط ترافیکی را که برای آن پورت تعیین شده است، ضبط می کند، نه همه ترافیک. این امنیت را با یک شبکه مرکزی محور مقایسه کنید. هنگامی که یک مرکز در مرکز شبکه ستاره ها قرار دارد، یک اسنیفر بدون توجه به پورتی که به آن وصل شده است، تمام ترافیک را جذب می کند، زیرا همه پورت ها در همان دامنه تصادم هستند.

در شکل ۴-۲۷، یک سوئیچ دارای چندین دستگاه و یک هاب متصل به آن با هر دامنه تصادم است که نشان می دهد چگونه این دو دستگاه دامنه های تصادم را ایجاد می کنند. توجه داشته

باشید که هر پورت سوئیچ یک دامنه تصادم است در حالی که کل هاب یک دامنه تصادم واحد است.



شکل ۴-۲۷: Collision Domains

CSMA / CD

در شبکه‌های 802.3، مکانیسمی به نام دسترسی چندگانه با قابلیت شنود سیگنال حامل/تشخیص تصادم (Carrier Sense Multiple Access / Detection Collision (CSMA / CD)) در هنگام استفاده از یک رسانه مشترک برای بازیابی از تصادم‌های اجتناب ناپذیر استفاده می‌شود. این فرایند یک مکانیسم گام به گام است که هر ایستگاه هر بار که نیاز به ارسال یک فریم واحد دارد از آن پیروی می‌کند. مراحل انجام به شرح زیر است:

- ۱- هنگامی که یک دستگاه نیاز به انتقال دارد، سیم را برای ترافیک موجود بررسی می‌کند. این فرایند به معنای شنود حامل Carrier sense نامیده می‌شود.
- ۲- اگر سیم روشن است، دستگاه شنود حامل را انتقال داده و ادامه می‌دهد.

۳- در صورت مشاهده ی تصادم، هر دو وسیله یک سیگنال وضعیت شلوغ را به تمام دستگاه های دیگر صادر می کنند که این امر عدم انتقال آنها را نشان می دهد. سپس هر دو دستگاه شمارنده انتقال مجدد را افزایش می دهند. این یک مجموعه کلی از تعداد دفعات انتقال این فریم و تصادم اتفاقی است. حداکثر تعداد آن در انتقال فریم وجود دارد.

۴- هر دو دستگاه مقدار تصادفی زمان را محاسبه می کنند (Random back off نامیده می شود) و قبل از انتقال مجدد منتظر آن زمان هستند.

۵- در بیشتر موارد چون هر دو وسیله مقدار تصادفی زمان انتظار را انتخاب می کنند، تصادم دیگری رخ نمی دهد. اگر این کار انجام شود، این روند تکرار می شود.

CSMA / CA

در 11.802 شبکه های بی سیم، CSMA / CD نمی تواند به عنوان یک روش حکمیت مورد استفاده قرار گیرد زیرا برخلاف استفاده از رسانه محدود، دستگاه ها نمی توانند یک تصادم را تشخیص دهند.

روش مورد استفاده دسترسی چندگانه با قابلیت شنود سیگنال حامل/پیشگیری از تصادم Carrier Sense Multiple Access / Collision Avoidance یا CSMA / CA نامیده می شود. این یک فرایند بسیار دشوار است زیرا هر ایستگاه باید هر فریم منتقل شده را تصدیق Acknowledge کند.

در قسمت "شبکه های بی سیم" عملیات شبکه 802.11 را با جزئیات بیشتری پوشش داده می شود، اما برای درک CSMA / CA حداقل باید مقدمات اساسی را ارائه دهیم. شبکه بی سیم معمولی شامل یک نقطه دسترسی AP و حداقل یک یا چند ایستگاه بی سیم است. در این نوع شبکه (به نام حالت زیرساخت شبکه بی سیم Infrastructure mode wireless network نامیده می شود)، ترافیک هرگز به طور مستقیم بین ایستگاه ها عبور نمی کند بلکه همیشه از طریق AP منتقل می شود. مراحل CSMA / CA به شرح زیر است:

۱- ایستگاه A دارای فریم برای ارسال به ایستگاه B است. از دو طریق ترافیک را بررسی می کند. ابتدا شنود حامل Carrier sense را انجام می دهد، به این معنی که گوش می دهد که آیا امواج رادیویی در فرستنده آن دریافت می شود یا خیر. ثانیاً، پس از ارسال گیرنده، به نظارت بر شبکه برای تصادم های احتمالی ادامه خواهد داد.

- ۲- در صورت انتقال ترافیک، ایستگاه A از یک مکانیزم شمارش معکوس داخلی به نام الگوریتم برگشت خاموش تصادفی Random back-off استفاده می‌کند. این شمارنده یا کانتر بعد از آخرین باری که به این ایستگاه اجازه انتقال داده می‌شود، شمارش را شروع می‌کند. همه ایستگاه‌ها تایمرهای شخصی خود را در نظر می‌گیرند. وقتی تایمر ایستگاه منقضی شد، ارسال آن مجاز است.
- ۳- اگر ایستگاه A شنود حامل را انجام می‌دهد، هیچ ترافیکی وجود ندارد و تایمر آن به صفر برخورد می‌کند، و فریم را ارسال می‌کند.
- ۴- فریم به AP می‌رود.
- ۵- برنامه تأییدیه ACK را به ایستگاه A ارسال می‌کند تا زمانی که این تأییدیه توسط ایستگاه A دریافت شود، همه ایستگاه‌های دیگر باید ساکت باشند. برای هر فریمی که AP نیاز به رله دارد، باید منتظر بماند که نوبت آن با استفاده از مکانیسم مشابه ایستگاه‌ها ارسال شود.
- ۶- هنگامی که نوبت آن در صف کش رسید، فریم از ایستگاه A به ایستگاه B منتقل می‌شود.
- ۷- ایستگاه B یک تأییدیه را به AP ارسال می‌کند. تا زمانی که این تأییدیه توسط AP دریافت نشود، تمام ایستگاه‌های دیگر باید ساکت باشند.
- همانطور که مشاهده می‌کنید، این فرایندها سربار Overhead زیادی ایجاد می‌کنند اما برای جلوگیری از تصادم در یک شبکه بی سیم مورد نیاز است.

عبور توکن Token Passing

هر دو شبکه FDDI و Token Ring از فرآیندی به نام عبور توکن استفاده می‌کنند. در این فرآیند، یک بسته ویژه به نام توکن در سراسر شبکه منتقل می‌شود. یک ایستگاه نمی‌تواند ارسال کند تا زمانی که توکن به آن رسیده و خالی شود. با استفاده از این فرآیند، هیچ تصادمی رخ نمی‌دهد زیرا دو دستگاه هرگز مجاز به ارسال همزمان نیستند. مشکلی که در این فرآیند وجود دارد این است که امکان وجود یک دستگاه واحد برای دستیابی به کنترل توکن و انحصار شبکه وجود دارد.

نظرسنجی Polling

روش مباحثه نهایی برای رای گیری، نظرسنجی است. در این سیستم، یک دستگاه اصلی با استفاده از هر دستگاه دیگر نظرسنجی می کند تا ببیند آیا نیاز به انتقال دارد یا خیر. به این ترتیب، هر دستگاه یک فرصت انتقال پیدا می کند. این روش در محیط اصلی رایج است.

WAN Technologies

بسیاری از فن آوری های مختلف برای دسترسی WAN به یک LAN توسعه یافته اند. آنها از نظر ظرفیت، در دسترس بودن و هزینه، متفاوت هستند. در این بخش به مقایسه فناوری های مختلف می پردازیم.

خطوط T

حامل های T خطوط اختصاصی هستند که مشترک، دسترسی خصوصی داشته و با مشتری دیگری اشتراکی ندارند. مشتریان می توانند یک T1 کامل را خریداری کنند، یا می توانند بخشی از T1 را با نام T1 کوچک (Fractional T1) خریداری کنند. خطوط T1 از ۲۴ کانال تشکیل شده است که هر یک قادر به ۶۴ Kbps است. این بدان معنی است که T1 دارای ظرفیت کلی ۱,۵۴۴ Mbps است. T1 از طریق فرآیندی به نام تقسیم بندی زمان Time-division multiplexing (TDM) به کانال ها تقسیم می شود.

حامل های T نیز با افزایش بیشتری همراه هستند. جدول ۴-۸ خلاصه ای از حامل های T و ظرفیت آنها را نشان می دهد.

Carrier	Number of Channels	Speed (Mbps)
Fractional	1	0.064
T1	24	1.544
T2	96	6.312
T3	672	44.736
T4	4032	274.176
T5	5760	400.352

جدول ۴-۸: حامل های T

خطوط E

در اروپا، فناوری مشابه خطوط حامل T با نام حاملهای E وجود دارد. با استفاده از این فناوری، ۳۰ کانال به جای ۲۴ کانال دسته بندی شده اند. این فناوری ها سازگار نبوده و اندازه های موجود کمی متفاوت است. جدول ۴-۹ برخی از توسعه حامل های E انتخاب شده را نشان می دهد.

Signal	Rate
E0	64 Kbps
E1	2.048 Mbps
E2	8.448 Mbps
E3	34.368 Mbps
E4	139.264 Mbps
E5	565.148 Mbps

جدول ۴-۹: حامل های E

خطوط OC (SONET)

شبکه نوری همزمان Synchronous Optical Networking (SONET) از پیوندهای مبتنی بر فیبرنوری استفاده می کند که روی خطوط اندازه گیری شده در سرعت انتقال حامل نوری Optical carrier (OC) کار می کنند. این خطوط با یک عدد صحیح از واحد اصلی نرخ Rate تعریف می شوند. نرخ اصلی OC-1، 55.84 مگابیت بر ثانیه است، و تمام نرخ های دیگر چند برابر هستند. به عنوان مثال، OC-3 بازده 155.52 Mbps است. جدول ۴-۱۰ برخی از این نرخ ها را نشان می دهد. ممکن است توسعه های کوچکتری توسط یک شرکت استفاده شود، در حالی که لوله های (Pipe) بزرگتری توسط یک ارائه دهنده خدمات قابل استفاده هستند.

Optical Carrier	Speed
OC-3	155 Mbps
OC-12	622 Mbps
OC-48	2.5 Gbps
OC-192	9.6 Gbps

جدول ۴-۱۰: RATE حامل

CSU / DSU

بدون شک در مورد دستگاهی که بسیاری از مشتریان برای اتصال WAN به آن متصل می شوند، مبحث اتصالات WAN، کامل نخواهد بود. واحد خدمات داده / واحد کانال خدمات channel (CSU/DSU) Service unit/Data service unit یک شبکه LAN را به یک WAN متصل می کند. این دستگاه ترجمه ای از اطلاعات را از یک فرمت قابل قبول در LAN به محلی که می تواند از طریق اتصال WAN منتقل شود، انجام می دهد.

CSU / DSU یک دستگاه مجهز ارتباطات داده (DCE) Data communications equipment در نظر گرفته می شود و واسط را برای روتر فراهم می کند که یک دستگاه مجهز ترمینال داده (DTE) Data terminal equipment محسوب می شود. CSU / DSU به احتمال زیاد متعلق به telco است، اما نه همیشه، و در بعضی موارد ممکن است این قابلیت در واسط روتر ساخته شود و یک دستگاه جداگانه غیر ضروری باشد.

سوئیچ مدار در مقابل تعویض بسته

Circuit-Switching Versus Packet-Switching

در مورد اتصالات WAN، بحث در مورد انواع شبکه هایی که ممکن است این اتصالات از آنجا عبور کنند نیز مفید است. برخی از آنها با سوئیچ مدار Circuit-switched، در حالی که برخی دیگر تعویض بسته Packet-switched هستند. شبکه های سوئیچینگ مدار (مانند تلفن) مسیر مشخصی را برای مقصد تعیین می کنند و فقط از آن مسیر برای کل ارتباطات استفاده می کنند. این امر با عملیاتی قابل پیش بینی با تأخیرهای ثابت انجام می شود. این شبکه ها معمولاً دارای ترافیک صوتی محور Voice-oriented هستند.

شبکه های تعویض بسته Packet-switching مانند اینترنت یا LAN یک مسیر بهینه را برای هر بسته ایجاد می کنند. این بدان معنی است که هر بسته ممکن است برای رسیدن به مقصد مسیر متفاوتی را طی کند. ترافیک در این شبکه ها دچار افت عملکردی می شود و میزان تأخیر می تواند بسیار متفاوت باشد. این نوع شبکه ها معمولاً دارای ترافیک داده محور Data-oriented هستند.

رله فریم Frame Relay

یک پروتکل لایه ۲ است که برای اتصالات WAN استفاده می شود. بنابراین، هنگامی که ترافیک اترنت باید از یک لینک Frame Relay عبور کند، هدر لایه ۲ بسته برای مطابقت با Frame

Relay کاملاً بازسازی می‌شود. با رسیدن فریم Frame به مقصد، یک هدر لایه ۲ اترنت جدید برای آن بخش از شبکه روی بسته قرار می‌گیرد.

هنگامی که اتصالات Frame Relay فراهم شد، مشتری حداقل مقدار پهنای باند به نام نرخ اطلاعات تضمین شده (پهنای باند تضمین شده) Committed Information Rate (CIR) را پرداخت می‌کند، که حداقل عملکرد خواهد بود. با این حال، از آنجا که Frame Relay یک شبکه بسته بندی شده با استفاده از کلیدهای Frame Relay است، عملکرد واقعی بر اساس شرایط متفاوت خواهد بود. مشتریان به جای داشتن یک خط اختصاصی، مانند خط T1 یا خدمات دیجیتال شبکه دیجیتال ISDN، شبکه را به اشتراک می‌گذارند. بنابراین در بسیاری موارد عملکرد واقعی از CIR فراتر خواهد رفت.

ATM

حالت انتقال ناهمگام (Asynchronous Transfer Mode (ATM)) یک فناوری تعویض سلول است. این سلول‌های اندازه ثابت ۵۳ بایت را به جای بسته‌ها منتقل می‌کند و پس از ایجاد مسیر، برای کل ارتباطات از همان مسیر استفاده می‌کنند. استفاده از یک مسیر ثابت، عملکرد را قابل پیش بینی می‌کند، و آن را به گزینه‌ای مناسب برای صدا و فیلم تبدیل کرده، که به چنین پیش بینی نیاز دارند. در جایی که شبکه‌های IP برای اطمینان از انتقال مناسب داده‌ها به مبدأ و مقصد وابسته هستند، این مسئولیت بر عهده دستگاه‌های بین این دو در دنیای ATM قرار می‌گیرد.

ATM بیشتر برای ستون فقراتشان از حامل‌ها و ارائه دهنده خدمات استفاده می‌کند، اما برخی از شرکت‌ها ستون فقرات ATM و سوئیچ‌های ATM را پیاده سازی کرده اند. این امر به آنها امکان ایجاد اتصال ATM به شرکت مخابراتی را می‌دهد، که می‌تواند از طریق اتصال با یک لینک T کم هزینه تر شده، زیرا هزینه اتصال ATM بر خلاف هزینه ثابت T1 مبتنی بر استفاده خواهد بود.

X.25

X.25 تا حدودی مانند Frame Relay است که در آن ترافیک از طریق شبکه تعویض بسته‌ها packet-switching حرکت می‌کند. وزن X.25 توسط پهنای باند استفاده شده است. داده‌ها به فریم‌های کنترل پیوند داده سطح بالا High-Level Data Link Control (HDLC) به ۱۲۸ بایت تقسیم می‌شوند. با این حال، این فناوری قدیمی است و در زمانی ایجاد شد که خطوط

انتقال پر سر و صدا یک دغدغه بزرگ محسوب می‌شد. بنابراین، بسیاری از مکانیسم‌های بررسی خطا بعدها ساخته شد که آن را بسیار ناکارآمد کرد.

تعویض سرویس داده مگا بیتی Switched Multimegabit Data Service

یک فناوری تعویض بسته از نوع بدون اتصال Connectionless است که در یک شبکه عمومی مستقر برقرار می‌شود. این دستگاه تا حد زیادی با سایر فن آوری‌های WAN بسته بندی شده است و می‌تواند کارایی شبکه مانند LAN را به یک WAN ارائه دهد و به طور کلی از طریق یک حلقه SONET با حداکثر شعاع خدمات مؤثر در حدود ۳۰ مایل تحویل داده شود.

پروتکل نقطه به نقطه Point-to-Point Protocol (PPP)

یک پروتکل لایه ۲ است که فریم بندی و کپسوله سازی داده‌ها را از طریق اتصالات نقطه به نقطه انجام می‌دهد. اینها اتصالی به ISP است که در آن فقط دستگاه مشتری و دستگاه ISP در هر دو قسمت ساکن هستند. این پروتکل می‌تواند تعدادی از پروتکل‌های مختلف LAN مانند TCP / IP را کپسوله کند و این کار را با استفاده از یک پروتکل هسته اصلی شبکه Network Core Protocol (NCP) برای هر یک از پروتکل‌های LAN مورد استفاده، انجام می‌دهد. در کنار استفاده از چندین NCP، از یک پروتکل کنترل پیوند واحد Link Control Protocol (LCP) برای برقراری ارتباط استفاده می‌کند. PPP امکان تأیید صحت ارتباط بین دستگاه‌ها را با استفاده از پروتکل احراز هویت گذرواژه Password Authentication Protocol (PAP) یا پروتکل احراز هویت دست دادن با چالش Challenge Handshake Authentication Protocol (CHAP) فراهم می‌کند. در حالی که PAP اعتبارنامه را به صورت متن واضح منتقل می‌کند، CHAP اعتبارنامه را به خط ارسال نمی‌کند و بسیار امن تر است.

واسط سریال پر سرعت High-Speed Serial Interface (HSSI)

یکی از پیاده سازی‌های فیزیکی یک واسط سریال است. از آنجا که این واسطها در دستگاه‌ها وجود دارند، اینگونه در نظر گرفته می‌شوند که در لایه ۱ مدل OSI کار می‌کنند. لایه فیزیکی لایه‌ای است که به سیگنالینگ پیام و واسط بین فرستنده یا گیرنده و رسانه مربوط می‌شود. نمونه‌هایی از واسط‌های سریال دیگر عبارتند از:

○ X.25

V.35 ○

X.21 ○

واسط کاربری HSSI در هر دو روتر و مالتی پلکسر یافت می‌شود و اتصال به سرویس‌هایی مانند Frame Relay و ATM را فراهم می‌کند و با سرعت حداکثر ۵۲ مگابیت بر ثانیه کار می‌کند.

PSTN (POTS, PBX)

احتمالاً حداقل جذابیت اتصال از نوع WAN، حداقل از نقطه نظر کارایی، شبکه تلفن سوئیچ عمومی (PSTN) Public switched telephone network است. همچنین به آن سرویس تلفنی قدیمی ساده (POTS) Plain old telephone service نیز گفته می‌شود، این شبکه تعویض مدار Circuit-switched است که سالهاست که برای سرویس تلفن آنالوگ استفاده می‌شود و اکنون عمدتاً یک عملیات دیجیتالی است.

این شبکه با استفاده از مودم‌های یک خط آنالوگ یا ISDN برای خطوط تلفن دیجیتال قابل استفاده است. هر دو گزینه در بخش "فناوری ارتباط اتصال از راه دور" با جزئیات بیشتری مورد بحث شده است زیرا کاربرد اصلی آنهاست. در بعضی موارد، این اتصالات ممکن است بین دفاتر مورد استفاده قرار گیرد، اما به دلیل عملکرد ضعیف، معمولاً فقط به عنوان یک راه حل پشتیبان در صورت عدم موفقیت گزینه مناسبی می‌باشد. این اتصالات باید هر بار که بر خلاف راه‌های "همیشه روشن" Always on مانند کابل یا DSL استفاده شوند، برقرار شود.

VoIP

اگرچه صدا روی PSTN تعویض مدار (سوئیچ مدار) Circuit-switched است، صدا نیز می‌تواند در بسته‌ها کپسوله شود و در شبکه‌های تعویض بسته ارسال شود. وقتی این کار بر روی یک شبکه IP انجام شود، به آن Voice over IP (VoIP) گفته می‌شود. در جایی که شبکه‌های سوئیچینگ مدار از پروتکل سیگنالینگ سیستم هفت (SS7) Signaling System 7 برای تنظیم، کنترل و قطع ارتباط استفاده می‌کنند، VoIP از پروتکل شروع جلسه SIP برای قطع شدن جلسات تماس استفاده می‌کند. در پیاده‌سازی‌های VoIP، QoS به منظور اطمینان از برخورداری از ترافیک خاص (بویژه صدا) نسبت به شبکه، ترجیح داده شده است.

SIP یک پروتکل لایه کاربردی است که می‌تواند از طریق TCP یا UDP کار کند. آدرس دهی از منظر آدرس‌های IP است و ترافیک voice از همان شبکه‌ای استفاده می‌کند که برای داده‌های منظم استفاده می‌شود. از آنجا که همیشه تأخیر در این شبکه‌ها امکان‌پذیر است، پروتکل‌هایی

برای کاهش اثر اجرا شده است زیرا این نوع ترافیک بسیار بیشتر تحت تأثیر تأخیر قرار می گیرد. اپلیکیشن هایی مانند صدا و فیلم نیاز به داشتن پروتکل ها و دستگاه هایی دارند که می توانند یک شبکه متقارن یا همگام Isochronous را فراهم کنند. شبکه های همگام پهنای باند مداوم و بدون وقفه را تضمین می کنند. از منبع ساعت داخلی و بیت های شروع و توقف استفاده نمی شود. همه بیت ها از اهمیت برابر برخوردار هستند و پیش بینی می شود که در فواصل منظم اتفاق بیفتند. VoIP را می توان با انجام اقدامات زیر ایمن کرد:

- ✓ برای تلفن های IP یک VLAN یا زیر شبکه جداگانه ایجاد کنید و از دسترسی سایر رایانه ها به این VLAN جلوگیری کنید.
- ✓ یک دیوار آتش آگاهانه VoIP را در محیط مستقر کنید.
- ✓ مطمئن شوید که کلمه عبورهای مرتبط با VoIP قوی هستند.
- ✓ لایه شبکه را با IPsec ایمن کنید.

دستگاه های دسترسی به شبکه Network Access Control Devices

کنترل دسترسی به شبکه (NAC) سرویسی است که فراتر از احراز هویت کاربر است و شامل بررسی وضعیت رایانه ای است که کاربر هنگام ایجاد دسترسی از راه دور یا اتصال VPN به شبکه معرفی می کند.

دنیای سیسکو این سرویس ها را کنترل پذیرش شبکه Network Admission Control می نامد. علیرغم اصطلاح مورد استفاده، اهداف ویژگی های یکسانی دارد.

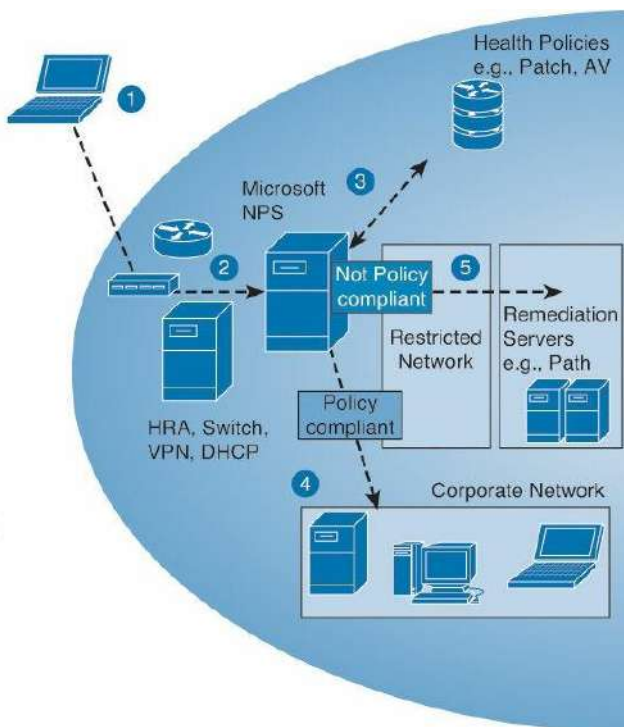
بررسی تمام درخواست دستگاه های دسترسی به شبکه برای بدافزارها (Malware)، روزرسانی های امنیتی از دست رفته و سایر مشکلات امنیتی دستگاه ها که به طور بالقوه می توانند به شبکه معرفی شوند.

مراحلی که در Microsoft NAP رخ می دهد در شکل ۴-۲۸ نشان داده شده است. وضعیت سلامتی درخواست دستگاه دسترسی، جمع آوری شده و به سرور خط مشی شبکه Network Policy Server (NPS) فرستاده می شود، جایی که این وضعیت با شرایط و مقررات مورد مقایسه قرار می گیرد. در صورت برآورده شدن شرایط و مقررات، دسترسی مجاز است.

Network Access Protection

How it works

- 1 Access requested
- 2 Health state sent to NPS (RADIUS)
- 3 NPS evaluates against local health policies
- 4 If compliant, access granted
- 5 If not compliant, restricted network access and remediation



شکل ۴-۲۸: مراحل NAP

این موارد محدودیت‌های استفاده از NAC یا NAP می‌باشد:

- ✓ آنها برای رایانه‌های تحت مدیریت شرکت خوب فعالیت می‌کنند اما برای مهمانان guests کمتر فعالیت می‌کنند.
- ✓ آنها تمایل دارند فقط به تهدیدهای شناخته شده واکنش نشان دهند نه تهدیدهای جدید.
- ✓ بازده سرمایه گذاری هنوز تأیید نشده است.
- ✓ برخی از پیاده سازی‌ها و اجراها شامل پیکربندی گیج کننده هستند.

قرنطینه / ترمیم Quarantine/Remediation

اگر مرحله ۵ را در فرآیند نشان داده شده در شکل ۴-۲۸ بررسی کنید، می‌بینید که دستگاهی که در تست شکست خورده، در یک شبکه محدود قرار می‌گیرد تا بتوان آن را ترمیم کرد. یک سرور ترمیم Remediation server، مشکلات کشف شده در دستگاه را برطرف می‌کند. ممکن

است بدافزار را حذف کرده، بروزرسانی های سیستم عامل مفقوده را نصب کرده یا تعاریف ویروس را بروزرسانی کند. پس از اتمام فرآیند ترمیم، به دستگاه دسترسی کامل شبکه داده می شود.

فایروال ها / پروکسی ها

می توان از فایروال ها و پروکسی ها به عنوان بخشی از استقرار NAC استفاده کرد. فایروال ها با فیلتر کردن ترافیک ورودی از طریق آدرس منبع، آدرس مقصد یا خدمات، قوانین امنیتی را اعمال می کنند. مهم است که قوانین به درستی پیکربندی شوند تا اطمینان حاصل شود که دسترسی شبکه به ترافیک مخرب یا کاربران، داده نمی شود. پروکسی ها به عنوان واسطه بین مشتری یا سرور قابل اعتماد و غیر قابل اعتماد عمل می کنند. هنگامی که پروکسی ها مستقر شدند، به نظر می رسد که تمام بسته های ارسال شده به مشتری یا سرورهای غیر قابل اعتماد از پروکسی ها سرچشمه می گیرند، بنابراین به همه میزبان های داخلی امکان می دهند تا پشت یک آدرس IP عمومی پنهان شوند.

امنیت Endpoint

امنیت Endpoint یک حوزه امنیتی است که سعی می کند با ماندن در تماس مداوم با سیستم های فردی از یک مکان مرکزی، از سیستم های فردی در یک شبکه محافظت کند. به طور معمول در مدل سرور مشتری Client server کاری می کند به این دلیل که هر سیستم دارای نرم افزاری است که با نرم افزار روی سرور مرکزی ارتباط برقرار می کند و عملکرد ارائه شده می تواند متفاوت باشد. در ساده ترین شکل، شامل نظارت و بروز رسانی خودکار و پیکربندی پچ های امنیتی و تنظیمات فایروال شخصی است. در سیستم های پیشرفته تر، ممکن است هر بار اتصال به شبکه، سیستم را بررسی کند. این آزمایش تضمین می کند که همه پچ های امنیتی به روز هستند و حتی در سناریوهای پیشرفته تر می تواند به صورت خودکار ترمیم را به رایانه ارائه دهند. در هر صورت رایانه تا زمانی که مشکل برطرف نشود، به صورت دستی یا خودکار، اجازه اتصال به شبکه را نمی دهد. اقدامات دیگر شامل استفاده از رمزگذاری دستگاه یا درایو، فعال کردن قابلیت های مدیریت از راه دور (مانند پاک کردن از راه دور و موقعیت مکانی از راه دور) و اجرای سیاست ها و توافق های مربوط به مالکیت دستگاه است تا سازمان بتواند دستگاه را مدیریت یا تصرف کند.

شبکه‌های توزیع محتوا Content Distribution Networks

شبکه توزیع محتوا یا CDN که به آن نیز شبکه تحویل محتوا Content Delivery Network گفته می‌شود، شبکه توزیع شده از سرورها است که معمولاً در چندین مرکز داده به اینترنت متصل است. محتوای موجود در CDN می‌تواند شامل متن، گرافیک، اپلیکیشن‌های، رسانه‌های جریان و سایر مطالب مهم برای کاربران باشد. CDNها بسیار مقیاس پذیر هستند و به صاحبان این امکان را می‌دهند تا به سرعت مطابق نیاز کاربران نهایی تنظیم شوند. مثالهای CDN شامل Microsoft Azure CDN و Amazon CloudFront هستند

کانال‌های ارتباطی امن Secure Communication Channels

سازمان‌ها باید از امنیت کانال‌های ارتباطی مطمئن شوند. در این بخش به بحث در مورد صدا، همکاری چندرسانه‌ای، دسترسی از راه دور و شبکه‌های مجازی می‌پردازیم.

• صدا Voice

کانال‌های ارتباط Voice شامل سیستم‌های PSTN، POTS، PBX هستند که برای مدیریت بیشتر ارتباطات Voice از طریق شبکه‌های ارتباطی استفاده می‌شوند. سیستم‌های POTS از ارتباطات آنالوگ استفاده می‌کنند، در حالی که PSTN در ابتدا آنالوگ بود اما به استفاده از ارتباطات عمدتاً دیجیتال تغییر کرده است.

ارتباطات آنالوگ از کیفیت Voice و ویژگی‌های اصلی تلفن از جمله انتقال تلفن پشتیبانی می‌کند. ارتباط دیجیتال فراتر از آنالوگ برای پشتیبانی از موسیقی در حالت آماده باش، ادغام VoIP و آلارم‌ها است. علاوه بر این، سیستم‌های دیجیتال با سیم کشی مسی مورد استفاده سیستم‌های آنالوگ اعتماد ندارند.

• همکاری چندرسانه‌ای Multimedia Collaboration

در شرکت‌های مدرن امروز، اشتراک گذاری چندرسانه‌ای در هر دومورد ارائه وب یا جلسات و برنامه‌های پیام رسانی فوری گسترش یافته است. توجه داشته باشید که همه ابزارها و محصولات همکاری با توجه به امنیت به طور یکسان ایجاد نمی‌شوند. بسیاری با تأکید بر سهولت استفاده نسبت به امنیت ساخته شده اند. این یک مسئله اساسی است که باید هنگام انتخاب محصول در نظر گرفته شود. برای ارائه دهنده و گیرنده، شرایط امنیتی زیر باید رعایت شود:

- ✓ محرمانه بودن داده ها Data confidentiality
- ✓ احراز هویت مبدا Origin authentication
- ✓ محرمانه بودن هویت Identity confidentiality
- ✓ یکپارچگی داده Data integrity
- ✓ عدم تکذیب رسید Non-repudiation of receipt
- ✓ رد انتقال Repudiation of transmission
- ✓ عدم تکذیب انتقال Non-repudiation of transmission
- ✓ دسترسی حضوری Availability to present
- ✓ دسترسی به دریافت کردن Availability to receive

اپلیکیشن های همتا به همتا (P2P) امروزه بیشتر مورد استفاده قرار می گیرد. با این حال، بسیاری از سازمان ها دغدغه استفاده آنها را دارند زیرا سهم مالکیت معنوی در این اپلیکیشن ها بسیار آسان است. اپلیکیشن های P2P اغلب برای نقض قوانین مالکیت معنوی استفاده می شوند.

از آنجا که اپلیکیشن های P2P با دزدی و نقض حق چاپ همراه است، سازمان ها باید این اپلیکیشن ها را در سیاست های امنیتی خود درج کنند. از آنجا که این اپلیکیشن ها می توانند به عنوان ابزاری برای ورود به شبکه سازمان مورد استفاده قرار گیرند، معمولاً بهتر است برای جلوگیری از اپلیکیشن های P2P، خط مشی و قوانینی پیاده سازی شود.

فناوری جلسات از راه دور Remote Meeting Technology

بسیاری از شرکت ها، فناوری ها و خدماتی را ارائه می دهند که اجازه می دهد جلسات مجازی از طریق اینترنت اتفاق بیفتد. در بیشتر موارد، آنها از افزونه های مرورگر در رایانه میزبان استفاده می کنند و اجازه به اشتراک گذاری دسکتاپ و کنترل از راه دور را می دهند. اگر سازمان ها قصد دارند فناوری جلسات از راه دور را پیاده سازی کنند، متخصصان امنیت باید به طور کامل در مورد گزینه های ممکن و امنیت موجود در بخشی از فناوری جلسات از راه دور، به طور خاص احراز هویت و رمزگذاری تحقیق کنند. علاوه بر این، هر پرسنلی که میزبان جلسات مجازی هستند باید در مورد استفاده صحیح از چنین اپلیکیشن هایی و هرگونه سیاست امنیتی که در استفاده از آنها تأثیر می گذارد، آموزش ببینند.

پیام رسانی فوری Instant Messaging

در حالی که اپلیکیشن‌های پیام رسانی فوری ارتباط برقرار کردن با یکدیگر را بسیار ساده تر می‌کنند، می‌توانند ویژگی‌هایی را نیز در بر گیرند که بسیاری از سازمان‌ها ریسک‌های امنیتی را در نظر می‌گیرند. اپلیکیشن‌های پیام فوری معمولاً از سیستم‌های هم‌تا به هم‌تا P2P، سیستم‌های سرور محور یا سیستم‌های کارگزاری استفاده می‌کنند. سازمان مجبور است اجازه دهد به استفاده از پروتکل پیام رسانی فوری مناسب برای اپلیکیشن‌هایی که سازمان اجرا می‌کند. پروتکل‌های مورد استفاده شامل پروتکل پیام رسانی و حضور گسترده Extensible Messaging and Presence Protocol (XMPP) و چت رله اینترنت (IRC) Internet Relay Chat هستند.

به خاطر داشته باشید که شناسایی کاربر به راحتی در اپلیکیشن‌های پیام رسانی فوری جعل می‌شود. همه پیام‌ها به صورت Cleartext از جمله پیام‌های انتقال پرونده ارسال می‌شوند. بسیاری از اپلیکیشن‌های پیام رسانی فوری دارای اسکریپت هستند، به این معنی که کاربر می‌تواند به راحتی در اجرای یک دستور که فکر می‌کند بخشی معتبر از اپلیکیشن است فریب بخورد که در واقع یک اسکریپت مخرب است که توسط یک مهاجم درج شده است. سرانجام، حملات مهندسی اجتماعی و هرزنامه‌ها بر روی پیام‌های فوری (SPIM) instant messaging رایج هستند زیرا کاربران به راحتی می‌توانند اطلاعاتی را که برای کاربران معتبر در نظر می‌گیرند به اشتراک بگذارند.

• دسترسی از راه دور Remote Access

هرچه دنیای ما مجازی تر می‌شود، فن آوری‌های دسترسی از راه دور برای سازمان‌ها اهمیت بیشتری پیدا می‌کنند. این فناوری‌ها به کارکنان امکان می‌دهند، تقریباً در هر نقطه از جهان کار کنند، مشروط بر اینکه وسیله‌ای برای اتصال به اینترنت یا شبکه دیگر داشته باشند. در این بخش فن آوری‌های اتصال از راه دور، دستگاه‌های صفحه نمایش VPN، اپلیکیشن‌های مجازی / دسکتاپ و ارتباط از راه دور مورد بحث قرار می‌گیرد.

فن آوری‌های اتصال از راه دور Remote Connection Technologies

در بسیاری از موارد اتصالات باید به شبکه اصلی از خارج شبکه برقرار شود. دلایل این ارتباطات متفاوت است. در بعضی موارد، به این منظور است که از طریق راه دور بتوانیم به کار خود بپردازیم،

گویی در دفتر با تمام منابع شبکه‌ای که در دسترس است، نشستیم. در موارد دیگر، به منظور مدیریت دستگاه‌های شبکه است، در حالی که در سایر موارد این امکان وجود دارد که بین دفاتر کوچک و دفتر اصلی ارتباط برقرار شود.

در این بخش، برخی از این نوع اتصالات به همراه برخی از اقدامات امنیتی که به صورت دستی با آنها انجام می‌شود، مورد بحث قرار می‌گیرد. این اقدامات هم مکانیسم رمزگذاری و هم برنامه‌های احراز هویت را شامل می‌شود.

Dial-up

اتصال Dial-up ارتباطاتی است که از PSTN استفاده می‌کند. اگر از طریق خط تلفن آنالوگ آغاز شده باشد، به یک مودم نیاز دارد که داده‌های دیجیتالی را در انتهای (End) ارسال به آنالوگ تبدیل کند و یک مودم در انتهای (End) دریافت آن را به دیجیتال تبدیل کند. این خطوط تا ۵۶ کیلوبیت بر ثانیه کار می‌کنند.

اتصالات Dial-up می‌توانند از پروتکل Serial Line Internet Protocol (SLIP) یا PPP در لایه ۲، استفاده کنند. SLIP یک پروتکل قدیمی است که توسط PPP منسوخ شده است. PPP امکان احراز هویت و قابلیت چند لینی را فراهم می‌کند. تماس گیرنده توسط سرور دسترسی از راه دور Remote access server تأیید می‌شود. این فرآیند احراز هویت را می‌توان با استفاده از سرور + TACACS یا RADIUS متمرکز کرد. این سرورها بعداً به طور کامل مورد بحث قرار می‌گیرند. برخی اقدامات اساسی امنیتی که هنگام استفاده از Dial-up باید انجام شود عبارتند از:

- سرور دسترسی از راه دور، تماسی با شماره از پیش تعیین شده دارد. انتقال تماس را اجازه ندهید زیرا می‌تواند برای خنثی کردن این اقدامات امنیتی استفاده شود.
- مودم باید تنظیم شود که پس از تعداد مشخصی از حلقه‌ها برای خنثی کردن جنگ ضد Dial-up پاسخگو باشد.
- برای امنیت فیزیکی مودم‌ها را در یک مکان ادغام کنید و مودم‌هایی که استفاده نمی‌شوند را غیرفعال کنید.
- از قوی ترین مکانیسم‌های احراز هویت ممکن استفاده کنید.

اگر اتصال از طریق یک خط دیجیتال انجام شود، می‌توان از ISDN استفاده کرد. همچنین برای برقراری ارتباط باید شماره گیری Dial-up شود اما قابلیت بسیار بیشتری را ارائه می‌دهد و کل فرایند دیجیتال است.

ISDN

شبکه دیجیتال خدمات یکپارچه Integrated Services Digital Network (ISDN) گاهی به آن شماره گیری دیجیتال نیز گفته می‌شود. تفاوت بزرگ بین ISDN و Dial-up آنالوگ در عملکرد است. ISDN از دو طریق قابل ارائه است:

- نرخ پایه (Basic rate (BRI): سه کانال - دو کانال B را فراهم می‌کند که هر یک ۶۴ Kbps و یک کانال D که ۱۶ Kbps است، مجموعاً ۱۴۴ Kbps فراهم می‌کند.
- نرخ اصلی (Primary Rate (PRI: می‌تواند حداکثر ۲۳ کانال B و یک کانال D مجموعاً 1.544 Mbps فراهم کند.

اگرچه ISDN در حال حاضر معمولاً فقط به عنوان یک راه حل اتصال پشتیبان مورد استفاده قرار می‌گیرد و بسیاری ISDN را یک اتصال اختصاصی و در نتیجه امن می‌دانند، اما می‌توان حملات را بر ضد اتصالات ISDN پیاده سازی کرد، از جمله

- حملات فیزیکی *Physical attacks*: حملات افرادی است که قادر به دستیابی فیزیکی به تجهیزات شبکه دارند. با توجه به ISDN، کدهای مخابراتی مشترک می‌توانند AP را ارائه دهند. اقدامات امنیتی فیزیکی که باید دنبال شود در فصل ۷ توضیح داده شده است.
- حملات روتر *Router attacks*: اگر روتر متقاعد شود که تماس ISDN را از روتر قلابی بپذیرد، ممکن است به مهاجمان اجازه ورود به شبکه را بدهد. روترها باید برای احراز هویت قبل از پذیرش درخواست تماس، پیکربندی شوند.

DSL

خط دیجیتال مشترک Digital Subscribers Line (DSL) گزینه‌ای بسیار متداول است که یک اتصال سریع پر سرعت را از خانه یا اداره کوچک به ISP فراهم می‌کند. اگرچه از خطوط تلفن موجود استفاده می‌کند، اما این اتصال همیشه روشن است. با استفاده از فرکانسهای مختلف نسبت به انتقال voice در خطوط مسی، صحبت کردن در تلفن و استفاده از شبکه داده (اینترنت) به طور همزمان امکان پذیر است.

همچنین بسیار سریعتر از ISDN یا Dial-up است. در چندین نوع مختلف ارائه می‌شود، برخی از آنها آپلود uploading و دانلود Downloading همزمان را ارائه می‌دهند (که به آن خدمات متقارن Symmetric service گفته می‌شود) در حالی که بیشتر عملکرد دانلود بهتر از عملکرد

آپلود را (خدمات نامتقارن Asymmetric service) ارائه می دهند. برخی از نسخه های ممکن عبارتند از:

- Symmetric DSL (SDSL): معمولاً از ۱۹۲ Kbps تا ۱,۱ Gbps در هر دو جهت ارائه می شود. معمولاً توسط کسب و کارها مورد استفاده قرار می گیرد.
- Asymmetric DSL (ADSL): معمولاً بارگذاری از ۱۲۸ Kbps به ۳۸۴ Kbps و دانلود تا ۷۶۸ Kbps را ارائه می دهد. معمولاً در خانه ها استفاده می شود.
- DSL با نرخ بیت بالا (HDSL): High Bit-Rate DSL: سرعت T1 را فراهم می کند.
- DSL با نرخ بیت بسیار بالا (VDSL): Very High Bit-Rate DSL: قادر به پشتیبانی از تلویزیون با کیفیت بالا HDTV و VoIP است.

برخلاف اتصالات کابل، اتصالات DSL پیوندهای اختصاصی هستند، اما هنوز هم مسائل امنیتی برای در نظر گرفتن وجود دارد. رایانه های شخصی و سایر دستگاه هایی که برای دسترسی به خط DSL استفاده می شوند باید طبق گزینه های زیر در گزینه های اینترنت تنظیم شوند:

- برای فسخ مجوز، گواهی نامه Certificate ناشر بررسی شود.
- حفاظت از حافظه را برای کمک به کاهش حملات آنلاین فعال شود.
- فیلتر صفحه نمایش هوشمند فعال شود.
- از SSL 3.0 استفاده شود.
- از TLS 1.1 یا بالاتر استفاده شود.
- درباره عدم تطابق آدرس گواهی نامه هشدار داده شود.
- اگر Submittal به منطقه ای هدایت شود که اجازه ارسال پیام را نداشته باشد، هشدار داده شود.

Submittal: همه چیز در مدیریت ساخت و ساز نقشه های فروشگاه، داده های مواد، نمونه ها و داده های محصول است. Submittals در درجه اول برای معمار و مهندس لازم است تا تأیید کند که محصولات صحیح روی پروژه نصب می شود.

مسئله دیگر در مورد DSL این واقعیت است که همیشه اتصال برقرار است. این بدان معنی است که دستگاه به طور معمول همان آدرس IP را نگه می دارد. یک آدرس IP استاتیک یک هدف ثابت را برای مهاجم فراهم می کند. بنابراین، اقداماتی مانند NAT به پنهان کردن آدرس IP واقعی دستگاه از دنیای خارج کمک می کند.

کابل Cable

اتصال به ISP با استفاده از همان سیستم کابل کشی که برای تهیه تلویزیون کابل استفاده می‌شود نیز ممکن است. مودم‌های کابل می‌توانند ۵۰ مگابیت بر ثانیه و بالاتر از کابل کشی کواکسیال مورد استفاده برای تلویزیون کابل را فراهم کنند. مودم‌های کابل مطابق با استاندارد مشخصات واسط سرویس روی کابل Data-Over-Cable Service Interface Specification است.

دغدغه امنیتی و کارایی در مورد مودم‌های کابلی این است که هر مشتری در یک خط مشترک با همسایگان قرار دارد. این بدان معناست که عملکرد با زمان روز و تراکم و شلوغی متفاوت است و داده‌ها از طریق یک رسانه مشترک در حال انتقال هستند. به همین دلیل، بسیاری از شرکت‌های کابلی اکنون این انتقال‌ها را رمزگذاری می‌کنند.

کابل باند پهن Broadband به تازگی رایج شده است و به یک مودم کابلی در محل مشتری و یک سیستم پایانی Termination system کابل مودم در تأسیسات کابلی شرکت و به طور معمول به یک سر انتهای تلویزیون کابلی نیاز دارد. این دو از طریق کابل کواکسیال یا یک دستگاه فیبرنوری کواکسیال هیبریدی (HFC) hybrid fiber coaxial متصل می‌شوند. آنها به طور معمول می‌توانند تا ۱۶۰ کیلومتر بین مودم و سیستم پایانی کار کنند. نرخ بیت پایین دست برای مشتری متفاوت است اما به طور کلی در منطقه ۳۰۰ مگابیت در ثانیه و بالاتر اجرا می‌شود. ترافیک بالادست برای ارائه دهنده معمولاً فقط تا ۲۰ مگابیت بر ثانیه را تأمین می‌کند.

VPN

اتصالات شبکه خصوصی مجازی (VPN) Virtual private network اتصال است که از یک شبکه حامل غیرقابل اعتماد استفاده می‌کند اما حفاظت از اطلاعات را از طریق پروتکل‌های احراز هویت قوی و مکانیسم‌های رمزگذاری انجام می‌دهد. اگرچه ما معمولاً از غیرقابل اطمینان ترین شبکه، اینترنت به عنوان نمونه کلاسیک استفاده می‌کنیم، و بیشتر VPN‌ها از طریق اینترنت انتقال می‌یابد، اما در هر زمان که نیاز به محافظت از ترافیک از چشمان افراد کنجکاو باشد، می‌توان از آنها در شبکه‌های داخلی نیز استفاده کرد.

هنگام بحث در مورد اتصالات VPN، بسیاری از افراد تازه وارد به موضوع با تعداد و نوع پروتکل‌های درگیر سردرگم می‌شوند. در اینجا بهتر است که آنچه پروتکل‌های مورد نیاز، اختیار و نحوه اجرای همه آنها باهم را از هم تفکیک کرد. به خاطر دارید که روند کپسوله سازی چگونه کار می‌کند. این مفهوم را هنگامی که از ایجاد بسته‌ها صحبت شد، مورد بحث قرار دادیم و در آن زمینه این

کار را انجام دادیم که چگونه یک لایه از مدل " OSI پیچیده می شود " یا داده های دیگر را که قبلاً در لایه های دیگر ایجاد شده اند محصور می کند.

در عملیات VPN، کل پروتکل ها در اطراف پروتکل های دیگر پیچیده می شوند (فرآیندی به نام کپسوله سازی).

آنها شامل

- یک پروتکل لازم LAN
 - دسترسی از راه دور یا پروتکل خط (لازم) Remote access or line protocol
 - پروتکل احراز هویت (اختیاری) An authentication protocol
 - پروتکل رمزگذاری (اختیاری) An encryption protocol
- قبل از ارسال در سراسر VPN با بسته اصلی شروع می کنیم. یک بسته LAN، احتمالاً یک بسته TCP / IP است. تغییری که در این بسته ایجاد می شود این است که در یک پروتکل دسترسی از راه دور یا خط بسته بندی می شود. تنها وظیفه این پروتکل حمل بسته TCP / IP است که هنوز کاملاً دست نخورده روی خط است و دقیقاً مانند یک کشتی با بار اتومبیل می باشد که یک اتومبیل را در آن طرف یک رودخانه رها می کند، پس می توان گفت بسته اصلی را کپسوله می کند و آن را بدون تغییر در LAN به مقصد تحویل می دهد.

چندین پروتکل خط یا دسترسی از راه دور در دسترس هستند. از جمله آنها:

- پروتکل تونلینگ نقطه به نقطه (PPTP) Point-to-Point-Tunneling Protocol
 - پروتکل تونلینگ لایه ۲ (L2TP) Layer 2 Tunneling Protocol
- PPTP یک پروتکل میکروسافت مبتنی بر PPP است. از رمزگذاری داخلی P2P برای میکروسافت Microsoft Point-to-Point Encryption (MPPE) استفاده می کند و می تواند از چندین روش احراز هویت از جمله CHAP، MS-CHAP، EAP-TLS استفاده کند. یکی از نقاط ضعف PPTP این است که فقط در شبکه های مبتنی بر IP کار می کند. در صورت استفاده از اتصال WAN که مبتنی بر IP نیست، باید از L2TP استفاده شود.
- MS-CHAP در دو نسخه ارائه می شود. هر دو نسخه ممکن است مستعد حملات گذرواژه باشند. نسخه ۱ ذاتاً ناامن است و باید از آن اجتناب کرد. نسخه ۲ بسیار ایمن تر است اما هنوز هم می تواند حملات بی رحمانه Brute-force را روی گذرواژه متحمل شود، اگرچه چنین حملات معمولاً ۲۳ ساعت طول می کشد تا گذرواژه را بشکنند. علاوه بر این، MPPE استفاده شده با MS-CHAP می تواند نسبت به حملات بر روی الگوریتم RC4 که در آن مستقر است، مشکل ساز باشد.

اگرچه PPTP یک راه حل بهتر است، اما مشخص شده است که آسیب پذیری‌های شناخته شده مربوط به پروتکل‌های احراز هویت PPP دیگر توسط مایکروسافت توصیه نمی‌شود. اگرچه EAP-TLS از هر دو MS-CHAP و PPTP برتر است، اما استقرار آن نیاز به یک زیرساخت کلید عمومی (PKI) Public key infrastructure دارد، که اغلب در توانایی‌های فنی تیم شبکه نیست یا منابع برای حفظ آن در دسترس نیست.

L2TP یک پروتکل جدیدتر است که در لایه ۲ مدل OSI عمل می‌کند و می‌تواند از مکانیسم‌های مختلف احراز هویت مانند PPTP استفاده کند اما هیچ رمزگذاری را ارائه نمی‌دهد. معمولاً از IPsec که مکانیسم رمزگذاری بسیار قوی می‌باشد، استفاده می‌کند. با استفاده از PPTP، رمزگذاری گنجانده شده، و همچنین تنها انتخاب باقیمانده از آن باید پروتکل احراز هویت باشد. این پروتکل‌های احراز هویت بعداً در بخش "پروتکل‌های احراز هویت از راه دور" مورد بحث قرار می‌گیرند.

با L2TP، در صورت تمایل هر دو پروتکل رمزگذاری و احراز هویت، باید اضافه شوند. IPsec می‌تواند رمزگذاری، یکپارچگی داده‌ها و تأیید هویت مبتنی بر سیستم را ارائه دهد، که این امر آن را به گزینه‌ای انعطاف پذیر و توانمند تبدیل می‌کند. با پیاده سازی قسمت‌های خاصی از مجموعه IPsec می‌توان از این ویژگی‌ها استفاده کرد یا استفاده نکرد.

IPsec در واقع مجموعه‌ای از پروتکل‌ها به همان روش TCP / IP است که شامل اجزای زیر است: ✓ هدر احراز هویت (Authentication Header (AH): یکپارچگی داده‌ها، تأیید هویت مبدا داده و محافظت از حملات پخش مجدد را فراهم می‌کند.

✓ ظرفیت امنیت کپسوله سازی: Encapsulating Security Payload (ESP) تمام آنچه را که AH انجام می‌دهد و همچنین محرمانه بودن اطلاعات را ارائه می‌دهد.

✓ انجمن امنیت اینترنت و پروتکل مدیریت کلید

Internet Security Association and Key Management Protocol (ISAKMP) مسئولیت ایجاد انجمن امنیتی برای جلسه و تبادل کلید را بر عهده دارد.

✓ تبادل کلید اینترنتی (Internet Key Exchange (IKE): که گاهی اوقات به عنوان

تبادل کلید IPsec نیز یاد می‌شود: اساس احراز هویت مورد استفاده برای ایجاد کلیدهای رد و بدل شده توسط ISAKMP را در حین احراز هویت همسان خود فراهم می‌کند. پیشنهاد شده که توسط پروتکلی به نام اوکلی انجام شود که به الگوریتم Diffie-Hellman تکیه داشته باشد، اما اوکلی توسط IKE جانشین شده است.

IPsec یک چارچوب می باشد، به این معنی که بسیاری از مؤلفه های مورد استفاده با آن را مشخص نمی کند. این مؤلفه ها باید در پیکربندی مشخص شوند و برای ایجاد امنیت موفقیت آمیز لازم است و قبل از اینکه انتقال هر داده وجود داشته باشد، باید برای دو انتها تطابق داشته باشند. انتخاب هایی که باید انجام شود عبارتند از:

- الگوریتم رمزگذاری (رمزگذاری داده ها)
- الگوریتم هشینگ (تضمین می کند که داده ها تغییر نکرده و منشأ آن را تأیید می کنند)
- حالت (تونل یا انتقال)
- پروتکل (AH، ESP یا هر دو)

همه این تنظیمات باید در هر دو انتهای اتصال مطابقت داشته باشند. برای سیستم ها امکان انتخاب این موارد در حرکت وجود ندارد. همچنین باید به طور صحیح از پیش تنظیم شوند تا مطابقت داشته باشند.

در صورت پیکربندی در حالت تونل، تونل فقط بین دو دروازه Gateway وجود دارد، و تمام ترافیکی که از طریق تونل عبور می کند محافظت می شود. به طور معمول برای محافظت از ترافیک بین دو دفترکار استفاده می شود. انجمن امنیتی (SA) Security association میان دروازه های بین دفاترکار قرار دارد. می توان گفت این نوع اتصال است که می تواند VPN سایت به سایت نامگذاری شود.

SA بین دو نقطه پایانی از شاخص پارامتر امنیتی (SPI) Security parameter index و ترکیب AH / ESP تشکیل شده است. SPI، مقدار موجود در هر هدر IPsec که به دستگاهها کمک می کند تا رابطه بین هر SA (که یکباره چندین اتفاق می افتد) و پارامترهای امنیتی (که به آن Transform Set یا مجموعه تبدیل نیز گفته می شود) برقرار کند. هر جلسه یک مقدار جلسه منحصر به فرد دارد که به جلوگیری از موارد زیر کمک می کند:

- مهندسی معکوس Reverse engineering
- اصلاح محتوا Content modification
- حمله فاکتور سازی Factoring attacks (مهاجم سعی می کند تمام رمزهای عددی را

که می توان با الگوریتم برای رمزگشایی متن رمزگذاری استفاده کند، امتحان کند) با توجه به تأیید صحت اتصال، کلیدها می توانند از قبل به اشتراک گذاشته شده یا از PKI گرفته شوند. PKI یک جفت کلید عمومی یا خصوصی ایجاد می کند که با کاربران و رایانه هایی که از یک گواهی استفاده می کنند در ارتباط باشد. این جفت های کلیدی در جای کلیدهای از قبل به

اشتراک گذاشته شده در آن حالت استفاده می‌شوند. همچنین می‌توان از گواهینامه‌هایی استفاده کرد که از PKI حاصل نمی‌شوند.

در حالت انتقال، SA بین دو ایستگاه انتهایی یا یک ایستگاه انتهایی و یک دروازه یا سرور دسترسی از راه دور است. در این حالت، تونل از رایانه به رایانه یا از رایانه به دروازه توسعه می‌یابد. این نوع ارتباط می‌تواند برای VPN با دسترسی از راه دور باشد و همچنین فقط یکی از اپلیکیشن‌های IPsec باشد. در سایر اپلیکیشن‌ها مانند سرویس رادیویی بسته عمومی General Packet Radio Service (GPRS)، یک راه حل VPN برای دستگاه‌هایی که از یک شبکه تلفن همراه 2G یا 3G استفاده می‌کنند، می‌باشد.

وقتی ارتباط از دروازه به دروازه یا میزبان تا دروازه باشد، می‌توان از حالت انتقال یا تونل استفاده کرد. اگر ارتباط از طریق رایانه به رایانه باشد، تونل باید در حالت انتقال باشد. اگر تونل در حالت انتقال از دروازه به میزبان پیکربندی شده باشد، دروازه باید به عنوان میزبان عمل کند. مؤثرترین حمله علیه IPsec VPN، حمله‌ی Man-in-the-Middle است. در این حمله، مهاجم از مرحله مذاکرات امنیتی پیش می‌رود و زمانی که قربانی هویت خود را فاش کرد، مذاکره اصلی انجام شود. در یک سیستم که به خوبی پیاده سازی شده، وقتی مهاجمی نتواند هویت خود را اثبات کند باعث شکست مهاجم می‌شود.

TACACS + و RADIUS

هنگامی که کاربران از طریق مکانیسم‌های مختلفی به شبکه متصل می‌شوند، ابتدا باید احراز هویت شوند. این کاربران می‌توانند به شبکه دسترسی پیدا کنند از طریق:

- شماره گیری Dial-up سرورهای دسترسی از راه دور
- سرورهای دسترسی VPN
- نقاط دسترسی بی سیم
- سوئیچ‌های دارای امنیت

در هر زمان هر یک از این دستگاه‌های دسترسی، فرآیند احراز هویت را به صورت محلی در دستگاه انجام می‌دهند. ادمین‌ها باید اطمینان حاصل کنند که همه سیاست‌ها و تنظیمات دسترسی از راه دور در همه سازگار است. وقتی یک گذرواژه نیاز به تغییر دارد، باید در همه دستگاه‌ها انجام شود.

Remote Authentication Dial-In سرویس کاربری شماره گیری در احراز هویت از راه دور Service User (RADIUS) و سیستم کنترل دسترسی ناظر دسترسی ترمینال ثانویه Terminal Access Controller AccessControl System Plus (TACACS +) پروتکل های شبکه ای هستند که احراز هویت و مجوز متمرکز را ارائه می دهند. این سرویس ها می توانند در یک مکان مرکزی اجرا شوند و کلیه دستگاه های دسترسی (AP، دسترسی از راه دور، VPN و غیره) می توانند مشتری های سرور باشند. هر زمان که احراز هویت انجام شود، سرور TACACS + یا RADIUS عملیات احراز هویت و مجوز را انجام می دهد، و یک مکان را برای مدیریت سیاست های دسترسی از راه دور و گذرواژه ها را برای شبکه فراهم می کند. یکی دیگر از مزایای استفاده از این سیستم ها این است که اطلاعات ممیزی و دسترسی اطلاعات (logs) در سرور دسترسی نگهداری نمی شوند.

TACACS + و TACACS خدمات اختصاصی هستند که در دستگاه های سیسکو کار می کنند، در حالی که RADIUS یک استاندارد تعریف شده در RFC 2138 است. سیسکو در طول زمان چندین نسخه از TACACS را پیاده سازی کرده است. از TACACS به XTACACS و سپس آخرین نسخه، TACACS + می باشد. آخرین نسخه TACACS + احراز هویت، حسابداری، مجوز (Authentication, Accounting, Authorization) را ارائه می دهد، به همین دلیل است که گاهی به آن سرویس AAA نیز گفته می شود.

TACACS + از توکن هایی برای تأیید هویت گذرواژه دو عاملی و پویا استفاده می کند. همچنین به کاربران امکان تغییر گذرواژه های خود را می دهد.

RADIUS به منظور ارائه چارچوبی است که شامل سه مولفه می باشد. خواهان دستگاهی است که به دنبال احراز هویت می باشد. دستگاه تأیید کننده (Authenticator) در تلاش برای اتصال به آنها (AP، سوئیچ، سرور دسترسی از راه دور) هستند و سرور RADIUS سرور احراز هویت می باشد. با توجه به RADIUS، دستگاه مورد نظر برای ورود مشتری RADIUS نیست. سرور احراز هویت، سرور RADIUS بوده و تأیید کننده (AP، سوئیچ، سرور دسترسی از راه دور) مشتری RADIUS است.

در بعضی موارد، یک سرور RADIUS می تواند مشتری یک سرور دیگر RADIUS باشد. در این حالت، سرور RADIUS به عنوان پروکسی مشتری برای مشتریان RADIUS عمل می کند.

قطر Diameter، پروتکل احراز هویت دیگری است که براساس RADIUS ساخته شده و با RADIUS سازگار نیست. قطر مجموعه ای بسیار بزرگتر از جفت های ویژگی / صفت (AVP)

نسبت به RADIUS دارد که امکان ارتباط و قابلیت‌های بیشتر را فراهم می‌کند، اما به طور گسترده مورد استفاده قرار نگرفته است.

پروتکل‌های احراز هویت از راه دور Remote Authentication Protocols

پیشتر گفتیم که یکی از گزینه‌های پروتکل که هنگام تهیه راه حل دسترسی از راه دور باید انجام شود پروتکل احراز هویت است. در این بخش برخی از مهمترین پروتکل‌ها مورد بحث قرار می‌گیرد:

- پروتکل احراز هویت گذرواژه Password Authentication Protocol (PAP): احراز هویت را ارائه می‌دهد اما مدارک معتبر به صورت جداگانه ارسال می‌شوند و با یک اسنیفر قابل خواندن هستند.
- پروتکل احراز هویت دست دادن با چالش

:Challenge Handshake Authentication Protocol (CHAP)

با عملیاتی کردن بدون ارسال اعتبارنامه به سراسر لینک، مشکل متن واضح Cleartext را حل می‌کند. سرور مجموعه‌ای از متون تصادفی به نام چالش Challenge را برای مشتری ارسال می‌کند. مشتری متن را با گذرواژه رمزگذاری می‌کند و دوباره آن را ارسال می‌کند. سپس سرور آن را با همان گذرواژه رمزگشایی می‌کند و نتیجه را با آنچه در ابتدا ارسال شده است مقایسه می‌کند. اگر نتایج مطابقت داشته باشد، می‌توان اطمینان داد که کاربر یا سیستم دارای گذرواژه صحیح است و نیازی به ارسال آن در شبکه غیرقابل اعتماد Untrusted Network نیست.

- پروتکل احراز هویت گسترده Extensible Authentication Protocol (EAP):
- یک پروتکل منفرد نیست بلکه چارچوبی برای کنترل دسترسی مبتنی بر پورت است که از سه مؤلفه Component مشابه استفاده شده در RADIUS استفاده می‌کند. طیف گسترده‌ای از این پیاده سازی‌ها می‌توانند از انواع مکانیسم‌های احراز هویت، از جمله گواهینامه ها، PKI یا حتی گذرواژه‌های ساده استفاده کنند.

Telnet

Telnet یک پروتکل دسترسی از راه دور است که برای اتصال به یک دستگاه به منظور اجرای دستورات روی آن دستگاه استفاده می‌شود. برای دسترسی به سرورها، روترها، سوئیچ‌ها و بسیاری

از دستگاه‌های دیگر به منظور مدیریت آنها می‌توان از آن استفاده کرد. Telnet یک پروتکل مدیریت از راه دور مطمئن محسوب نمی‌شود زیرا مانند پروتکل دیگری که با سیستم‌های مبتنی بر UNIX، rlogin کار می‌کند، تمام اطلاعات از جمله فرآیند احراز هویت را به صورت واضح انتقال می‌دهد. گزینه‌های دیگری همچون SSH برای انجام همان عملکرد در حالی که رمزنگاری می‌شوند، اتخاذ شده است.

اتصالات Telnet و rlogin اتصال گرا Connection-oriented هستند بنابراین از TCP به عنوان پروتکل انتقال استفاده می‌کنند.

ورود به سیستم از راه دور، پوسته از راه دور، کپی از راه دور

:(Remote Log-in (rlogin), Remote Shell (rsh), Remote Copy (rcp))

خانواده پروتکل‌های rlogin / rsh / rcp به کاربران امکان می‌دهد از راه دور متصل شوند، دستورات را اجرا کنند و داده‌ها را در رایانه‌های مبتنی بر UNIX کپی کنند. احراز هویت بر اساس آدرس میزبان یا IP صورت می‌گیرد. اگر سازمانی نیاز به اجازه دسترسی داشته باشد، SSHv2 باید با این پروتکل‌ها پیاده سازی شود.

:Transport Layer Security / Secure Sockets Layer (TLS / SSL)

امنیت لایه انتقال TLS / لایه سوکت ایمن SSL گزینه دیگری برای ایجاد اتصالات امن به سرورها است. در لایه کاربردی مدل OSI کار می‌کند و عمدتاً برای محافظت از ترافیک HTTP یا سرورهای وب استفاده می‌شود. عملکرد آن در اکثر مرورگرها تعبیه شده است، و استفاده از آن به طور معمول نیازی به اقدامی از طرف کاربر ندارد. همچنین برای تضمین معاملات اینترنتی به صورت گسترده مورد استفاده قرار می‌گیرد. این کار به دو روش قابل اجرا است:

- SSL portal VPN: کاربر یک اتصال SSL واحد دارد که برای دسترسی به چندین سرویس در وب سرور استفاده می‌شود. پس از احراز هویت، صفحه‌ای در اختیار کاربر قرار می‌گیرد که بعنوان پورتال سایر سرویس‌ها عمل می‌کند.
- SSL tunnel VPN: کاربران برای دسترسی به خدمات روی سروری که وب سرور نیست از تونل SSL استفاده می‌کنند. یک SSL tunnel VPN از برنامه نویسی اختصاصی برای دسترسی به خدمات غیر وب از طریق یک مرورگر وب استفاده می‌کند.

TLS و SSL بسیار مشابه هستند اما باید توجه داشت که یکسان نیستند. TLS 1.0 و ورژن بالاتر بر اساس مشخصات SSL 3.0 است اما از نظر عملیاتی سازگار نیستند. هر دو محرمانه بودن، احراز هویت و یکپارچگی را بالاتر از لایه انتقال پیاده سازی می کنند. سرور همیشه احراز هویت می شود و به صورت اختیاری مشتری نیز می تواند باشد. SSL v2 باید برای احراز هویت در سمت مشتری استفاده شود. هنگام پیکربندی SSL، باید طول کلید جلسه مشخص شود که دو گزینه ۴۰ بیتی و ۱۲۸ بیتی می باشد. با استفاده از گواهی های خود امضا شده برای تصدیق کلید عمومی سرور، مانع از حمله Man-in-the Middle می شود.

VPN زداینده صفحه نمایش (Scraper Screen VPN)

اپلیکیشنی است که به یک مهاجم اجازه می دهد آنچه را که در صفحه نمایش کاربر قرار دارد ضبط کند. مهاجمان می توانند از Scraper Screen استفاده کنند تا اعتبار کاربر، توالی PIN، داده اختصاصی یا محرمانه و سایر اطلاعات نمایش داده شده را بدست آورند.

دسکتاپ / اپلیکیشن مجازی Virtual Application/Desktop

در حالی که مجازی سازی به طور فزاینده ای رایج شده است، سازمان ها همیشه امنیت کانال های ارتباطی مورد استفاده اپلیکیشن های مجازی سازی را در نظر نمی گیرند. با استفاده از مجازی سازی، کاربران از راه دور قادرند دستورات دسکتاپ را به گونه ای اجرا کنند که گویی در رایانه مجازی که به آنها متصل هستند، نشسته اند. متخصصان امنیت باید در مورد تمام گزینه های اپلیکیشن مجازی تحقیق کنند تا مطمئن شوند که اپلیکیشن انتخاب شده تمام قابلیت های مورد نیاز را در اختیار سازمان قرار می دهد و در عین حال تضمین کند که راه حل انتخاب شده سطح امنیت مناسبی را ارائه می دهد. هنگام استفاده از مجازی سازی، متخصصان امنیت باید مطمئن شوند که همان اقدامات امنیتی که بر روی رایانه میزبان انجام می شود، در هر دستگاه مجازی نیز اجرا می شود. به عنوان مثال، نرم افزار آنتی ویروس باید روی رایانه میزبان و بر روی هر دستگاه مجازی که روی رایانه کار می کند، نصب شود.

ارتباط از راه دور Telecommuting

سازمانها ناچارند محیط های کاری خود را تطبیق دهند تا نیازهای روزافزون دنیای پیشرفت تکنولوژی را برآورده سازند. امروزه بسیاری از سازمان ها در جذب استعداد لازم برای پر کردن

جایگاه‌های موجود، مشکل دارند. در نتیجه، ارتباط از راه دور یا کار از راه دور بطور فزاینده‌ای برای کمک به استخدام و اطمینان از اشتغال کارمندان ماهر مورد استفاده قرار می‌گیرد. سازمانها باید مطمئن شوند که کارکنان از راه دور Remote workers، کاملاً در تمام سیاستهای امنیتی، به ویژه سیاستهای مربوط به دسترسی VPN و دسترسی و ذخیره اطلاعات محرمانه، کاملاً آموزش دیده اند. همچنین پیشنهاد می‌شود قابلیت پاک کردن از راه دور و رمزگذاری کامل در هر دستگاه مختص سازمان پیاده سازی شود. در نهایت، کاربران باید پیامدهای دسترسی به منابع سازمانی را از اماکن عمومی درک کنند.

شبکه‌های مجازی Virtualized Networks

در تأمین امنیت شبکه‌های ارتباطی، سازمان‌ها باید تأثیرات شبکه‌های مجازی بر امنیت را درک کنند. در این بخش SDN، VSAN، سیستم عامل‌های مهمان و تفکیک پورت را بررسی می‌کنیم.

شبکه تعریف شده نرم افزاری (SDN) Software-defined networking

شبکه تعریف شده نرم افزاری (SDN) استقرار و تحویل نرم افزار را تسريع می‌کند، بدین ترتیب هزینه‌های فناوری اطلاعات را از طریق اتوماسیون گردش کار با فعال بودن سیاست کاهش می‌دهد و همچنین معماری‌های ابری را بوسیله ارائه خودکار و تحویل اپلیکیشن در صورت تقاضا و پویایی در مقیاس، فعال می‌کند.

SDN امکان تفکیک فیزیکی صفحه کنترل شبکه از صفحه انتقال را می‌دهد و صفحه کنترل می‌تواند چندین دستگاه را کنترل کند. بنابراین، ادمین‌ها می‌توانند ترافیک شبکه سنتی، سیمی و بی سیم را به سه مؤلفه جدا کنند: داده‌های خام، روش انتقال و قصد داده‌ها. SDN شامل سه لایه معماری می‌باشد:

- ✓ لایه زیرساخت Infrastructure layer: شامل سوئیچ‌ها، روترها و داده‌ها و فرآیند انتقال اطلاعات است. همچنین به آن سطح داده (Data plane) نیز گفته می‌شود.
- ✓ لایه کنترل Control layer: شامل هوشمندی دستگاهی است که جریان ترافیک را تعیین می‌کند و به آن سطح کنترل (Control plane) نیز گفته می‌شود.
- ✓ لایه کاربردی Application layer: شامل خدمات شبکه، برنامه‌ها و اپلیکیشن‌ها است. به آن سطح کاربردی (Application plane) نیز گفته می‌شود.

به خاطر این لایه ها، سخت افزاری که ترافیک شبکه را کنترل می‌کند، نیازی به هدایت ترافیک ندارد.

SDN ممکن است با اجازه دادن به آنها به علت کارآمدتر شدن، قابل اعتماد تر شدن و ساده تر شدن، از لحاظ ابری و مجازی سازی بسیار مفید باشد.

شبکه منطقه ذخیره سازی مجازی (VSAN) Virtual storage area network

شبکه منطقه ذخیره سازی مجازی (VSAN) یک روش ذخیره سازی تعریف شده نرم افزاری است که امکان جمع آوری ظرفیت‌های ذخیره سازی و تهیه سریع و شرط خودکار کردن ماشین ذخیره سازی مجازی را فراهم می‌آورد. درواقع یک روش نرم افزاری تعریف شده ذخیره سازی Software-defined storage (SDS) است. معمولاً شامل لایه بندی پویا، QoS، کشینگ، تکثیر Replication و همسان سازی Cloning است. در دسترس بودن داده‌ها از طریق نرم افزار تضمین می‌شود، و باید توجه داشت که با پیاده سازی سخت افزار اضافی تضمین نمی‌شود. ادمین‌ها قادر به تعیین سیاست هایی هستند که به نرم افزار اجازه می‌دهد تا بهترین جایگاه داده‌ها را تعیین کنند. با استفاده از قراردادن اطلاعات هوشمند و کنترلرهای مبتنی بر نرم افزار و نرم افزار RAID، یک VSAN می‌تواند حفاظت و در دسترس بودن داده‌های بهتری را نسبت به گزینه فقط سخت افزار سنتی داشته باشد.

سیستم عامل‌های مهمان Guest Operating Systems

اگر یک سازمان شبکه‌های مجازی را پیاده سازی کند، در برخی مواقع دسترسی به سیستم عامل‌های مهمان امکان پذیر است. در این مرحله، بهترین گزینه پیکربندی یک VLAN خصوصی (PVLAN) است که فقط برای دسترسی به سیستم مهمان می‌باشد. اولین PVLAN ایجاد شده PVLAN اصلی است و می‌تواند شامل بسیاری از PVLAN‌های ثانویه باشد. یک PVLAN ثانویه می‌تواند در حالت اعلان Promiscuous، حالت ایزوله (عایق) Isolated یا حالت عمومی Community تنظیم شود. بسته به نوع استفاده، نودهای درون یک PVLAN حالت محدودیت‌های ارتباطی خواهند داشت. استفاده از PVLAN به عنوان پورت ایزوله (عایق) Port Isolation نیز شناخته می‌شود.

حملات شبکه Network Attacks

قبل از اینکه بتوانید تهدیدات امنیتی شبکه را برطرف کنید، باید از آنها آگاه بوده، نحوه عملکرد آنها را درک کرده و اقدامات لازم برای جلوگیری از موفقیت حملات را بدانید. در این بخش طیف گسترده‌ای از انواع حمله به همراه اقدامات لازم برای جلوگیری از وقوع آنها پوشش داده می‌شود.

کابل کشی Cabling

اگرچه استراق سمع در یک شبکه کابلی آسانتر از یک شبکه بی سیم است، اما هنوز هم باید از برخی مسائل امنیتی آگاهی داشته باشید. همچنین باید برخی از رفتارهای کلی کابل کشی را که بر عملکرد تأثیر گذاشته و در نهایت هم می‌تواند بر در دسترس بودن تأثیر بگذارد، را درک کنید. همانطور که به خاطر دارید، حفظ دسترسی به شبکه نیز یکی از اهداف CIA است. بنابراین، ویژگی‌های عملکرد کابل کشی که می‌تواند بر در دسترس بودن تأثیر بگذارد که قبلاً بحث شده است.

نویز Noise

اصطلاحی است که برای پوشش چندین نوع تداخل Interference از آن استفاده می‌شود تا بتوان به کابل معرفی کرد که باعث ایجاد مشکل می‌شود. نویز می‌تواند از موتورهای الکتریکی بزرگ، رایانه‌های دیگر، روشنایی و منابع دیگر باشد. نویز با سیگنال‌های داده (بسته‌ها) در خط ترکیب شده و باعث اعوجاج (Distortion) سیگنال می‌شود. هنگامی که حتی یک بیت در یک انتقال منتقل می‌شود (به عنوان مثال ۱ خوانده می‌شود که باید ۰ خوانده شود یا برعکس)، داده‌های پوچ دریافت می‌شود و باید مجدداً ارسال شود. انتقال مجدد منجر به پایین آمدن توان و در برخی موارد موجب توان عملیاتی صفر می‌شود.

در هر حالتی که این مسئله به مشکل تبدیل شود، ساده ترین راه برای کاهش مشکل استفاده از حفاظ کابل کشی Shielded Cabling است. در مواردی که هنوز هم نویز وجود دارد، یافتن منبع خاص و اقدامات لازم برای حذف آن (حداقل تداخل ایجاد شده) از محیط ممکن است لازم باشد.

تضعیف Attenuation

تضعیف، ضعیف شدن سیگنال در هنگام عبور از کابل و مقاومت در برابر آن می‌باشد. در بحث در مورد کابل کشی در اوایل این فصل، آموختیم که تمام کابل‌ها دارای حداکثر طول توصیه شده هستند. هنگامی که از کابلی استفاده می‌شود که از طول توصیه شده آن طولانی تر است، تضعیف باعث ضعیف شدن سیگنال می‌شود تا نتوان آن را به درستی خواند و در نتیجه همان مشکلی حاصل می‌شود که نتیجه نویز می‌باشد. داده‌ها باید دوباره با پایین آمدن توان ارسال شود. راه حل این مشکل در طراحی است. توصیه‌های طول ذکر شده را در بخش مربوط به کابل‌ها در ابتدای این فصل با هر نوع کابل کشی دنبال کنید، که شامل کواکسیال، زوج بهم پیچ خورده و فیبر نوری است. انواع مختلف دارای حداکثر طول هستند بدون ریسک تضعیف، که نباید از آن طول تجاوز کند.

شکاف متقاطع Crosstalk

رفتاری است که می‌تواند هر زمان که سیم‌های تکی در یک کابل به موازات یکدیگر اجرا شوند، رخ می‌دهد. Crosstalk زمانی رخ می‌دهد که سیگنال‌های دو سیم (یا بیشتر) با یکدیگر تداخل داشته و باعث اعوجاج (Distortion) انتقال می‌شود. کابل‌هایی مانند کابل‌های زوج بهم پیچ خورده اگر مانند یکدیگر پیچیده نشوند از این مسئله رنج می‌برند. پیچ خوردگی مانع از وقوع شکاف متقاطع می‌شود.

استراق سمع Eavesdropping

اگرچه کابل کشی یک رسانه محدود و امن تر از بی سیم است، اما هنوز هم امکان استراق سمع وجود دارد. کلیه کابل کشی که به ولتاژهای الکتریکی بستگی دارد، از جمله کواکسیال و زوج بهم پیچ خورده، می‌توان با تجهیزات مناسب از آن بهره برداری کرد. کمترین حساسیت به استراق سمع (اگرچه کاملاً مصون نیست) کابل کشی فیبر نوری است زیرا از ولتاژ الکتریکی استفاده نمی‌کند، بلکه به صورت امواج نور است. در هر شرایطی که استراق سمع نگران کننده باشد، استفاده از کابل کشی فیبر نوری می‌تواند اقدامی باشد که حداقل به سختی، مشکل استراق سمع را افزایش دهد. راه حل واقعی تضمین امنیت فیزیکی کابل کشی است. کابل‌های اجرایی نباید در فضای باز و در دسترس باشند.

حملات مؤلفه شبکه Network Component Attacks

اجزای شبکه اغلب اهداف (Targets) حمله می‌باشند زیرا بسیاری از سازمان‌ها از همان دستگاه‌ها استفاده می‌کنند. متخصصان امنیت باید حملات علیه این دستگاه‌ها را درک کنند، از جمله کلاهبرداری غیر جعلی (Non-blind spoofing)، کلاهبرداری جعلی (Blind spoofing)، حملات (Man-in-the-Middle)، حملات سیل و طغیان 802.1 Q، MAC، حملات برچسب زدن پروتکل پیوند بین سوئیچ (Inter-Switch Link protocol tagging attacks)، حملات دوبل VLAN 802.1q / nest کیسوله شده می‌باشند.

کلاهبرداری غیر جعلی Non-Blind Spoofing

هنگامی اتفاق می‌افتد که مهاجمی در همان زیر شبکه قربانی قرار داشته باشد. این حمله تعداد دنباله‌ها و شماره‌های تأیید را Sniff کرده (گوش کند) و از آنها برای ربودن جلسه استفاده می‌کند. برای جلوگیری از این حملات، متخصصان امنیت ممکن است بخواهند اقدامات زیر را در نظر بگیرند:

- استفاده از فیلتر ورودی روی بسته‌ها برای فیلتر کردن ترافیک ورودی
- بکارگیری پروتکل‌ها از طریق یک دنباله عددی که برای ایجاد اتصال امن به سیستم‌های دیگر استفاده می‌شود.
- پیکربندی شبکه برای رد کردن بسته‌های شبکه که ادعا می‌کنند از یک آدرس محلی منشا گرفته اند.
- فعال کردن جلسات رمزگذاری در روتر در صورت امکان اتصال به خارج از میزبان‌های قابل اعتماد

کلاهبرداری جعلی Blind Spoofing

دنباله و شماره‌های تأیید را نمی‌توان بدست آورد. بسته‌ها برای بدست آوردن نمونه گیری از اعداد دنباله به هدف ارسال می‌شوند تا مهاجم بتواند عدد دنباله معتبر برای حمله ایجاد کند. معمولاً در سیستم‌های قدیمی بهتر کار می‌کند زیرا از یک فرمول دقیق برای تعیین اعداد دنباله‌ای استفاده می‌کنند. با این حال، بسیاری از سیستم عامل‌های مدرن امروز از تولید شماره دنباله تصادفی استفاده می‌کنند.

کاهش موارد ذکر شده در مورد Non-Blind Spoofing، در مورد حملات Blind Spoofing نیز اعمال می‌شود.

حمله انسان در وسط Man-in-the-Middle Attack

این نوع حمله ترافیک قانونی بین دو نهاد را متوقف می‌کند. مهاجم می‌تواند جریان اطلاعات را کنترل کند و می‌تواند ارتباط بین دو طرف را از بین ببرد یا تغییر دهد. هر دو کلاهبرداری جعلی و غیر جعلی از انواع حملات انسان در وسط Man-in-the-Middle (MITM) هستند. برخی از حملات MITM با رمزگذاری پیام‌ها می‌توانند کاهش یابد. سایر دفاع‌ها شامل استفاده از پسوندهای امن DNS، PKI، احراز هویت دوطرفه قوی تر و تأیید کانال امن ثانویه است.

حمله سیل MAC (MAC Flooding Attack)

از آنجا که سوئیچ‌ها و پلها (bridge) از نظر تعداد ورودی‌هایی که می‌توانند در جدول MAC وجود داشته باشد محدود است، مهاجمین می‌توانند چنین وسیله‌ای را با استفاده از ترافیک، سیلاب کنند تا دستگاه را به یک شبه هاب تبدیل کنند، از این طریق اطمینان حاصل می‌شود که مهاجم می‌تواند تمام ترافیک روی دستگاه را گوش کند. استفاده از امنیت پورت، 802.1X برابر و VLAN‌های پویا می‌توانند به جلوگیری از این حمله کمک کنند. حمله برچسب زدن (تگ زدن) پروتکل پیوند بین سوئیچ و 802.1Q

802.1Q and Inter-Switch Link protocol tagging attack

برچسب زدن یا همان تگ زدن حملات وقتی انجام می‌شود که کاربر در VLAN به صورت غیر مجاز به VLAN دیگری دسترسی پیدا کند. جلوگیری از این نوع حمله معمولاً شامل تنظیم پروتکل Dynamic Trunking Protocol (DTP) برای خاموش کردن همه پورت‌های غیر معتبر یا پیروی از دستورالعمل‌های پیکربندی ساده برای سوئیچ است.

Double-Encapsulated 802.1Q / Nested VLAN Attack

در یک حمله دوبل 802.1Q / nested VLAN کپسوله شده، یک مهاجم می‌تواند با تزریق بسته‌هایی که در یک 802.1Q VLAN تگ شده اند، باعث ایجاد ترافیک در هاب VLAN‌ها شود. می‌توان با پاک کردن VLAN محلی از همه بدنه 802.1Q یا انتخاب VLAN بلااستفاده به عنوان VLAN محلی جلوگیری کرد.

حمله ARP

در یک VLAN، از حملات مسمومیت ARP برای فریب روترها برای یادگیری هویت دستگاههای جعلی استفاده می شود. سپس مهاجم بجای آن وسیله قرار می گیرد و یک حمله MITM را انجام می دهد.

پیشگیری از این حمله به بهترین وجه با مسدود کردن ارتباط مستقیم در لایه ۲ بین دستگاه حمله کننده و دستگاه مورد حمله یا با استفاده از بازرسی ARP یا برخی مکانیسم مشابه در دستگاهها انجام می شود.

حملات ICMP

در اوایل این فصل با پروتکل پیام کنترل اینترنت (ICMP)، یکی از پروتکل های موجود در مجموعه TCP / IP آشنا شدید. این پروتکل توسط دستگاهها برای ارسال پیام های خطا به دستگاههای ارسال کننده هنگام بروز مشکلات انتقال استفاده می شود و همچنین در هنگام استفاده از دستور پینگ یا دستور Traceroute برای عیب یابی از دستگاهها استفاده می شود. مانند بسیاری از ابزارها و ابزارهای کاربردی (Tools , Utilities) که برای اهداف مناسب ایجاد شده اند، این پروتکل همچنین می تواند توسط مهاجمی که از عملکرد آن استفاده می کنند، بکار گرفته شود.

این قسمت حملات مبتنی بر ICMP را پوشش می دهد. یکی از راه های جلوگیری از حملات مبتنی بر ICMP، مجاز نبودن استفاده از آن با مسدود کردن شماره پروتکل برای ICMP است، که عدد ۱ می باشد. بسیاری از محصولات فایروال همچنین این امکان را دارند که فقط انواع خاصی از پیام های ICMP را مسدود کنند در حالی که مخالف ممنوع کردن استفاده کامل آن نیز نیستند. در این بخش برخی از انواع پیام ICMP مشکل ساز مورد بحث قرار می گیرد.

• پینگ مرگ Ping of Death

پینگ مرگ حمله ای است که از رفتار عادی دستگاه هایی که بسته های بزرگ ICMP دریافت می کنند، بهره می گیرد. بسته های ICMP معمولاً طول ۶۵۵۳۶ بایت قابلیت پیش بینی دارند. هرکس آموخته اند که چگونه داده های اضافی را در بسته های ICMP وارد کنند. یک حمله پینگ مرگ چندین مورد از این بسته های بزرگ را می فرستد، که می تواند باعث شود سیستم قربانی در کمترین حالت ناپایدار (Unstable) و احتمالاً منجمد (Freeze) قرار گیرد. این امر باعث انکار

سرویس (Denial-of-Service) می شود زیرا باعث می شود سیستم هدف قادر به انجام عملکرد عادی خود در شبکه نباشد.

• حمله Smurf

یک حمله انکار سرویس است که از نوعی بسته پینگ به نام درخواست اکو ICMP ECHO REQUEST (ICMP) استفاده می کند. این نمونه ای از حمله انکار سرویس توزیع شده Distributed Denial-of-Service (DDoS) است که در آن عامل مرتکب جنایت فهرست سایر دستگاه های موجود در شبکه قرار می گیرد.

هنگامی که یک سیستم یک بسته ICMP ECHO REQUEST را دریافت می کند، سعی می کند با یک بسته ICMP ECHO REPLY (معمولاً به طور پیش فرض چهار بار) به این درخواست پاسخ دهد. به طور معمول این پاسخ به سیستم ارسال کننده منفرد ارسال می شود. در این حمله، درخواست اکو ECHO REQUEST آدرس مقصد خود را بر روی آدرس پخش شبکه Network broadcast address در شبکه ای که در آن سیستم هدف ساکن است تنظیم کرده و آدرس منبع روی سیستم هدف تنظیم می شود. هنگامی که هر سیستم در شبکه به درخواست پاسخ می دهد بر دستگاه مورد نظر غلبه کرده و باعث Freeze یا خرابی آن می شود.

• Fraggle

اگرچه واقعاً یک حمله ICMP نیست زیرا از UDP استفاده می کند، اما حمله Fraggle از نوع حمله DDoS با همان هدف و روش مشابه حمله Smurf است. در این حمله یک مهاجم مقدار زیادی ترافیک اکو UDP را به یک آدرس پخش IP ارسال می کند، همه اینها دارای یک آدرس منبع جعلی است که سیستم هدف خواهد بود. هنگامی که تمام سیستم های شبکه پاسخ می دهند، بر هدف غلبه می کند.

• تغییر مسیر ICMP (ICMP Redirect)

یکی از انواع مختلفی از پیام های خطایی که از ICMP استفاده می کند، یک تغییر مسیر ICMP یا نوع ۵ بسته ICMP نامیده می شود. از تغییر مسیر ICMP توسط روترها برای تعیین مسیریابی بهتر مسیرها در یک شبکه استفاده می شود. وقتی این کار را انجام داد، مسیری را که بسته می گیرد تغییر می دهد.

مهاجم با ساخت بسته های تغییر مسیر ICMP، جدول مسیر میزبان را که پیام تغییر مسیر Redirect message دریافت می کند تغییر می دهد. این شیوه، روت کردن بسته ها در شبکه را به نفع وی تغییر می دهد و پس از تغییر جدول مسیریابی آن، میزبان ۱۰ دقیقه به استفاده از مسیر ادامه می دهد. به همین دلیل، بسته های تغییر مسیر ICMP ممکن است یکی از انواعی باشند که ممکن است شما تمایلی به اجازه در فایروال نداشته باشید.

• Ping Scanning

از ICMP می توان برای اسکن شبکه برای آدرس های IP زنده live یا فعال Active استفاده کرد. این حمله اساساً هر آدرس IP را پینگ می کند و پیگیری می کند که آدرس های IP به پینگ پاسخ دهند. این حمله معمولاً همراه با اسکن پورت انجام می شود که بعداً در این فصل پوشش داده می شود.

بهره برداری از ردیابی مسیر Traceroute Exploitation

برای تعیین مسیری که یک بسته بین یک مبدا و مقصد حرکت می کند، استفاده می شود. مهاجمان برای درک بهتر مسیریابی بسته ها می توانند از ردیابی مسیر برای نقشه برداری شبکه استفاده کنند. آنها همچنین می توانند برای تعیین قوانین فایروال از ردیابی مسیر با Nmap استفاده کنند.

حملات DNS

DNS نام رایانه و دامنه را در آدرس های IP قرار می دهد. این یک سرویس حیاتی برای شبکه است و به همین دلیل چندین سرور DNS همیشه برای تحمل خطا توصیه می شوند. سرورهای DNS به دلیل پایین بودن ضرب و شتم آنها، مورد علاقه حملات DoS و DDoS است. سرورهای DNS همچنین با تغییر سوابق DNS می توانند برای هدایت ترافیک، مورد استفاده مهاجم قرار گیرند. در این بخش به انواع حملات DNS همراه با روش های پوشش داده شده، که می تواند اثر این حملات را از بین ببرد یا کاهش دهد، می پردازیم.

• مسمومیت حافظه کش DNS (DNS Cache Poisoning)

مشتریان DNS درخواست هایی را برای تفکیک آدرس اسم به IP به نام (Query)، به سرور DNS ارسال می کنند. جستجوی آدرس IP که با یک رایانه یا نام دامنه انجام می شود، معمولاً با یک سرور محلی DNS آغاز می شود که برای دامنه DNS که رایانه یا وب سایت درخواستی در آن قرار دارد، معتبر نیست. هنگامی که این اتفاق می افتد، سرور DNS محلی درخواستی از سرور DNS را انجام می دهد که سوابق مورد نظر را در اختیار دارد. بعد از دریافت سرور DNS محلی، آن را به مشتری DNS محلی باز می گرداند. پس از این، سرور محلی DNS این سابقه را در حافظه کش DNS خود برای مدت زمانی به نام Time to Live (TTL) حفظ می کند، که معمولاً یک ساعت می باشد اما می تواند متفاوت باشد.

در حمله مسمومیت کش DNS، مهاجم سعی می کند با ضبط آدرس متفاوت از آدرس صحیح، آن رکورد را Refresh یا به روز کند. اگر او بتواند سرور DNS را متقاعد کند که این Refresh را بپذیرد، سرور DNS محلی با آدرس وارد شده توسط مهاجم، به درخواست های مشتری برای آن رایانه پاسخ می دهد. معمولاً آدرسی که اکنون دریافت می کند مربوط به وب سایت جعلی است و به نظر می رسد مانند سایتی که مشتری درخواست می کند، می باشد. سپس هکر می تواند تمام ترکیبات نام و گذرواژه را از سایت جعلی خود برداشت کند.

برای جلوگیری از این نوع حمله، سرورهای DNS باید در بروزرسانی هایی که قبول می کنند محدودیت ایجاد کند. در بیشتر نرم افزارهای DNS، می توانید سرورهای DNS را محدود کنید و فقط یک سرور بروزرسانی ها را بپذیرد. این امر می تواند مانع از پذیرش سرورهایی با این بروزرسانی های نادرست شود.

• DoS

سرورهای DNS مورد علاقه حملات انکار سرویس (Denial-of-service) (DoS) هستند. این امر به این دلیل است که از بین رفتن سرویس DNS در شبکه، شبکه را متوقف می کند زیرا بسیاری از خدمات شبکه به عملکرد آن بستگی دارد. هر یک از انواع مختلف حملات DoS که در این کتاب مورد بحث قرار گرفته است، می توانند برای سرورهای DNS هدفمند باشند. به عنوان مثال، پینگ مرگ Ping of Death ممکن است حمله انتخابی باشد.

• DDoS

هر یک از حملات DoS متنوع را می توان توسط مهاجم با جذب سایر دستگاه ها برای کمک به حمله تقویت کرد. برخی از نمونه های این حملات، حملات Fraggle،Smurf در بعضی موارد، ممکن است مهاجم از بدافزارها برای نصب نرم افزار بر روی هزاران رایانه (به نام زامبی) که به آنها دستورات در یک زمان معین ارسال می شود، استفاده کند و به همه دستگاه ها دستور دهد تا حمله را انجام دهند. این عمل نه تنها حمله را تقویت می کند بلکه به مخفی کردن مبدا حمله نیز کمک می کند زیرا به نظر می رسد به یکباره از بسیاری از مناطق آمده است.

• DNSSEC

یکی از رویکردهای جدید برای جلوگیری از حملات DNS، مکانیسم احراز هویت قوی تر نام دامنه پسوندهای امنیتی سیستم (DNSSEC) Domain Name System Security Extensions است. بسیاری از پیاده سازی های فعلی نرم افزار DNS حاوی این قابلیت است. از امضاهای دیجیتالی برای تأیید منبع همه پیامها استفاده می کند تا تضمین شود که حقه نیستند. مشکل با DNSSEC مبادله کلاسیک بین امنیت و سادگی را نشان می دهد. برای استقرار DNSSEC، باید یک PKI ساخته و نگهداری شود تا جفت های کلید عمومی / خصوصی و گواهی نامه ها برای همه سرورهای DNS صادر شده و اعتبار داشته باشد. علاوه بر این، برای امنیت کامل DNS، تمام سرورهای DNS در اینترنت نیز نیاز به مشارکت دارند، که این وضعیت را پیچیده تر می کند.

• مخفی سازی URL

یک روش جایگزین و به نوعی ساده تر برای مهاجم برای هدایت ترافیک به وب سایت جعلی روشی به نام مخفی سازی URL می باشد. این حمله از مزیت تعبیه کردن آدرس اینترنتی در صفحات وب و ایمیل استفاده می کند. ممکن است مهاجم در متن صفحه وب یا ایمیل نام صحیح وب سایت را ارجاع دهد، اما وقتی URL را که با پیوند همراه است وارد کند، URL به سایت جعلی وارد می شود. بهترین راه محافظت در برابر این مسئله این است که از کاربران بخواهید روی لینک ها در وب سایت های ناشناخته یا غیر قابل اعتماد کلیک نکنند.

• قاپیدن یا گرفتن دامنه Domain Grabbing

قاپیدن دامنه زمانی اتفاق می‌افتد که افراد قبل از اینکه شانس این کار را داشته باشند، نام دامنه یک شرکت مشهور را ثبت کنند. بعداً افراد نام آن را که گروگان گرفته اند نگه می‌دارند تا اینکه شرکت حاضر به پرداخت نام دامنه شود. در بعضی موارد، این افراد زمانهای تمدید را برای وبسایتهای شناخته شده رصد می‌کنند و قبل از اینکه شانس اجرای این تمدید شرکت را داشته باشد، نام آنها را ثبت می‌کنند. برخی از شیوه‌هایی که می‌تواند به جلوگیری از این امر کمک کند، ثبت نام دامنه برای مدت زمان طولانی‌تر و ثبت همه جایگشت‌های نام دامنه انتخاب شده (اشتباهات غلط و غیره) می‌باشد.

• مداخله مجازی Cybersquatting

هنگامی که نام دامنه‌ها، بدون هدف استفاده کردن از آنها ثبت شده است ولی با هدف نگه داشتن آنها به صورت گروگان (همانطور که در مورد قبل توضیح داده شد)، به آن مداخله مجازی می‌گویند. شیوه‌هایی که برای جلوگیری از قاپیدن دامنه می‌باشد برای جلوگیری کردن شرکت از قربانی شدن در مداخله مجازی نیز به کار می‌رود.

• حملات ایمیل Email Attacks

یکی از راه‌های رایج برای حملات، ابزاری است که همه ما باید هر روز از آن استفاده کنیم. در این بخش چندین حمله که از ایمیل به عنوان وسیله استفاده می‌شود، پوشانده شده است. در بیشتر موارد، بهترین راه برای جلوگیری از این حملات، آموزش و آگاهی کاربران می‌باشد زیرا بسیاری از این حملات مبتنی بر رویه‌های امنیتی ضعیف، از طرف کاربر می‌باشد.

✓ جعل ایمیل Email Spoofing

جعل ایمیل فرایند ارسال ایمیلی است که به نظر می‌رسد از منبعی تهیه می‌شود ولی واقعا از منبعی دیگر تهیه شده است. این کار با تغییر فیلدهای هدر ایمیل مانند "مسیر برگشت Return Path" و "پاسخ به Reply-to" امکان پذیر است. هدف آن متقاعد کردن گیرنده برای اعتماد به پیام و پاسخ دادن به آن با برخی از اطلاعات حساس است که گیرنده نمی‌تواند به اشتراک بگذارد مگر اینکه یک پیام قابل اعتماد باشد.

اغلب این یک مرحله در حمله است که برای برداشت نام کاربری و گذرواژه برای سایت های بانکی یا مالی طراحی شده است. این حمله می تواند از چند طریق کاهش یابد. یکی احراز هویت SMTP است، که در صورت فعال بودن، ارسال ایمیل توسط یک کاربر که نمی تواند سرور ارسال کننده را احراز هویت کند، مجاز نمی باشد.

یکی دیگر از روش های کاهش احتمالی، پیاده سازی یک چارچوب سیاست فرستنده Sender Policy Framework (SPF) است. SPF یک سیستم اعتبارسنجی ایمیل است که با استفاده از DNS کار می کند تا تشخیص دهد که آیا یک ایمیل ارسال شده بوسیله شخص همان میزبان می باشد که توسط ادمین آن دامنه معین شده است. در صورت عدم تأیید اعتبار، آن را به جعبه گیرنده تحویل نمی دهد.

✓ نیزه فیشینگ Spear Phishing

یک حمله مهندسی اجتماعی است که در آن، گیرنده اطمینان دارد و روی لینک در ایمیل کلیک می کند که به نظر می رسد به یک سایت قابل اعتماد می رود اما در واقع به سایت هکر می رود. این حمله برای برداشت نام کاربری و گذرواژه استفاده می شود. نیزه فیشینگ فرایند مسدود کردن این حمله به یک شخص خاص می باشد تا یک مجموعه تصادفی از افراد. این حمله ممکن است با آموختن جزئیات در مورد شخص از طریق رسانه های اجتماعی متقاعد کننده تر شود که ایمیل ممکن است برای تقویت ظاهر قانونی خود باشد.

✓ Whaling

درست همانطور که نیزه فیشینگ زیر مجموعه فیشینگ است، Whaling نیز زیر مجموعه ای از نیزه فیشینگ است. این حمله یک فرد را هدف قرار می دهد و در صورت Whaling، آن شخص کسی است که بسیار مهم می باشد. به عنوان مثال ممکن است یک مدیر عامل، CFO، CSO، COO یا CTO باشد. این حمله بر اساس این فرض استوار است که این افراد اطلاعات حساس تری برای افشا کردن دارند.

✓ هرزنامه ها Spam

هیچ کس از پر شدن صندوق های ایمیل هر روز با ایمیل های ناخواسته که معمولاً سعی می کنند چیزی را بفروش برسانند، لذت نمی برد. در بسیاری موارد، هنگام خرید چیزی یا بازدید از سایتی،

به این جزئیات توجه نمی‌شود. هنگامی که ایمیل به صورت انبوه ارسال می‌شود که درخواست نشده به آن هرزنامه گفته می‌شود.

هرزنامه بیشتر از یک آزار است زیرا می‌تواند جعبه‌های ایمیل را مسدود کرده و باعث شود سرورهای ایمیل برای مصرف شما منابع در اختیارشان قرار دهند. ارسال اسپم غیرقانونی است، بنابراین بسیاری از اسپم‌ها سعی می‌کنند با ارتباط برقرار کردن (رله شدن)، در سرورهای ایمیل شرکت‌های دیگر منبع اسپم را مخفی کنند. این عمل نه تنها منبع واقعی ایمیل را پنهان می‌کند، بلکه می‌تواند باعث شود شرکتی که ارتباط برقرار کرده یا در واقع رله شده را نیز دچار مشکل کند.

سرورهای ایمیل امروزی این توانایی را دارند که هر سرور ایمیلی که شما مشخص نکرده اید، را رد کنند. این عمل می‌تواند مانع از استفاده سیستم ایمیل شما به عنوان مکانیسم اسپم سازی شود. این نوع ارتباط مجدد باید روی سرورهای ایمیل شما مجاز نباشد. علاوه بر این، فیلترهای اسپم را می‌توان از طریق ایمیل شخصی، مانند سرویس گیرندگان ایمیل مبتنی بر وب پیاده سازی کرد.

• حملات بی سیم Wireless Attacks

جلوگیری از حملات بی سیم به دلیل اینکه محیط آن طبیعت می‌باشد، بسیار سخت است. اگر می‌خواهید انتقال رادیو را در اختیار کاربران قرار دهید، شما باید آنها را در دسترس هر کس دیگری در آن منطقه وجود دارد نیز قرار دهید. علاوه بر این، هیچ راهی برای تعیین اینکه چه کسی امواج رادیویی شما را ضبط می‌کند وجود ندارد! ممکن است بتوانید از اتصال کسی یا تبدیل شدن به مشتری بی سیم در شبکه جلوگیری کنید، اما نمی‌توانید آنها را از استفاده از یک اسنiffer (گوش کردن) بی سیم برای گرفتن بسته‌ها متوقف کنید. در این بخش، برخی از حملات متداول تحت پوشش قرار گرفته و برخی از روشهای کاهش نیز مورد بحث قرار می‌گیرد.

✓ Wardriving

فرآیند حرکت کردن اطراف یک دستگاه بی سیم متصل به آنتن با قدرت بالا است که در جستجوی WLANها است. این حمله می‌تواند به منظور دستیابی به اینترنت رایگان یا شناسایی شبکه‌های باز در معرض حمله باشد.

Warchalking ✓

روشی است که به طور معمول با Wardriving همکاری می کند. وقتی یک WLAN، Wardriving را پیدا می کند، وی را با علامت سفید در مسیر یا ساخت SSID و حروف امنیتی مورد استفاده در شبکه نشان می دهد. این فعالیت اکنون به صورت آنلاین انجام می شود زیرا بسیاری از سایتها به جمع آوری لیست WLAN های یافت شده و مکان آنها، اختصاص داده شده است.

✓ حملات از راه دور Remote Attacks

اگرچه به یک معنا همه حملات مانند حملات DoS، مسمومیت با DNS، اسکن پورت و حملات ICMP از طریق شبکه قابل اجرا هستند و از راه دور هستند، اما حملات از راه دور نیز می توانند روی سیستمهای دسترسی از راه دور مانند سرورهای VPN یا سرورهای شماره گیری قرار گیرند. با تحول روشهای امنیتی، این نوع حملات تا حدودی کاهش یافته است.

Wardialing تهدیدی نیست زیرا ما به اندازه گذشته از مودم و بانکهای مودم استفاده نمی کنیم. در این حمله، برنامه های نرم افزاری برای شناسایی شماره های متصل به مودمها تلاش می کنند تا لیستهای بزرگی از شماره تلفن ها را شماره گیری کنند. هنگامی که یک شخص یا دستگاه فکس پاسخ می دهد، آن عمل را ثبت می کند، و هنگامی که مودم پاسخ می دهد، سعی می کند اتصال برقرار کند. اگر این اتصال موفقیت آمیز باشد، اکنون هکر یک ورودی برای ورود به شبکه دارد.

حملات دیگر

در این بخش پایانی این فصل، حملات دیگری پوشش داده شده است که ممکن است در هیچ یک از دسته های دیگر که تاکنون مورد بحث قرار گرفته، نباشند.

SYN ACK Attack

حمله SYN ACK از دست دادن سه طرفه TCP بهره می برد، که در بخش "لایه انتقال" توضیح داده شده است. در این حمله، هکر تعداد زیادی بسته را با مجموعه پرچم SYN ارسال می کند، که باعث می شود رایانه گیرنده حافظه را برای هر بسته ACK که در انتظار دریافت آن است، تفکیک کند. این بسته ها هرگز به نتیجه نمی رسند و در بعضی مواقع منابع رایانه گیرنده را خسته کرده و باعث حمله ای از نوع DoS می شود.

ربودن جلسه Session Hijacking

در یک حمله ربودن جلسه، هکر تلاش می‌کند تا به منظور تصاحب جلسه یکی از دو رایانه، خود را در وسط یک گفتگوی فعال بین دو رایانه قرار دهد و بدین ترتیب تمام داده‌های ارسال شده به آن رایانه را دریافت می‌کند. Juggernaut و Hunt Project به مهاجمان اجازه می‌دهد تا از جلسه TCP بین رایانه‌ها جاسوسی کند. سپس او از نوعی حمله DoS برای حذف یکی از دو رایانه در شبکه در زمان جعل آدرس IP آن رایانه و جایگزینی با آن رایانه در گفتگو، استفاده می‌کند. این امر باعث می‌شود هکر تمام ترافیکی را که برای رایانه‌ای که مورد حمله DoS قرار گرفته است، دریافت کند.

اسکن پورت Port Scanning

همچنین می‌توان از ICMP برای اسکن شبکه برای پورت باز استفاده کرد. پورت‌های باز نشان می‌دهد سرویسی که در حال اجرا و گوش دادن به وسیله‌ای باشد، ممکن است مستعد حمله باشد. این حمله اساساً هر آدرس و شماره پورت را پینگ می‌کند و پیگیری می‌کند که کدام پورت‌ها روی هر دستگاه باز است زیرا به پینگ‌ها توسط پورت‌های باز با سرویس گوش دادن پاسخ داده می‌شود و به پورت‌های بسته پاسخ داده نمی‌شود.

NMAP یکی از رایج ترین ابزارهای اسکن پورت است که امروزه مورد استفاده قرار می‌گیرد. متخصصان امنیت باید اسکنهای NULL، FIN، XMAS را که توسط Nmap انجام می‌شود درک کنند. هر بسته‌ای که حاوی بیت‌های SYN، RST یا ACK نباشد، در صورت بسته بودن پورت، پاسخی را بر می‌گرداند. اگر پورت باز باشد، پاسخی ارسال نمی‌شود. اسکن NULL هیچ بیتی ارسال نمی‌کند. یک اسکن FIN بیت FIN را تنظیم می‌کند. اسکن XMAS پرچم‌های FIN، PSH، URG را تنظیم می‌کند. دو مزیت این نوع اسکن این است که می‌توانند از طریق فایروال‌های غیر دولتی و روترهای فیلتر بسته بندی، گشت و گذار کنند، و کم و بیش مخفی تر از اسکن SYN هستند.

Teardrop

نوعی حمله قطعه قطعه کننده Fragmentation است. واحد حداکثر انتقال Maximum Transmission Unit (MTU) یک بخش از شبکه ممکن است باعث شکسته شدن یا قطعه قطعه شدن بسته شود، که نیاز به جمع شدن قطعات در هنگام دریافت دارد. هکر قطعات ناقص بسته‌ها

را ارسال می کند که هنگام جمع شدن مجدد توسط گیرنده باعث خراب شدن یا ناپایدار شدن گیرنده می شود.

کلاهبرداری یا جعل آدرس IP Address Spoofing

کلاهبرداری یا جعل آدرس IP تکنیکی است که هکرها برای پنهان کردن ردپای خود یا به صورت نقاب بجای رایانه دیگر استفاده می کنند. هکر آدرس IP را همانطور که در بسته ظاهر می شود تغییر می دهد. ممکن است گاهی اوقات باعث شود، بسته بتواند از طریق ACL بر مبنای آدرس های IP باشد. همچنین می توان از آن برای برقراری ارتباط با سیستمی استفاده کرد، که فقط به آدرسهای خاص IP یا دامنه آدرسهای IP اعتماد دارند.

فصل ۵

هویت و مدیریت دسترسی
(Identity and Access Management)

این فصل موضوعات زیر را در بر می گیرد:

- ❖ فرآیند کنترل دسترسی Access Control Process : مفاهیم مورد بحث شامل مراحل رویه های کنترل دسترسی می باشد.
- ❖ دسترسی فیزیکی و منطقی به دارایی ها Physical and Logical Access to Assets: مفاهیم مورد بحث شامل مدیریت کنترل دسترسی، دسترسی به اطلاعات، دسترسی به سیستم ها، دسترسی به دستگاه و دسترسی به تاسیسات می باشد.
- ❖ مفاهیم شناسایی و احراز هویت Identification and Authentication Concepts : مفاهیم مورد بحث شامل عوامل دانش، عوامل مالکیت، عوامل ویژگی و عوامل زمان می باشد.
- ❖ شناسایی و اجرای احراز هویت Identification and Authentication Implementation: مفاهیم مورد بحث شامل تفکیک وظایف، حداقل امتیاز / نیاز به دانستن، پیش فرض عدم دسترسی، خدمات دایرکتوری، ورود یکپارچه، مدیریت جلسه، ثبت نام و اثبات هویت، سیستم های مدیریت اعتبار و پاسخگویی است.
- ❖ هویت به عنوان یک سرویس اجرا Identity as a Service (IDaaS) Implementation : هنگام اجرای IDaaS ملاحظات را توصیف می کند.
- ❖ پیاده سازی خدمات هویت شخص ثالث Third-Party Identity Services Implementation: جزئیات مربوط به ادغام سرویس های هویت شخص ثالث در یک شرکت.
- ❖ مکانیسم های مجوز Authorization Mechanisms : شامل مدل های کنترل دسترسی و سیاست های کنترل دسترسی می شود.
- ❖ تهدیدهای کنترل دسترسی Access Control Threats: مفاهیم مورد بحث شامل تهدیدهای گذرواژه، تهدیدهای مربوط به مهندسی اجتماعی، DoS / DDoS، سرریز بافر، کد سیار، نرم افزارهای مخرب، کلاهبرداری، Sniffing و استراق سمع، انتشار و Trapdoor / Backdoor است.
- ❖ جلوگیری یا کاهش تهدیدات کنترل دسترسی Prevent or Mitigate Access Control Threats: روشهای پیشگیری یا کاهش تهدیدهای کنترل دسترسی را توصیف می کند.

مدیریت هویت و دسترسی عمدتاً مربوط به کنترل دسترسی به دارایی‌ها و مدیریت هویت است. این دارایی‌ها شامل رایانه، تجهیزات، شبکه‌ها و اپلیکیشن‌ها است. متخصصان امنیت باید نحوه کنترل دسترسی فیزیکی و منطقی به دارایی‌ها و مدیریت سیستم‌های شناسایی، احراز هویت و مجوز را درک کنند. سرانجام، باید تهدیدات کنترل دسترسی مورد توجه قرار گیرد.

مدیریت هویت و دسترسی شامل چگونگی عملکرد مدیریت دسترسی، اهمیت هویت و مدیریت دسترسی (IAM) و چگونگی عملکرد مؤلفه‌ها و دستگاه‌های IAM در یک سازمان مهم است. کنترل دسترسی فقط به کاربران، اپلیکیشن‌ها، دستگاه‌ها و سیستم‌های مجاز اجازه می‌دهد تا از منابع و اطلاعات شرکت استفاده کنند. این کنترل دسترسی شامل تاسیسات، سیستم‌های پشتیبانی، سیستم‌های اطلاعاتی، دستگاه‌های شبکه و پرسنل است. متخصصان امنیت از کنترل دسترسی استفاده می‌کنند تا مشخص کنند که کاربران می‌توانند به یک منبع دسترسی داشته باشند و به کدام منابع دسترسی پیدا کنند، کدام عملیات ممکن است انجام شود و کدام اقدامات کنترل می‌شوند. بار دیگر، سه گانه CIA در ارائه IAM سازمانی از اهمیت برخوردار است.

فرآیند کنترل دسترسی Access Control Process

اگرچه بسیاری از رویکردها برای اجرای کنترل‌های دسترسی طراحی شده‌اند، اما کلیه رویکردها مراحل زیر را شامل می‌شوند:

- ۱- شناسایی منابع Identify resources .
- ۲- شناسایی کاربران Identify users .
- ۳- شناسایی روابط بین منابع و کاربران. Identify the relationships between the resources and users

• شناسایی منابع

مرحله اول در فرآیند کنترل دسترسی شامل تعریف همه منابع در زیرساخت فناوری اطلاعات با تصمیم‌گیری در مورد حمایت از موجودیت‌ها است. هنگام تعریف این منابع، باید نحوه دسترسی به منابع را نیز در نظر بگیرید. سوالات زیر می‌تواند به عنوان نقطه شروع در هنگام شناسایی منابع استفاده شود:

✓ آیا این اطلاعات توسط اعضای جامعه عمومی قابل دسترسی خواهد بود؟

✓ آیا دسترسی به این اطلاعات فقط به کارمندان محدود می شود؟

✓ آیا دسترسی به این اطلاعات باید به زیر مجموعه کوچکتر کارمندان محدود شود؟

به خاطر داشته باشید که داده ها، اپلیکیشن ها، سرویس ها، سرورها و دستگاه های شبکه، منابع در نظر گرفته می شوند. منابع هر دارایی سازمانی است که کاربران می توانند به آنها دسترسی پیدا کنند. در کنترل دسترسی، منابع اغلب به عنوان اشیاء objects نامگذاری می شوند.

• شناسایی کاربران

پس از شناسایی منابع، یک سازمان باید کاربرانی را که نیاز به دسترسی به منابع دارند شناسایی کند. یک متخصص امنیت معمولی باید چندین سطح کاربرانی را که نیاز به دسترسی به منابع سازمانی دارند، مدیریت کند. در طی این مرحله، فقط شناسایی کاربران مهم است. سطح دسترسی به این کاربران داده خواهد شد و در مرحله بعدی بیشتر مورد تجزیه و تحلیل قرار می گیرد. به عنوان بخشی از این مرحله، باید نیازهای کاربران را تجزیه و تحلیل و درک کرده و سپس اعتبار آن نیازها را در برابر نیازهای سازمانی، سیاست ها، مسائل حقوقی، حساسیت داده ها و ریسک اندازه گیری کرد.

به خاطر داشته باشید که هر استراتژی کنترل دسترسی و سیستم مستقر در پیاده سازی آن باید از پیچیدگی جلوگیری کند. هرچه سیستم کنترل دسترسی پیچیده تر باشد، مدیریت آن سیستم سخت تر است. علاوه بر این، پیش بینی مسائل امنیتی که می توانند در سیستم های پیچیده تر رخ دهند بسیار دشوار تر می باشد. به عنوان متخصصان امنیت، باید بین نیازهای کاربران و سیاست ها و نیازهای امنیتی سازمان تعادل برقرار کنیم. اگر مکانیسم امنیتی که ما آن را پیاده سازی می کنیم، مشکل زیادی را برای کاربر ایجاد کند، کاربر ممکن است درگیر کارهایی شود که مکانیسم هایی را که پیاده سازی شده را زیر پا بگذارد. به عنوان مثال، اگر یک سیاست گذرواژه را اجرا کنید که به یک گذرواژه بسیار طولانی و پیچیده احتیاج دارد، ممکن است کاربران به خاطر داشته باشند که گذرواژه های خود را سخت می کنند و کاربران پس از آن ممکن است گذرواژه های خود را بر روی یادداشت های چسبنده ای که به مانیتور یا صفحه کلید آنها چسبانده اند، بنویسند.

• شناسایی روابط بین منابع و کاربران

آخرین مرحله در فرآیند کنترل دسترسی، تعیین سطح کنترل دسترسی است که برای هر منبع و روابط بین منابع و کاربران باید وجود داشته باشد. به عنوان مثال، اگر یک سازمان وب سرور را به عنوان منبع تعریف کرده باشد، ممکن است کارمندان عمومی میزان دسترسی محدودتر به منابع نسبت به عموم و دسترسی محدودتر به منابع نسبت به کارمندان توسعه وب احتیاج داشته باشند. کنترل‌های دسترسی باید برای پشتیبانی از عملکرد کسب و کار منابعی که از آنها محافظت می‌شود، طراحی شوند. کنترل عملکردهایی که می‌توانند برای یک منبع خاص و بر اساس نقش کاربر انجام شوند، بسیار مهم است.

دسترسی فیزیکی و منطقی به دارایی Physical and Logical Access to Assets

کنترل دسترسی همه چیز در مورد استفاده از کنترل‌های فیزیکی یا منطقی برای کنترل افرادی است که به یک شبکه، سیستم یا دستگاه دسترسی دارند. همچنین شامل نوع دسترسی به شبکه، سیستم یا دستگاه می‌شوند. کنترل دسترسی در درجه اول با استفاده از کنترل‌های فیزیکی و منطقی ارائه می‌شود.

دسترسی فیزیکی بر کنترل دسترسی به شبکه، سیستم یا دستگاه متمرکز است. در بیشتر موارد، دسترسی فیزیکی شامل استفاده از کنترل دسترسی برای جلوگیری از امکان لمس کردن اجزای شبکه (از جمله سیم کشی)، سیستم‌ها یا دستگاه‌ها می‌باشد. در حالی که قفل‌ها رایج ترین روش کنترل دسترسی فیزیکی برای جلوگیری از دسترسی به دستگاه‌ها در یک مرکز داده است، باید با توجه به نیاز سازمان و ارزش دارایی مورد حمایت سازمان، سایر کنترل‌های فیزیکی مانند نگهبانان و سیستم بیومتریک نیز در نظر گرفته شود.

کنترل‌های منطقی دسترسی کاربر از طریق نرم افزار یا قطعات سخت افزاری را محدود می‌کند. احراز هویت و رمزگذاری نمونه هایی از کنترل‌های منطقی هستند.

در هنگام نصب سیستم کنترل دسترسی، متخصصان امنیت باید درک کنند که چه کسی نیاز به دسترسی به دارایی را دارد که محافظت می‌شود و چگونه کاربران دسترسی به دارایی دارند. وقتی چندین کاربر دسترسی به دارایی را نیاز دارند، سازمان باید یک سیستم کنترل دسترسی چند لایه را تنظیم کند. به عنوان مثال، کاربرانی که مایل به دسترسی به ساختمان هستند فقط ممکن است نیاز به ورود به سیستم داشته باشند. با این حال، برای دسترسی به مرکز داده (Data Center)

قفل شده در همان ساختمان، کاربران به کارت هوشمند نیاز دارند، هر دوی اینها کنترل دسترسی فیزیکی هستند. برای محافظت از داده ها روی یک سرور واحد در داخل ساختمان (اما نه در مرکز داده)، سازمان باید مکانیزم هایی مانند احراز هویت، رمزگذاری و لیست های کنترل دسترسی (ACL) را به عنوان کنترل دسترسی منطقی مستقر کند اما می تواند سرور را در یک اتاق سرور قفل شده قرار دهند تا بتواند کنترل دسترسی فیزیکی را ارائه دهد.

متخصصان امنیت هنگام استفاده از کنترل های دسترسی فیزیکی و منطقی، باید روش های کنترل دسترسی و دارایی های مختلفی که باید محافظت شوند و کنترل های دسترسی احتمالی آنها را بدانند.

مدیریت کنترل دسترسی Access Control Administration

مدیریت کنترل دسترسی در دو حالت اساسی صورت می گیرد: متمرکز و غیرمتمرکز.

• متمرکز Centralized

در کنترل دسترسی متمرکز، یک بخش مرکزی یا پرسنل، نظارت بر دسترسی به همه منابع سازمانی دارند. این روش مدیریت تضمین می کند که دسترسی کاربر به طور مداوم در کل شرکت کنترل می شود. با این وجود، این روش می تواند کند باشد زیرا کلیه درخواست های دسترسی توسط واحد مرکزی پردازش می شود.

• غیر متمرکز Decentralized

در کنترل دسترسی غیرمتمرکز، پرسنل نزدیک به منابع، مانند مدیران بخش و صاحبان داده، کنترل دسترسی را برای منابع فردی نظارت می کنند. این روش مدیریت تضمین می کند که افرادی که اطلاعات را می شناسند، حق دسترسی به آن را کنترل می کنند. با این وجود، مدیریت این روش دشوار است زیرا فقط یک نهاد مسئولیت پیکربندی حقوق دسترسی را ندارد و در نتیجه یکنواختی و عدالت امنیت را از دست می دهد.

برخی از شرکتها ممکن است رویکرد هیبریدی را اجرا کنند که هم کنترل دسترسی متمرکز و هم غیر متمرکز را شامل می شود. در این مدل استقرار، از مدیریت متمرکز برای دسترسی پایه ای استفاده می شود، اما دسترسی دانه ای (Granular Access) به دارایی های فردی، مانند داده های روی سرور دپارتمان، توسط صاحب داده اداره می شود.

ارائه چرخه عمر Provisioning Life Cycle

سازمانها باید یک فرآیند رسمی برای ایجاد، تغییر و از بین بردن کاربران ایجاد کنند، که همان چرخه حیات است. این فرایند شامل تأیید کاربر، ایجاد کاربر، استانداردهای ایجاد کاربر و مجوز است. کاربران باید بیانیه کتبی امضا کنند که در آن شرایط دسترسی، از جمله مسئولیت‌های کاربر توضیح داده شود. سرانجام، روشهای دسترسی و حذف باید مستندسازی شوند. سیاست‌های تأمین کننده کاربر باید به عنوان بخشی از مدیریت منابع انسانی یکپارچه شود. سیاست‌های منابع انسانی باید رویه‌هایی را شامل شود که اداره منابع انسانی بطور رسمی خواهان ایجاد یا حذف حساب کاربری در هنگام استخدام یا خاتمه کارکنان جدید باشد.

اطلاعات Information

برای محافظت کامل از اطلاعاتی که در شبکه، سرورها یا سایر دستگاههای سازمان ذخیره می‌شود، متخصصان امنیت باید کنترل دسترسی فیزیکی و منطقی را ارائه دهند. کنترل‌های دسترسی فیزیکی، مانند قرار دادن وسایل در یک اتاق قفل شده که از دستگاه‌هایی که اطلاعات در آن قرار دارد محافظت می‌شود. کنترل‌های دسترسی منطقی مانند استقرار داده‌ها یا رمزگذاری درایو، رمزگذاری انتقال، ACLها و دیواره آتش، داده‌ها را از دسترسی غیر مجاز محافظت می‌کنند. ارزش اطلاعاتی که محافظت می‌شود احتمالاً کنترل‌هایی را که یک سازمان مایل به استقرار است تعیین می‌کند. به عنوان مثال، مکاتبات منظم در رایانه مشتری احتمالاً به کنترل‌های مشابه داده‌های مالی ذخیره شده در سرور احتیاج ندارند. برای رایانه مشتری، سازمان ممکن است به سادگی یک فایروال نرم افزار محلی و مجوزهای ACL مناسب را در پوشه‌ها (folders) و فایل‌های محلی مستقر کند. برای سرور، سازمان ممکن است نیاز به انجام اقدامات پیچیده تر، از جمله رمزگذاری درایو، رمزگذاری انتقال، ACLها و سایر اقدامات داشته باشد.

سیستم‌ها Systems

برای محافظت کامل از سیستم‌های مورد استفاده سازمان، از جمله رایانه‌های مشتری و سرور، متخصصان امنیت ممکن است به کنترل‌های دسترسی فیزیکی و منطقی اعتماد کنند. با این حال، برخی از سیستم‌ها، مانند رایانه‌های مشتری، ممکن است بگونه‌ای مستقر شوند که فقط از حداقل کنترل‌های فیزیکی استفاده کنند. اگر کاربر به یک ساختمان دسترسی پیدا کند، ممکن

است از رایانه‌های مشتری در اتاقکهای غیر امن در کل ساختمان استفاده کند. برای این سیستم ها، یک متخصص امنیت باید از استقرار مکانیسم‌های مناسب احراز هویت اطمینان حاصل کند. اگر اطلاعات محرمانه در رایانه‌های مشتری ذخیره شود، باید رمزگذاری نیز صورت گیرد. اما تنها سازمان می‌تواند به بهترین وجه تعیین کند که کنترل‌ها برای مستقر شدن در رایانه‌های مشتری خاص چگونه باشد.

هنگام مراجعه به سرورها، تعیین اینکه کدام کنترل دسترسی برای استقرار می‌باشد معمولاً روش پیچیده تری است. متخصصان امنیت برای تعیین ارزش دارایی و حفاظت مورد نیاز باید با صاحب سرور، خواه رئیس بخش یا متخصص IT همکاری کنند. البته بیشتر سرورها باید در یک اتاق قفل شده قرار گیرند که در بسیاری موارد، یک مرکز داده یا اتاق سرور خواهد بود. با این حال، سرورها در صورت لزوم می‌توانند در دفاتر کار قفل شده و مستقر شوند. بعلاوه، برای اطمینان از کامل بودن سیستم، باید سایر کنترل‌ها مستقر شوند. نیازهای کنترل دسترسی یک فایل سرور با نیازهای وب سرور یا سرور پایگاه داده متفاوت است. بسیار مهم است که سازمان قبل از تعیین اینکه کدام کنترل‌های دستیابی را برای استقرار انجام دهد، ارزیابی کاملی از داده‌های پردازش شده و ذخیره شده در سیستم انجام دهد. اگر منابع محدودی در دسترس باشد، متخصصان امنیت باید مطمئن شوند که مهمترین سیستم‌های آنها دارای کنترل دسترسی بیشتری نسبت به سایر سیستم‌ها هستند.

دستگاه‌ها Devices

مانند سیستم ها، قرار دادن دستگاه‌ها در یک اتاق امن، دسترسی فیزیکی به دستگاه‌ها بهتر است. دسترسی منطقی به دستگاه‌ها با اجرای لیست مناسب ACL یا قوانین، احراز هویت و رمزگذاری و همچنین امنیت هرگونه واسطه از راه دور که برای مدیریت دستگاه استفاده می‌شود فراهم می‌شود. علاوه بر این، متخصصان امنیت باید از تغییر یا غیرفعال کردن حساب‌های پیش فرض و غیرفعال بودن دستگاه اطمینان حاصل کنند.

برای هر متخصص IT که نیاز دسترسی به دستگاه دارد، باید یک حساب کاربری برای سطح حرفه‌ای با سطح مناسب دسترسی لازم تنظیم شود. در صورت استفاده از واسطه از راه دور، حتماً رمزگذاری مانند SSL را فعال کنید تا اطمینان حاصل شود که ارتباط از طریق واسطه از راه دور رهگیری و خوانده نمی‌شود. متخصصان امنیت باید اعلان‌های مربوط به فروشنده برای هر دستگاه

را از نزدیک کنترل کنند تا تضمین شود که دستگاه‌ها با جدیدترین نسخه‌های امنیتی و بروزرسانی‌های سیستم عامل به روز شده‌اند.

تأسیسات Facilities

در مورد تأسیسات، دغدغه اصلی دسترسی فیزیکی است که می‌توان با استفاده از قفل، نرده کشی، تابلوها، نگهبان و تلویزیون مدار بسته (دوربین مدار بسته CCTV) تهیه کرد. بسیاری از سازمان‌ها فکر می‌کنند که چنین اقداماتی کافی است. اما با وجود سیستم‌های پیشرفته کنترلی صنعتی و اینترنت اشیا (IoT)، سازمانها باید دستگاههای درگیر در امنیت تأسیسات را نیز در نظر بگیرند. اگر یک سازمان دارای سیستم زنگ خطر / امنیت باشد، که امکان دسترسی از راه دور را از طریق اینترنت مشاهده می‌کند، باید کنترل‌های منطقی مناسبی در نظر گرفته شود تا از دسترسی کاربر مخرب به سیستم و تغییر تنظیمات آن یا استفاده از سیستم برای دستیابی به اطلاعات داخلی در مورد سیستم، طرح تأسیسات و عملیات روزانه، جلوگیری شود. اگر سازمان از سیستم کنترل صنعتی (ICS) Industrial Control System استفاده می‌کند، کنترل‌های منطقی نیز باید در اولویت باشند. متخصصان امنیت باید با سازمانها همکاری کنند تا مطمئن شوند که کنترل‌های فیزیکی و منطقی به درستی انجام می‌شود تا از کل تأسیسات محافظت شود.

مفاهیم شناسایی و احراز هویت Identification and Authentication Concepts

برای دسترسی به یک منبع، یک کاربر باید هویت خود را تصدیق کند، مدارک لازم را ارائه دهد و از حق لازم برای انجام کارهایی که در حال انجام است برخوردار باشد. اولین قدم در این فرآیند، شناسایی Identification نامیده می‌شود، که فعالیت یک کاربر است که هویت یک سیستم کنترل دسترسی را دارد.

احراز هویت Authentication، دومین بخش از فرآیند، اقدام به اعتبارسنجی کاربر با شناسه منحصر به فرد، از طریق تهیه اعتبارنامه مناسب است. هنگام تلاش برای تفکیک بین این دو، متخصصان امنیت باید بدانند که شناسایی، کاربر را شناسایی می‌کند و احراز هویت تأیید می‌کند که هویت ارائه شده توسط کاربر معتبر است. احراز هویت معمولاً از طریق گذرواژه کاربر ارائه شده در ورود به سیستم انجام می‌شود. هنگامی که کاربر به سیستم وارد می‌شود، پس از اینکه کاربر تمام داده‌های ورودی را وارد کرد، مراحل ورود وی باید ورود به سیستم را تأیید کند.

پس از احراز هویت کاربر باید به کاربران، حقوق و مجوزهایی برای منابع داده شود. این پروسه با عنوان مجوز Authorization خوانده می شود. رایجترین شکل شناسایی کاربر شامل شناسه کاربر یا حساب کاربری، شماره حساب و شماره شناسایی شخصی (PINs) Personal identification numbers است.

پنج عامل احراز هویت

پس از تعیین روش شناسایی کاربر، یک سازمان باید تصمیم بگیرد که از کدام روش احراز هویت استفاده کند.

روش احراز هویت به پنج دسته گسترده تقسیم می شود:

✓ احراز هویت عامل دانش Knowledge factor authentication: چیزی که فرد می داند.

✓ احراز هویت عامل مالکیت Ownership factor authentication: چیزی که یک شخص مالک آن است یا در اختیار دارد.

✓ احراز هویت عامل ویژگی Characteristic factor authentication: چیزی که برای یک شخص است.

✓ احراز هویت عامل موقعیت مکانی Location factor authentication: در جایی که شخصی قرار دارد.

✓ احراز هویت عامل زمان Time factor authentication: زمان احراز هویت شخص است. احراز هویت معمولاً تضمین می کند که کاربر حداقل یک عامل را از این دسته ها ارائه می دهد، که به آن احراز هویت تک عاملی گفته می شود. نمونه ای از این امر می تواند نام کاربری و گذرواژه باشد که هنگام ورود به سیستم وارد می کند. احراز هویت دو عاملی تضمین می کند که کاربر دو عامل از پنج عامل را ارائه می دهد. نمونه ای از احراز هویت دو عاملی ارائه نام کاربری، گذرواژه و کارت هوشمند برای ورود می باشد. تأیید هویت سه عاملی تضمین می کند که کاربر سه عامل را ارائه می دهد. نمونه ای از تأیید هویت سه عاملی می تواند نام کاربری، گذرواژه، کارت هوشمند و اثر انگشت در هنگام ورود به سیستم باشد. برای اینکه احراز هویت به عنوان هویت قوی در نظر گرفته شود، کاربر باید حداقل دو دسته مختلف از عوامل را ارائه دهد. (توجه داشته باشید که نام کاربری عامل شناسایی است، نه یک عامل احراز هویت.)

توجه داشته باشید

در اصل سه عامل وجود داشت (چیزی که می‌دانید، چیزی را که دارید و چیزی که هستید). که به ترتیب عامل‌های نوع اول و نوع دوم و نوع سوم در نظر گرفته شدند. با این وجود، فناوری مدرن زمینه امنیتی را مجبور کرده است که اخیراً دو عامل دیگر را بشناسید: جایی که در آن هستید و زمان احراز هویت.

باید درک کنید که ارائه عامل‌های احراز هویت چندگانه از همان دسته، هنوز تصدیق تک عاملی در نظر گرفته می‌شود. به عنوان مثال، اگر یک کاربر نام کاربری، گذرواژه و نام خانوادگی مادر کاربر Mother's maiden name را در اختیار شما قرار دهد، از احراز هویت تک عاملی استفاده می‌شود. در این مثال، کاربر هنوز تنها عواملی را ارائه می‌دهد که چیزی است که یک شخص از آن می‌داند.

عوامل دانش Knowledge Factors

همانطور که در بخش قبل به اختصار توضیح داده شد، احراز هویت عامل دانش، احراز هویتی است که براساس چیزی که فرد می‌داند ارائه می‌شود. اگرچه رایجترین شکل احراز هویت مورد استفاده توسط این دسته، احراز هویت گذرواژه است، از سایر دانش‌ها می‌توان از جمله تاریخ تولد، نام خانوادگی مادر، ترکیب کلید یا PIN استفاده کرد.

هویت و مدیریت حساب Identity and Account Management

هویت و مدیریت حساب برای هر فرآیند احراز هویت حیاتی است. به عنوان یک متخصص امنیت، باید مطمئن شوید که سازمانتان رویه رسمی برای کنترل ایجاد و تخصیص اعتبارنامه یا هویت دسترسی را کنترل می‌کند. اگر مجوز ایجاد حساب‌های نامعتبر وجود داشته باشد و غیرفعال نشود، نقض امنیتی رخ می‌دهد. اکثر سازمانها روشی را برای بررسی روند شناسایی و احراز هویت به منظور اطمینان از جاری بودن حسابهای کاربری پیاده سازی می‌کنند. سؤالاتی که احتمالاً در این فرآیند کمک می‌کنند عبارتند از:

- آیا لیست فعلی کاربران مجاز و دسترسی آنها حفظ و تصویب شده است؟
- آیا در صورت لزوم گذرواژه‌ها حداقل هر ۹۰ روز یا زودتر تغییر می‌کنند؟
- آیا حسابهای غیرفعال کاربر پس از مدت زمانی مشخص غیرفعال می‌شوند؟

هر روش مدیریت هویت باید فرآیندهای ایجاد (تأمین Provisioning)، تغییر و نظارت (بررسی Reviewing) و حذف کاربران از سیستم کنترل دسترسی (ابطال Revoking) را شامل شود. به این چرخه عمر تأمین کننده گفته می شود. هنگام ایجاد یک حساب کاربری، کاربران جدید موظفند شناسه معتبر عکس را ارائه دهند و باید بیانیهای را در مورد محرمانه بودن گذرواژه امضا کنند. حسابهای کاربری باید منحصر به فرد باشند و باید سیاست هایی در نظر گرفته شود که ساختار حسابهای کاربری را استاندارد کند. به عنوان مثال، تمام حسابهای کاربر باید Firstname یا Lastname یا ساختار دیگری باشند که تضمین می کند، کاربران درون یک سازمان می توانند شناسایی کاربر جدید را، عمدتاً برای اهداف ارتباطی، تعیین کنند.

پس از ایجاد، باید حسابهای کاربر کنترل شود تا از فعال بودن آنها اطمینان حاصل شود. حسابهای غیرفعال باید بطور خودکار پس از مدت معینی از عدم فعالیت براساس نیازهای کسب و کار غیرفعال شوند.

علاوه بر این، هر سیاست پایانی باید شامل مراحل رسمی باشد تا تضمین شود که همه حسابهای کاربر غیرفعال یا حذف شده اند. عناصر مدیریت صحیح حساب شامل موارد زیر است:

- ایجاد یک فرآیند رسمی برای ایجاد، صدور و بستن حسابهای کاربری.
- بطور دوره ای بررسی کردن حساب های کاربر.
- فرایندی را برای ردیابی مجوز دسترسی پیاده سازی شود.
- بطور دوره ای، پرسنل در موقعیت های حساس قرار گیرند.
- بطور دوره ای تأیید شدن مشروعیت حساب های کاربر.

بررسی حساب کاربری یک بخش حیاتی از مدیریت حساب است. حسابهای کاربری باید بر اساس تطابق با اصل حداقل امتیاز بررسی شود. بررسیهای حساب کاربر می تواند به صورت سازمانی، سیستم گسترده یا مبتنی بر اپلیکیشن به اپلیکیشن انجام شود. اندازه سازمان تا چه اندازه از این روش ها استفاده می کند. به عنوان بخشی از بررسی حساب کاربری، سازمانها باید مشخص کنند که آیا همه حسابهای کاربری فعال هستند یا خیر.

انواع گذرواژه و مدیریت آن Password Types and Management

همانطور که قبلاً ذکر شد، احراز هویت گذر واژه رایجترین احراز هویت است که امروزه به کار گرفته شده است. با این حال، انواع گذرواژه می توانند از سیستمی به سیستم دیگر متفاوت باشند. دانستن انواع گذرواژه ها قابل استفاده بسیار حیاتی است.

انواع گذرواژه‌ها که باید با آنها آشنا شوید عبارتند از:

✓ *Standard word or simple passwords* کلمات استاندارد یا گذرواژه‌های ساده

همانطور که از نام آن پیداست، این گذرواژه از کلمات منفرد تشکیل شده اند که غالباً ترکیبی از حروف و اعداد بزرگ و کوچک را شامل می‌شوند. مزیت این نوع گذرواژه این است که به راحتی می‌توان آن را بخاطر آورد. یک نقطه ضعف از این نوع گذرواژه این است که برای حمله یا شکستن مهاجمان آسان است و در نتیجه یک حساب به خطر افتاده ایجاد می‌شود.

✓ *Combination passwords* گذرواژه‌های ترکیبی

کلمات فرهنگ لغت، معمولاً از دو کلمه غیر مرتبط استفاده می‌کند. به اینها گذرواژه‌های فرمولی *Composition Passwords* نیز گفته می‌شود. مانند گذرواژه‌های استاندارد، آنها می‌توانند حروف و اعداد بزرگ و کوچک را شامل شوند. مزیت این گذرواژه این است که شکستن آن از گذرواژه ساده دشوارتر است و نقطه ضعف آن اینگونه است که به خاطر سپردن آن دشوار می‌باشد.

✓ *Static passwords* گذرواژه‌های ایستا

این نوع گذرواژه حداقل امنیت را ایجاد می‌کند زیرا گذرواژه هرگز تغییر نمی‌کند. این گذرواژه اغلب در شبکه‌های *Peer-to-Peer* مشاهده می‌گردد.

✓ *Complex passwords* گذرواژه‌های پیچیده

این نوع گذرواژه کاربر را مجبور می‌کند تا مخلوطی از حروف بزرگ، کوچک و حروف، اعداد و کاراکترهای خاص را درج کند. امروزه برای بسیاری از سازمان‌ها، این نوع گذرواژه را به عنوان بخشی از سیاست گذرواژه سازمان اعمال می‌کنند. مزیت این نوع گذرواژه این است که شکستن آن بسیار سخت است. یک نقطه ضعف این است که به خاطر سپردن آن سخت تر است و وارد کردن صحیح آن از گذرواژه‌های استاندارد یا ترکیبی معمولاً بسیار سخت تر می‌باشد.

✓ *Passphrase passwords* گذرواژه‌های عبارات عبور

این نوع گذرواژه نیاز به استفاده از یک عبارت طولانی دارد. به دلیل طول گذرواژه، به خاطر سپردن راحت تر اما حمله آن بسیار سخت تر است که هر دو مزیت مسلم هستند. با درج حروف بزرگ، حروف کوچک، اعداد و کاراکترهای ویژه در این نوع گذرواژه می‌توان امنیت احراز هویت را به میزان قابل توجهی افزایش داد.

✓ *Cognitive passwords* گذرواژه‌های شناختی. این نوع گذرواژه بخشی از اطلاعات است که برای احراز هویت فرد قابل استفاده است. این اطلاعات با پاسخ دادن به یک سری سؤالات مبتنی بر زندگی کاربر، مانند رنگ مورد علاقه، نام حیوان خانگی، نام خانوادگی مادر و غیره در اختیار سیستم قرار می‌گیرد. مزیت این نوع گذرواژه این است که کاربران معمولاً می‌توانند به راحتی این اطلاعات را به خاطر بسپارند. ضعف این نوع گذرواژه این است که کسی که از زندگی صمیمی فرد (همسر، فرزند، خواهر و برادر و غیره) اطلاع داشته باشد، ممکن است بتواند این اطلاعات را ارائه دهد.

✓ *One-time passwords* گذرواژه‌های یکبار مصرف. این گذرواژه نیز با عنوان رمز پویا خوانده می‌شود، فقط یک بار برای ورود به سیستم کنترل دسترسی استفاده می‌شود. این نوع گذرواژه بالاترین سطح امنیتی را ایجاد می‌کند زیرا این گذرواژه‌ها بعد از استفاده از آنها دور انداخته می‌شوند.

✓ *Graphical passwords* گذرواژه‌های گرافیکی. همچنین به آن CAPTCHA نیز می‌گویند که مخفف تست کاملاً اتوماتیک عمومی تورینگ برای گفتن رایانه‌ها و انسان‌ها به صورت جداگانه است. این نوع گذرواژه از گرافیک به عنوان بخشی از مکانیزم احراز هویت استفاده می‌کند. یک پیاده سازی مرسوم به یک کاربر نیاز دارد تا یک سری از کاراکترها را در گرافیک نمایش داده شده وارد کند. این پیاده سازی تضمین می‌کند که یک فرد گذرواژه را وارد می‌کند، نه یک ربات. یک پیاده سازی رایج دیگر اینگونه است که، کاربر را ملزم به انتخاب گرافیک مناسب برای حساب خود از لیست گرافیک‌های داده شده می‌کند.

✓ *Numeric passwords* گذرواژه‌های عددی. این نوع گذرواژه فقط اعداد را شامل می‌شود. به خاطر داشته باشید که انتخاب گذرواژه با تعداد رقم مجاز است. به عنوان مثال، اگر تمام گذرواژه‌ها ۴ رقمی باشد، حداکثر تعداد گذرواژه از ۰۰۰۰ تا ۹۹۹۹ که حداکثر ۱۰,۰۰۰ خواهد بود.

گذرواژه‌ها ضعیف تر از Passphrases، گذرواژه‌های یک بار مصرف، دستگاه‌های نشانه گذاری Token و عبارات ورود به سیستم هستند. بعد از اینکه سازمان تصمیم گرفت از کدام نوع گذرواژه استفاده کند، سازمان باید سیاست‌های مدیریت گذرواژه خود را تنظیم کند.

ملاحظات مدیریت گذرواژه شامل موارد زیر است:

- طول عمر گذرواژه *Password life*: گذرواژه تاچه مدت معتبر خواهد بود. برای بیشتر سازمانها، گذرواژه‌ها ۶۰ تا ۹۰ روز اعتبار دارند.
 - سابقه گذرواژه *Password history*: تاچه مدت قبل از استفاده مجدد از یک گذرواژه، امکانپذیر است. سیاست گذرواژه معمولاً تعداد معینی از گذرواژه‌های قبلاً استفاده شده را به خاطر می‌آورد.
 - دوره/حراز هویت *Authentication period*: چه مدت کاربر می‌تواند داخل سیستم باشد. اگر یک کاربر برای مدتی بدون فعالیت داخل سیستم باشد، کاربر به طور خودکار از سیستم خارج می‌شود.
 - پیچیدگی گذرواژه *Password complexity*: نحوه ساخت گذرواژه بیشتر سازمان‌ها به حروف بزرگ، کوچک و اعداد و شخصیت‌های خاص احتیاج دارند.
 - طول گذرواژه *Password length*: گذرواژه باید چه اندازه باشد اکثر سازمان‌ها به ۸ تا ۱۲ کاراکتر نیاز دارند.
 - پنهان کردن گذرواژه *Password masking*: با پنهان کردن کاراکترهای وارد شده به جز آخرین مورد، از یادگیری گذرواژه از طریق گشت و گذار در حاشیه جلوگیری می‌کند.
- به عنوان بخشی از مدیریت گذرواژه، سازمانها باید روشی را برای تغییر گذرواژه‌ها ایجاد کنند. اکثر سازمان‌ها خدماتی را پیاده سازی می‌کنند که به کاربران امکان می‌دهد گذرواژه خود را به طور خودکار قبل از انقضا رمز تنظیم مجدد کنند. علاوه بر این، بیشتر سازمان‌ها باید در مواردی که کاربران گذرواژه خود را فراموش کرده اند یا گذرواژه‌های خود را به خطر انداخته اند، سیاست تنظیم مجدد گذرواژه را در نظر بگیرند. یک روش تنظیم مجدد گذرواژه برای سرویس دهی به کاربران این امکان را می‌دهد تا بدون کمک کارمندان Helpdesk، گذرواژه‌های خود را تنظیم کنند. یک روش بازنشانی (Reset) گذرواژه کمک می‌کند تا کاربران برای کمک به تغییر گذرواژه‌های خود با Helpdesk راهنما تماس بگیرند.
- سیاست‌های ریست کردن گذرواژه همچنین می‌تواند تحت تأثیر سیاستهای سازمانی دیگر، مانند سیاست‌های قفل کردن حساب قرار گیرد. سیاست بستن حساب، سیاستهای امنیتی است که سازمانها برای محافظت در برابر حمله‌هایی که علیه گذرواژه‌ها انجام می‌دهند، اعمال می‌کنند. سازمانها معمولاً سیاست‌های حساب را پیکربندی می‌کنند تا حسابهای کاربری پس از تعداد مشخصی از تلاشهای ناموفق ورود به سیستم قفل شوند. در صورت قفل شدن یک حساب، ممکن

است ادمین سیستم نیاز به باز کردن یا فعال کردن مجدد حساب کاربر داشته باشد. متخصصان امنیت همچنین باید دلگرمی سازمانها را در نظر بگیرند که در صورت قفل شدن حساب کاربری یا پس از استفاده از گذرواژه برای مدت معینی (۹۰ روز برای بیشتر سازمانها)، کاربران را مجبور به تنظیم مجدد گذرواژه خود کنند. برای اکثر سازمانها، کلیه سیاستهای گذرواژه، از جمله سیاستهای قفل کردن حساب، در سطح سازمانی روی سرورهایی که شبکه را مدیریت می کنند، اجرا می شوند. سیاست بستن حساب اغلب برای محافظت در برابر حملات بی رحمانه (Brute-force) یا فرهنگ لغت (Dictionary) استفاده می شود.

توجه داشته باشید

اصطلاح قدیمی تر که شاید لازم باشد با آن آشنا باشید سطح قطع Clipping level است. سطح قطع یک خط مبنای تنظیم شده است که در بالای آن تخلفات ثبت می شود. به عنوان مثال، یک سازمان ممکن است بخواهد بعد از اولین تلاش، ثبت نام ناموفق برای ورود به سیستم را آغاز کند، و در صورت وجود وقفه پس از پنج تلاش ناموفق، حساب قفل می شود.

با توجه به نوع استفاده از سرورها برای مدیریت شرکت، متخصصان امنیت باید از موارد امنیتی که بر حساب کاربری و مدیریت گذرواژه تأثیر می گذارد آگاه باشند. دو سیستم عامل متداول سرور لینوکس و ویندوز هستند.

برای لینوکس، گذرواژه ها در فایل `etc/passwd` و `etc/shadow` ذخیره می شوند. از آنجا که فایل `etc/passwd` یک فایل متنی است که به راحتی قابل دسترسی است، باید تضمین شود که هر سرور لینوکس از فایل `etc/shadow` استفاده می کند که در آن می توان با استفاده از هش از گذرواژه در فایل محافظت کند.

کاربر اصلی در لینوکس یک حساب کاربری پیش فرض است که به کل سطح سرور دسترسی سطح اداری `Administrative-level` داده می شود. اگر حساب اصلی به خطر بیفتد، باید گذرواژه ها را تغییر داد. دسترسی به حساب `root` فقط باید برای سرورهای سیستم محدود شود و ورود به سیستم `root` فقط باید از طریق یک کنسول سیستم محلی انجام شود نه از راه دور.

برای رایانه های دارای ویندوز که در کارگروه ها قرار دارند، مدیر حساب های امنیتی `Security Accounts Manager (SAM)` گذرواژه های کاربران را با فرمت هش ذخیره می کند. با این حال، مسائل امنیتی شناخته شده با `SAM` وجود دارد، از جمله امکان دریافت هش گذرواژه به طور مستقیم از رجیستری. برای محافظت از این فایل باید تمام اقدامات امنیتی توصیه شده مایکروسافت را انجام دهید. اگر یک شبکه ویندوز را مدیریت می کنید، باید نام حساب پیش فرض

Administrator را تغییر دهید یا آن را غیرفعال کنید. اگر این حساب حفظ شده است، مطمئن شوید که به آن گذرواژه اختصاص داده اید. حساب پیش فرض Administrator ممکن است دسترسی کامل به سرور ویندوز را داشته باشد.

عوامل مالکیت Ownership Factors

احراز هویت عامل مالکیت، احراز هویتی است که براساس چیزی که شخص در اختیار دارد فراهم می‌شود. عوامل مالکیت می‌تواند شامل دستگاه‌های توکن، کارت‌های حافظه و کارت‌های هوشمند باشد.

توکن همگام و ناهمگام Synchronous and Asynchronous Token

دستگاه توکن (که اغلب به عنوان ژنراتور گذرواژه از آن یاد می‌شود) یک دستگاه دستی است که سرور احراز هویت را با رمز یک بار مصرف ارائه می‌دهد. اگر روش احراز هویت به دستگاه توکن نیاز دارد، کاربر برای تایید هویت باید در اختیار فیزیکی دستگاه باشد. بنابراین اگرچه دستگاه توکن گذرواژه را برای سرور احراز هویت فراهم می‌کند، دستگاه توکن یک عامل تأیید مالکیت محسوب می‌شود زیرا استفاده از آن مستلزم مالکیت دستگاه است.

دو روش اصلی احراز هویت دستگاه استفاده می‌شود: همگام یا ناهمگام. یک توکن همگام با سرور احراز هویت، گذرواژه منحصر به فردی را ایجاد می‌کند. یک توکن ناهمگام گذرواژه را براساس تکنیک چالش / پاسخ با سرور احراز هویت تولید می‌کند، با این دستگاه توکن پاسخ صحیح را برای چالش احراز هویت سرور ارائه می‌دهد.

دستگاه توکن معمولاً فقط به دلیل هزینه استقرار دستگاه توکن در محیط‌های بسیار امن اجرا می‌شود. علاوه بر این، راه حل‌های مبتنی بر توکن به دلیل طول عمر باتری دستگاه توکن می‌توانند مشکلاتی را ایجاد کند.

کارت‌های حافظه Memory Cards

کارت حافظه، کارتی برای کشیدن می‌باشد که برای کاربران معتبر صادر می‌شود. کارت حاوی اطلاعات احراز هویت کاربر است. هنگامی که کارت از طریق کارت خوان کشیده می‌شود، اطلاعات ذخیره شده روی کارت با اطلاعاتی که کاربر وارد می‌کند مقایسه می‌شود. اگر اطلاعات مطابقت

داشته باشند، سرور احراز هویت ورود به سیستم را تأیید می کند. اگر مطابقت نداشته باشد، احراز هویت رد می شود.

از آنجا که کارت باید توسط یک کارت خوان خوانده شود، هر رایانه یا دستگاه دسترسی باید خواننده کارت Card Reader مخصوص به خود را داشته باشد. علاوه بر این، کارت ها باید ایجاد و برنامه ریزی شوند. هر دوی این مراحل پیچیدگی و هزینه را به فرآیند احراز هویت اضافه می کنند. با این وجود، اغلب برای امنیت بیشتری که ارائه می دهد، پیچیدگی زیاد و هزینه مازادی دارد که این یک مزیت صریح این سیستم است. اما داده های کارتهای حافظه محافظت نمی شود، وضعی که سازمان ها قبل از اجرای این نوع سیستم باید در نظر بگیرند این است که کارتهای فقط حافظه بسیار آسان جعل می شوند.

کارت های هوشمند Smart Cards

مشابه کارت حافظه، کارت هوشمند داده را می پذیرد، ذخیره می کند و ارسال می کند اما می تواند داده های بیشتری را نسبت به کارت حافظه نگهداری کند. کارتهای هوشمند، که اغلب به عنوان کارتهای مدار مجتمع Integrated circuit cards (ICCs) شناخته می شوند، حاوی حافظه مانند کارت حافظه هستند، اما حاوی یک تراشه تعبیه شده مانند کارتهای بانکی یا اعتباری هستند. کارتهای هوشمند از کارت خوان استفاده می کنند. با این حال، داده های روی کارت هوشمند توسط سرور احراز هویت بدون ورودی کاربر استفاده می شود. برای محافظت در برابر کارتهای هوشمند گم شده یا دزدیده شده، اکثر پیاده سازی ها کاربر را مجبور به وارد کردن پین مخفی می کند، به این معنی که کاربر در واقع عامل تأیید هویت (PIN) و مالکیت (کارت هوشمند) را ارائه می دهد.

دو نوع اساسی کارتهای هوشمند استفاده می شود: کارتهای تماس و کارتهای بدون تماس (Contact cards , Contactless cards). کارتهای تماس معمولاً با کشیدن، به تماس فیزیکی با کارت خوان نیاز دارند. کارتهای بدون تماس، که به آنها کارتهای مجاورت Proximity Card نیز گفته می شود، لازم است که نزدیک دستگاه شوند. کارتهای هیبریدی در دسترس هستند که امکان استفاده از کارت را در سیستمهای تماسی و نیز بدون تماس دارند.

برای اهداف مقایسه ای، متخصصان امنیت باید به خاطر داشته باشند که کارتهای هوشمند به دلیل تراشه های تعبیه شده دارای قدرت پردازش هستند. کارتهای حافظه قدرت پردازش ندارند. سیستم های کارت هوشمند بسیار مطمئن تر از سیستم های کارت حافظه هستند.

کارت‌های هوشمند نسبت به کارت‌های حافظه گرانتر هستند. بسیاری از سازمانها کارت‌های هوشمند را بر کارت‌های حافظه ترجیح می‌دهند، زیرا جعل آنها سخت‌تر است و می‌توان اطلاعات مربوط به آنها با استفاده از رمزگذاری محافظت شود.

عوامل مشخصه Characteristic Factors

احراز هویت فاکتور مشخصه احراز هویت است که براساس چیزی که یک شخص است ارائه می‌شود. فناوری بیومتریک فناوری است که به کاربران اجازه می‌دهد تا براساس خصوصیات فیزیولوژیکی یا رفتاری احراز هویت شوند. خصوصیات فیزیولوژیکی شامل هر ویژگی فیزیکی منحصر به فرد کاربر از جمله عنبیه، شبکیه و اثر انگشت است. ویژگی‌های رفتاری اقدامات فرد را در یک وضعیت، از جمله الگوهای صوتی و خصوصیات ورود داده‌ها می‌سنجد. فن آوری‌های بیومتریک اکنون شروع به حرکت به برخی از رایج‌ترین سیستم‌عامل‌ها می‌کنند. مثالها از این نمونه شامل Windows Hello و فناوری Touch ID اپل می‌باشد. به عنوان یک متخصص امنیت، شما باید از چنین فن آوری‌های جدید آگاه باشید زیرا آنها برای تأمین امنیت اضافه شده گسترش پیدا کرده‌اند. آموزش کاربران در مورد این فناوری‌ها همچنین باید در اولویت قرار گیرد تا تضمین شود که کاربران هنگام استقرار، این فناوری‌ها را پذیرفته‌اند.

خصوصیات فیزیولوژیکی Physiological Characteristics

سیستم‌های فیزیولوژیکی از یک دستگاه اسکن بیومتریک برای اندازه‌گیری اطلاعات خاص در مورد ویژگی فیزیولوژیکی استفاده می‌کنند. باید سیستم‌های بیومتریک فیزیولوژیکی زیر را درک کنید:

- ✓ اثر انگشت Fingerprint
- ✓ اسکن انگشت Finger scan
- ✓ هندسه دست Hand geometry
- ✓ نقشه برداری دست Hand topography
- ✓ اسکن کف دست یا دست Palm or hand scans
- ✓ اسکن صورت Facial scans
- ✓ اسکن شبکیه Retina scans
- ✓ اسکن عنبیه Iris scans

✓ اسکن عروقی Vascular scans

اسکن اثر انگشت معمولاً خط الراس های انگشت را برای تطابق اسکن می کند. یک نوع خاص از اسکن اثر انگشت به نام تطابق جزئیات Minutiae از نظر میکروسکوپی بیشتر است زیرا باعث می شود که شکافها و سایر مشخصات دقیق را ثبت کند. تطابق Minutiae به فضای بیشتری برای سرور احراز هویت و زمان پردازش بیشتر نسبت به اسکنر خط الراس اثر انگشت احتیاج دارد. سیستم های اسکن اثر انگشت نسبت به بسیاری از سیستم ها میزان پذیرش کاربر سطح پایین تری دارند زیرا کاربران نگران نحوه استفاده و به اشتراک گذاری اطلاعات اثر انگشت هستند. اسکن انگشت فقط ویژگی های خاصی را از اثر انگشت استخراج می کند. از آنجا که مقدار محدودی از اطلاعات اثر انگشت مورد نیاز است، اسکن انگشت نسبت به هر نوع اسکن اثر انگشت به فضای سرور یا زمان پردازش کمتری نیاز دارد.

اسکن هندسه دست معمولاً اندازه، شکل یا سایر ویژگی های طرح دست کاربر را بدست می آورد، و همچنین می تواند طول استخوان یا طول انگشت را اندازه گیری کند. دو دسته از سیستم های هندسه دستی سیستم های کارآگاهی مرز تصویر و مکانیکی هستند. علیرغم این که کدام دسته مورد استفاده قرار می گیرد، اسکنرهای هندسه دست به فضای سرور و زمان پردازش کمتری نسبت به اثر انگشت یا اسکن انگشت نیاز دارند.

اسکن کف دست از فن آوری اثر انگشت و هندسه دست استفاده می کند. این نوع اسکن اطلاعات اثر انگشت را از هر انگشت و همچنین اطلاعات هندسه دست را ثبت می کند.

اسکن صورت ویژگی های صورت، از جمله ساختار استخوان، عرض چشم و اندازه پیشانی را ثبت می کند. در این روش بیومتریک از خاصیت خاص Eigenfeatures و خاصیت ویژه Eigenfaces استفاده می شود. هیچکدام از این روشها در واقع تصویری از صورت را ثبت نمی کنند. با خاصیت ویژه Eigenfaces، فاصله بین ویژگی های صورت اندازه گیری و ثبت می شود. با Eigenfeatures، اندازه گیری اجزای صورت جمع آوری شده و با مجموعه ای از Eigenfeatures استاندارد مقایسه می شود. به عنوان مثال، ممکن است چهره یک فرد از چهره متوسط به همراه ۲۱٪ از Eigen face 1، ۸۳٪ از Eigen face 2 و ۱۸٪ از Eigen face تشکیل شود.

اسکن شبکه الگوی رگهای خونی شبکه را اسکن می کند. اسکن شبکه نسبت به اسکن عنبیه توجه بیشتری به نفوذ دارد.

اسکن عنبیه قسمت رنگی چشم که شامل تمام شکافها، تاجها و شکافها است را بررسی می کند. اسکن های عنبیه از هر اسکن بیومتریک دیگر دقت بالاتری دارد.

اسکن عروقی الگوی رگها را در دست یا صورت کاربر اسکن می‌کند. اگرچه این روش می‌تواند انتخاب مناسبی باشد زیرا بسیار مزاحم نیست، اما صدمات جسمی به دست یا صورت، بستگی به نوع استفاده از سیستم، می‌تواند باعث رد نادرست شود.

خصوصیات رفتاری Behavioral Characteristics

سیستم‌های رفتاری برای اندازه‌گیری اقدامات شخص از یک دستگاه اسکن بیومتریک استفاده می‌کنند. باید سیستم‌های بیومتریک رفتاری زیر را درک کنید:

- امضای پویا Signature dynamics
 - ضربه زدن به کلید پویا Keystroke dynamics
 - الگوی صوتی یا چاپ Voice pattern or print
- امضای پویا، زمانی که کاربر امضا می‌کند سرعت ضربه زدن، فشار شیوه نگارش و شتاب و کاهش سرعت را اندازه‌گیری می‌کند. تأیید امضای پویا (DSV) Dynamic Signature Verification ویژگیهای امضا و ویژگیهای خاص فرآیند امضا را تجزیه و تحلیل می‌کند. ضربه زدن به کلید پویا Keystroke dynamics، الگوی تایپ را که کاربر هنگام وارد کردن گذرواژه یا عبارت دیگر از پیش تعیین شده را استفاده می‌کند، اندازه‌گیری می‌کند. در این حالت، حتی اگر گذرواژه یا عبارت صحیح وارد شود اما الگوی ورود به صفحه کلید متفاوت باشد، کاربر از دسترسی محروم می‌شود. زمان پرواز Flight time، اصطلاحی است که با ضربه زدن به کلید پویا ارتباط دارد، در واقع مدت زمان لازم برای جابجایی بین کلیدها است. زمان ماندگاری Dwell time، میزان زمانی است که یک کلید را نگه می‌دارید.
- الگوی صدا یا چاپ Voice pattern or print الگوی صوتی یک کاربر را با گفتن یک کلمه خاص اندازه‌گیری می‌کند. هنگامی که کاربر سعی در احراز هویت می‌کند، از وی خواسته می‌شود آن کلمات را به ترتیب‌های مختلف تکرار کند. اگر این الگو تطابق داشته باشد، احراز هویت مجاز است.

ملاحظات بیومتریک Biometric Considerations

- هنگام بررسی فن آوری‌های بیومتریک، متخصصان امنیت باید اصطلاحات زیر را درک کنند:
- زمان ثبت نام Enrollment time: فرایند بدست آوردن، نمونه‌ای است که توسط سیستم بیومتریک استفاده می‌شود. این روند نیاز به اقداماتی دارد که باید چندین بار تکرار شود.

- استخراج ویژگی Feature extraction : رویکرد بدست آوردن اطلاعات بیومتریک از یک نمونه جمع آوری شده از مشخصات فیزیولوژیکی یا رفتاری کاربر.
 - دقت Accuracy: مهمترین ویژگی سیستمهای بیومتریک است. این درست است که خواندن کلی صحیح خواهد بود.
 - میزان توان Throughput rate: سرعتی که سیستم بیومتریک قادر به اسکن خصوصیات و تکمیل آنالیز برای دسترسی یا انکار دسترسی خواهد بود. میزان قابل قبول ۶-۱۰ نفر در دقیقه است. یک کاربر واحد باید قادر باشد مراحل را در ۵-۱۰ ثانیه انجام دهد.
 - قابل قبول بودن Acceptability: احتمال پذیرش و پیگیری کاربران از سیستم را توصیف می کند.
 - نرخ رد خطا False rejection rate (FRR) : اندازه گیری کاربران معتبر است که به طور غلط توسط سیستم رد می شوند که به آن خطای نوع اول گفته می شود.
 - نرخ پذیرش خطا False acceptance rate (FAR) : اندازه گیری درصد کاربران نامعتبر است که به طور غلط توسط سیستم پذیرفته می شوند و به آن خطای نوع دوم نیز گفته می شود. خطاهای نوع دوم از خطاهای نوع اول خطرناک تر هستند.
 - نرخ خطای متقاطع Crossover error rate (CER) : نقطه ای که FRR با FAR برابر است. به عنوان درصد بیان شده، و مهمترین استاندارد است.
- هنگام تجزیه و تحلیل سیستمهای بیومتریک، متخصصان امنیت اغلب به نمودار Zephyr مراجعه می کنند که نقاط قوت و ضعف سیستم بیومتریک را نشان می دهد. با این حال، همچنین باید در نظر بگیرید که هر سیستم بیومتریک تا چه میزان کارایی دارد و میزان پذیرش کاربر چگونه می باشد. در زیر لیستی از رایج ترین روشهای بیومتریک رتبه بندی شده با اثربخشی قرار گرفته است که مؤثرترین آنها در مرحله اول است:
- ۱- اسکن عنبیه
 - ۲- اسکن شبکیه
 - ۳- اثر انگشت
 - ۴- چاپ دستی
 - ۵- هندسه دست
 - ۶- الگوی صوتی
 - ۷- الگوی ضربه زدن به کلید

۸- امضا پویا

در زیر لیستی از رایج ترین روش های بیومتریک رتبه بندی شده توسط پذیرش کاربر قرار گرفته است، با روش هایی که در درجه اول توسط کاربران محبوب تر است:

۱- الگوی صوتی

۲- الگوی ضربه زدن به کلید

۳- امضای پویا

۴- هندسه دست

۵- چاپ دستی

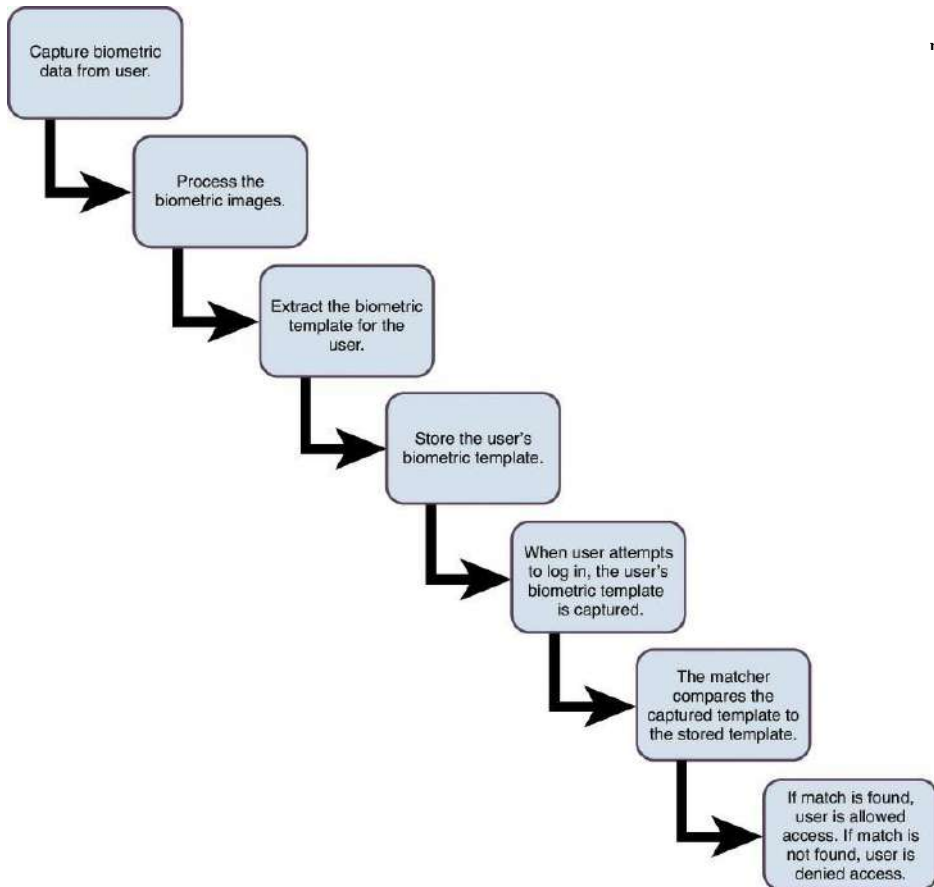
۶- اثر انگشت

۷- اسکن عنبیه

۸- اسکن شبکیه

هنگام در نظر گرفتن FAR، CER، FRR مقادیر کوچکتر بهتر می باشد. خطاهای FAR از خطاهای FRR خطرناک تر هستند. متخصصان امنیت می توانند در هنگام کمک به سازمان خود تصمیم بگیرند که کدام سیستم را پیاده سازی کند، از نرخ CER برای تحلیل مقایسه ای استفاده کنند. به عنوان مثال، سیستم های چاپ صوتی معمولاً دارای CER بالاتری نسبت به اسکن عنبیه، هندسه دست یا اثر انگشت هستند.

شکل ۵-۱ روند ثبت نام و احراز هویت بیومتریک را نشان می دهد.



شکل ۵-۱: فرآیند ثبت نام بیومتریک و احراز هویت

عوامل موقعیت مکانی Location Factors

احراز هویت عامل موقعیت مکانی، ابزاری برای احراز هویت کاربر بر اساس محلی که کاربر در آن تایید اعتبار می‌شود. این ابزار می‌تواند شامل رایانه یا دستگاهی باشد که شخص از آن استفاده می‌کند یا موقعیت جغرافیایی خود را بر اساس مختصات GPS تنظیم می‌کند. جذابیت اصلی این نوع احراز هویت این است که کاربر را برای ورود به سیستم از آن مکان‌های خاص محدود می‌کند. این امر به ویژه در محیط‌های بزرگ تولیدی برای کاربرانی که فقط باید وارد ترمینال‌های خاصی در تاسیسات شوند، بسیار مفید است.

حصار جغرافیایی Geo-fencing یکی از نمونه‌های استفاده از عوامل مکان یابی است. با استفاده از حصارهای جغرافیایی، دستگاه‌ها فقط به درستی در داخل مرزهای حصار جغرافیایی کار

می‌کنند. اگر یک دستگاه وارد منطقه جغرافیایی شده یا خارج شود، هشدار ایجاد می‌شود و به اپراتور ارسال می‌شود.

عوامل زمان Time Factors

احراز هویت عامل زمان، بر اساس زمان و یا تاریخ احراز هویت کاربر، تأیید اعتبار می‌کند. به عنوان مثال، اگر برخی از کاربران فقط با یک برنامه زمانی مشخص فعالیت می‌کنند، می‌توانید حساب‌های آنها را پیکربندی کنید و فقط به آنها اجازه می‌دهید که در طی این ساعاته فعالیت وارد سیستم شوند. با این حال، به خاطر داشته باشید که در صورت مجاز بودن ساعت اضافه کاری، چنین محدودیتی می‌تواند باعث مشکلات اداری شود. برخی سازمانها این کار را بطور موثری با پر کردن ساعات مجاز با یک یا دو ساعت آزاد برای زمان‌های شروع و پایان انجام می‌دهند. کارتهای اعتباری از این ویژگی برای محافظت از مشتریان خود به طور مؤثر استفاده می‌کنند. اگر تراکنش‌ها در یک بازه زمانی کوتاه از مکانهای پراکنده جغرافیایی انجام شوند، کارتهای اعتباری اغلب تراکنش دوم را مسدود می‌کنند.

شناسایی و اجرای احراز هویت

Identification and Authentication Implementation

شناسایی و احراز هویت اقدامات لازم برای ارائه مجوز است. مجوز Authorization، نقطه بعد از شناسایی و احراز هویت است که در آن به یک کاربر حقوق و مجوزهای لازم به منابع داده می‌شود. بخش‌های بعدی مؤلفه‌های مهم در مجوز را شامل می‌شود: تفکیک وظایف، حداقل امتیاز / نیاز به دانستن، پیش فرض عدم دسترسی، خدمات دایرکتوری، اولین ورود به سیستم (از جمله Kerberos، SESAME، مدیریت هویت فدرال، و حوزه‌های امنیتی)، مدیریت جلسه، ثبت نام و اثبات هویت، سیستم‌های مدیریت اعتبار و پاسخگویی.

• تفکیک وظایف Separation of Duties

تفکیک وظایف مفهوم مهمی است که باید در هنگام طراحی سیاست‌های احراز هویت و مجوز سازمان به خاطر داشته باشید. تفکیک وظایف با توزیع وظایف و حقوق و امتیازات مرتبط با آنها بین بیش از یک کاربر، از کلاهبرداری جلوگیری می‌کند. این امر به جلوگیری از کلاهبرداری و تبانی کمک می‌کند زیرا هرگونه عمل متقلبانه فقط در صورت تبانی ممکن است رخ دهد. یک

مثال خوب برای تفکیک وظایف، اجازه دادن به یک شخص برای مدیریت مراحل پشتیبان گیری و دیگری برای مدیریت مراحل ترمیم است.

تفکیک وظایف با کنترل دوگانه و تقسیم دانش همراه است. با کنترل های دوگانه، دو یا چند کاربر مجاز هستند و باید وظایف خاصی را انجام دهند. به عنوان مثال، یک شرکت خرده فروشی ممکن است نیاز به دو مدیر داشته باشد تا صندوق امانات را باز کنند. تقسیم دانش تضمین می کند که هیچ کاربر واحدی تمام اطلاعات برای انجام یک کار خاص را ندارد. یک نمونه از کنترل های تقسیم شده، ارتش است که به دو شخص نیاز دارد تا هر یک از آنها یک ترکیب منحصر به فرد را برای مجوز شلیک موشک وارد کنند.

• حداقل امتیاز / نیاز به دانستن Least Privilege/Need-to-Know

اصل حداقل امتیاز مستلزم این است که به یک کاربر یا فرایند فقط امتیاز حداقل دسترسی مورد نیاز برای انجام یک فعالیت خاص داده شود. هدف اصلی آن اطمینان از دسترسی کاربران فقط به منابع موردنیازش می باشد و مجاز به انجام روش هایی هستند که فقط برای انجام به آنها نیاز دارند. برای اجرای صحیح اصل حداقل امتیاز، سازمان ها باید کلیه مشاغل کاربران را شناسایی کرده و کاربران را فقط در امتیازات مشخص شده محدود کنند.

اصل نیاز به دانستن به مفهوم حداقل امتیاز نزدیک است. اگرچه حداقل امتیاز به دنبال کاهش حداقل دسترسی است، اما اصل نیاز به دانستن در واقع مشخص می کند که حداقل امتیازات برای هر شغل یا کارکرد چیست. در امتیازات بیش از حد وقتی که کاربر از حقوق، امتیازات و مجوزهای بیشتری نسبت به آنچه برای انجام فعالیت خود نیاز دارد، باعث می شود که به مشکل تبدیل می شود. کنترل بیش از حد امتیازات در محیط های بزرگ دشوار است.

اجرای مشترک اصول حداقل امتیاز و نیاز به دانستن زمانی است که برای یک ادمین سیستم یک حساب سطح ادمین و یک حساب کاربری عادی صادر می شود. در بیشتر کارکردهای روزانه، مدیر باید از حساب کاربری عادی خود استفاده کند. وقتی ادمین سیستم باید وظایف سطح مدیریتی را انجام دهد، باید از حساب سطح ادمین استفاده کند. اگر ادمین در حین انجام کارهای متدوال از حساب سطح ادمین خود استفاده کند، وی امنیت سیستم و کاربر را به خطر می اندازد.

قوانین سازمانی که از اصل حداقل امتیاز حمایت می کند شامل موارد زیر است:

- ✓ تعداد حسابهای ادمین را به حداقل برسانید.
- ✓ ادمین ها هنگام انجام عملیات معمول باید از حسابهای کاربر عادی استفاده کنند.

✓ مجوزهای مربوط به ابزارهایی که احتمالاً توسط مهاجمان استفاده می‌شود باید تا حد ممکن محدود کننده باشد.

برای سهولت در پشتیبانی از حداقل امتیازات و اصول نیاز به دانستن، کاربران باید به سه گروه تقسیم شوند تا اطلاعات مربوط به یک گروه یا منطقه را تسهیل کنند. این فرآیند به عنوان تقسیم بندی Compartmentalization شناخته می‌شود.

• پیش فرض عدم دسترسی Default to No Access

در طی مراحل مجوز، باید مکانیزم‌های کنترل دسترسی سازمان را پیکربندی کنید تا سطح پیش فرض امنیتی به طور پیش فرض عدم دسترسی باشد. این بدان معناست که اگر هیچ کاری به طور خاص برای کاربر یا گروه مجاز نشده باشد، کاربر یا گروه قادر به دسترسی به منبع نخواهند بود. بهترین رویکرد امنیتی این است که با عدم دسترسی و افزودن حقوق مبتنی بر نیاز کاربر به دانستن و حداقل امتیاز لازم برای انجام کارهای روزانه خود، شروع شود.

• خدمات دایرکتوری Directory Services

یک خدمات دایرکتوری یا خدمات کتاب راهنما یک پایگاه داده است که برای متمرکز کردن مدیریت داده‌ها در مورد موضوعات و اشیاء شبکه طراحی شده است. یک دایرکتوری معمولی حاوی سلسله مراتبی است که شامل کاربران، گروه‌ها، سیستم‌ها، سرورها، ایستگاه‌های کاری مشتری و غیره می‌شود. از آنجا که خدمات دایرکتوری حاوی داده‌های مربوط به کاربران و سایر دستگاه‌های شبکه است، می‌تواند توسط بسیاری از اپلیکیشن‌ها که نیاز به دسترسی به آن اطلاعات دارند، مورد استفاده قرار گیرد. رایج ترین استانداردهای خدمات دایرکتوری شامل:

- X.500

- پروتکل دسترسی به دایرکتوری سبک Lightweight Directory Access Protocol (LDAP)

- X.400

- خدمات دامنه دایرکتوری فعال Active Directory Domain Services (AD DS)

X.500 از پروتکل دسترسی دایرکتوری DAP استفاده می‌کند. در X.500، نام برجسته Distinguished name (DN) مسیر کامل در پایگاه داده X.500 را که ورودی در آن یافت می‌شود فراهم می‌کند. نام برجسته نسبی Relative distinguished name (RDN) در X.500 نام ورودی بدون مسیر کامل است.

براساس LDAP X.500، LDAP ساده تر از X.500 است. LDAP از DN و RDN پشتیبانی می کند، اما شامل ویژگی های بیشتری مانند نام مشترک (Common Name (CN)، مؤلفه دامنه (Domain Component (DC و ویژگی های واحد سازمانی (Unit Attributes (OU است. با استفاده از معماری مشتری / سرور، LDAP از پورت TCP 389 برای برقراری ارتباط استفاده می کند. در صورت نیاز به امنیت پیشرفته، LDAP از طریق SSL ارتباط با پورت TCP 636 برقرار می کند.

X.400 بیشتر برای انتقال و ذخیره پیام است. از عناصری (Element) استفاده می کند تا یک سری از جفت های نام / مقدار را با سمیکال (نقطه و ویرگول بدین شکل ؛) جدا کند. X.400 به تدریج با پیاده سازی پروتکل انتقال پست الکترونیکی ساده Simple Mail Transfer Protocol (SMTP) جایگزین شده است.

اجرای LDAP مایکروسافت سرویس دامنه Active Directory Domain Services (AD DS) است که داده های فهرست را در درختان و جنگل ها (Trees and Forests) ذخیره و سازماندهی می کند. همچنین فرایندهای ورود به سیستم و احراز هویت بین کاربران و دامنه ها را مدیریت می کند و به ادمین ها اجازه می دهد تا کاربران و دستگاه ها را به صورت منطقی در واحدهای سازمانی گروه بندی کنند.

اولین ورود یکپارچه Single Sign-on

در یک محیط ورود یکپارچه Single Sign-on (SSO)، کاربر یکبار اعتبار نامه ورود به سیستم را وارد می کند و می تواند به کلیه منابع موجود در شبکه دسترسی پیدا کند. انجمن امنیت گروه آزاد Open Group Security Forum اهداف بسیاری را برای SSO تعریف کرده است. برخی از اهداف واسط ورود به سیستم کاربر و مدیریت حساب کاربر شامل موارد زیر است:

- واسط باید مستقل از نوع اطلاعات احراز هویت مورد استفاده قرار گیرد.
- ایجاد، حذف و اصلاح حسابهای کاربری باید پشتیبانی شود.
- برای ایجاد یک پروفایل پیش فرض کاربر، باید یک کاربر را ایجاد و پشتیبانی کند.
- آنها باید مستقل از هر پلتفرم یا سیستم عامل باشند.

توجه داشته باشید:

برای بدست آوردن اطلاعات بیشتر در مورد استاندارد گروه ورود به سیستم آزاد، به وب سایت www.opengroup.org/secureance/sso_scope.html مراجعه کنید.

SSO هنگام اجرای آن مزایا و معایب بسیاری را ارائه می‌دهد.

مزایای استفاده از سیستم SSO عبارتند از:

- کاربران قادر به استفاده از گذرواژه‌های قوی تر هستند.
 - مدیریت کاربر و گذرواژه ساده شده است.
 - دسترسی به منابع بسیار سریعتر است.
 - ورود کاربر کارآمدتر است.
 - کاربران فقط باید اعتبار ورود به سیستم را برای یک سیستم واحد به خاطر بسپارند.
- معایب سیستم SSO شامل موارد زیر است:

- بعد از اینکه کاربر از طریق ورود به سیستم SSO اولیه دسترسی به سیستم را بدست آورد، کاربر می‌تواند به تمام منابعی که به آنها دسترسی پیدا کرده دسترسی یابد. اگرچه این نیز یک مزیت برای کاربر است (فقط یک ورود به سیستم مورد نیاز است)، اما یک نقطه ضعف نیز محسوب می‌شود زیرا تنها با یک بار ورود به سیستم می‌تواند کلیه سیستم‌های شرکت کننده در شبکه SSO را به خطر بیندازد.
- اگر اعتبار کاربر به خطر بیفتد، مهاجمان به تمام منابعی که کاربر به آنها دسترسی دارد دسترسی خواهند داشت.

اگرچه بحث در مورد SSO تاکنون به طور عمده در نحوه استفاده از آن برای شبکه‌ها و دامنه‌ها صورت گرفته است، SSO همچنین می‌تواند در سیستم‌های مبتنی بر وب پیاده سازی شود. مدیریت دسترسی به سازمان Enterprise Access Management (EAM) مدیریت کنترل دسترسی را برای سیستم‌های سازمانی مبتنی بر وب فراهم می‌کند. کارکردهای آن شامل تطابق انواع روشهای احراز هویت و کنترل دسترسی مبتنی بر نقش Role-based می‌باشد.

SSO را می‌توان در Kerberos و سیستم امن اروپایی برای اپلیکیشن‌ها در محیط‌های چند فروشنده Secure European System for Applications in a Multivendor Environment environments (SESAME) پیاده سازی کرد.

Kerberos

یک پروتکل احراز هویت، که از یک مدل مشتری / سرور توسعه یافته استفاده می‌کند که بوسیله پروژه آتن MIT تهیه شده است. این مدل احراز هویت پیش فرض در نسخه‌های اخیر ویندوز سرور است و همچنین در سیستم عامل‌های اپل، سان و لینوکس نیز استفاده می‌شود. Kerberos

یک سیستم SSO است که از رمزنگاری کلید متقارن استفاده می کند. Kerberos محرمانه و یکپارچگی را فراهم می کند.

Kerberos فرض می کند که پیام های رایانه ای، کابل کشی و رایانه های مشتری امن نیستند و به راحتی در دسترس هستند. در مبادله Kerberos شامل پیغام با یک تایید کننده می باشد، تایید کننده که شامل شناسه مشتری و زمان سنج را درج می کند. از آنجا که بلیط Kerberos برای مدت معینی معتبر است، زمان سنج اعتبار در خواست را تضمین می کند.

در یک محیط Kerberos، مرکز توزیع کلید (KDC) Key Distribution Center مخزن کلیه کلیدهای مخفی سرویس و کاربر است. مشتری درخواستی را به سرور احراز هویت (AS) ارسال می کند، که ممکن است KDC باشد یا نباشد. AS اعتبارنامه های مشتری را به KDC منتقل می کند. KDC با استفاده از کلیدهای جلسه، مشتری را برای سایر موجودیتها در شبکه تایید می کند و ارتباط را تسهیل می کند. KDC امنیت را برای مشتری یا مدیران، که کاربران خدمات شبکه و نرم افزار هستند، فراهم می کند. هر مدیر باید یک حساب کاربری در KDC داشته باشد. KDC برچسب اعطای بلیط (TGT) Ticket-granting Ticket را برای مدیر اصلی صادر می کند. وقتی مدیر نیاز به اتصال به نهاد دیگری داشته باشد، TGT به سرویس اعطای بلیط-Ticket-granting service (TGS) ارسال می شود. سپس TGS کلیدهای بلیط و جلسه را به مدیر منتقل می کند. مجموعه اصولی که مسئولیت یک KDC واحد را بر عهده دارد قلمرو Realm نامیده می شود.

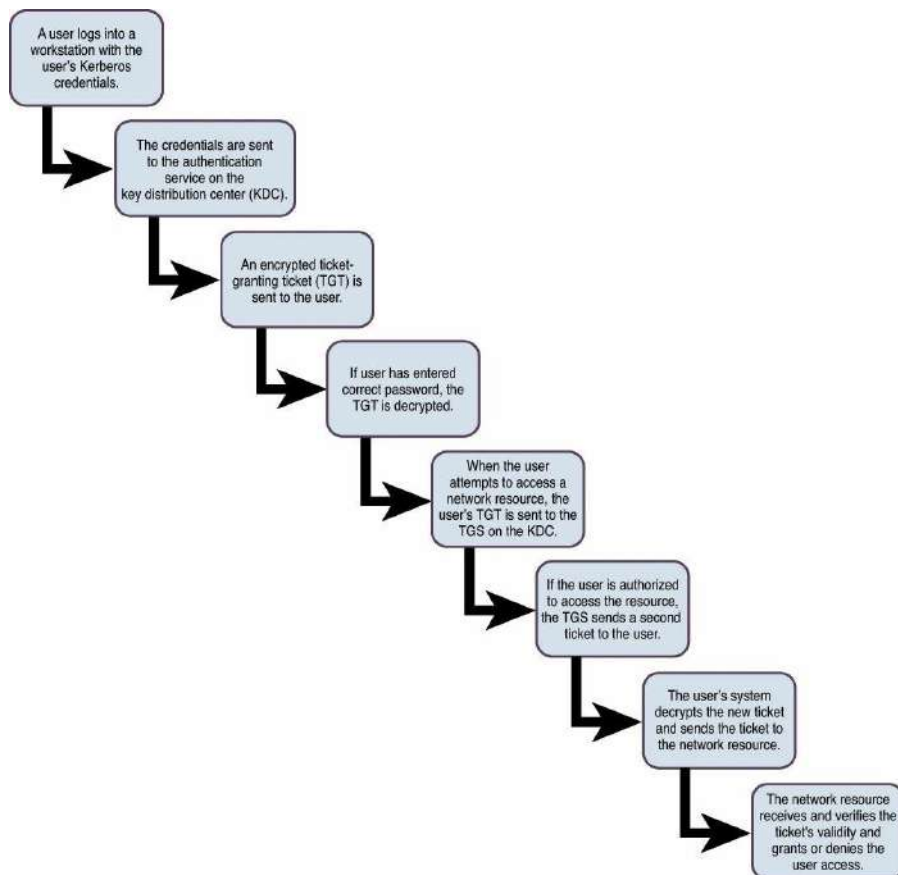
برخی از مزایای اجرای Kerberos شامل موارد زیر است:

- نیازی به ارسال گذرواژه های کاربر از طریق شبکه نیست.
- هر دو مشتری و سرور یکدیگر را تأیید می کنند.
- بلیط های منتقل شده بین سرور و مشتری زمان بندی شده و شامل اطلاعات مربوط به طول عمر هستند.
- پروتکل Kerberos از استانداردهای باز اینترنت استفاده می کند و فقط به کدهای اختصاصی یا مکانیسم های احراز هویت محدود نمی شود.

برخی از معایب اجرای Kerberos عبارتند از:

- اگر تأمین تحمل خطا یک التزام باشد، افزونگی KDC لازم است. KDC یک نقطه شکست است.
- KDC برای اطمینان از عدم تخریب عملکرد سیستم، باید مقیاس پذیر باشد.

- کلیدهای جلسه در دستگاههای مشتری قابل توافق هستند.
 - برای محافظت از اطلاعات از طریق شبکه، باید ترافیک Kerberos رمزگذاری شود.
 - کلیه سیستمهای شرکت کننده در فرایند Kerberos باید دارای ساعتی همگام باشند.
 - سیستمهای Kerberos مستعد حملات حدس زدن گذرواژه هستند.
- شکل ۵-۲: روند صدور بلیط برای Kerberos را نشان می‌دهد.



شکل ۵-۲: روند صدور بلیط Kerberos

Secure European System for Applications in a Multi-vendor Environment (SESAME)

سیستم امن اروپا برای اپلیکیشن‌ها در یک محیط چند فروشنده SESAME عملکرد Kerberos را برای رفع نقاط ضعف Kerberos گسترش داد. SESAME از رمزنگاری متقارن و نامتقارن برای

محافظت از داده های مبادله شده استفاده می کند. SESAME از یک سرور احراز هویت در هر میزبان استفاده می کند.

SESAME به جای بلیط از گواهی نامه های صفت ممتاز Privileged Attribute Certificates (PACs) استفاده می کند که شامل دو گواهی نامه می باشد: یکی برای احراز هویت و دیگری برای تعریف امتیازات دسترسی. سرور احراز هویت معتبر را نیز سرور صفت ممتاز Privileged Attribute Server (PAS) می نامند، که نقش هایی مشابه KDC در Kerberos را انجام می دهد. SESAME را می توان در یک سیستم Kerberos ادغام کرد.

مدیریت هویت هم پیمان Federated Identity Management

هویت هم پیمان یک هویت قابل حمل Portable است که می تواند در همه مشاغل و حوزه ها مورد استفاده قرار گیرد. در مدیریت هویت هم پیمان، هر سازمانی که به فدراسیون (سازمانهای متفق) بپیوندد موافقت می کند مجموعه ای از سیاست ها و استانداردها را اجرا کند. این سیاستها و استانداردها نحوه تهیه و مدیریت شناسه کاربر، احراز هویت و مجوز را تعریف می کنند. مدیریت هویت هم پیمان از دو مدل اساسی برای پیوند سازمانها در فدراسیون استفاده می کند: صدور گواهینامه متقابل و شخص ثالث یا مدل پل (Bridge).

در الگوی صدور گواهینامه متقابل Cross Certification، هر سازمان تأیید می کند که به هر سازمان دیگری اعتماد دارد. این اعتماد هنگامی ایجاد می شود که سازمانها استانداردهای یکدیگر را بررسی می کنند. هر سازمان باید با دقت کافی تأیید و تضمین کند که سایر سازمانها استانداردها را رعایت یا از آن فراتر رفته اند. یکی از مضرات صدور گواهینامه متقابل این است که تعداد روابط اعتماد که باید مدیریت شوند می تواند به مشکل تبدیل شود. علاوه بر این، احراز هویت سازمانهای دیگر می تواند وقت گیر و منابع فشرده (یک فرایند، موضوع یا مجموعه ای از فرایندها یا موضوعاتی که به منابع قابل توجه سیستم و زمان نیاز دارند، یا نیازمند دسترسی به حجم بالایی از داده ها را دارند) باشد.

در مدل مورد اعتماد شخص ثالث یا پل Trusted third-party or Bridge model، هر سازمان با معیارهای شخص ثالث مشترک می شود. شخص ثالث برای همه سازمانها تأیید، صدور گواهینامه و دقت کافی را مدیریت می کند. این مدل معمولاً در صورت نیاز داشتن به ایجاد روابط مدیریت هویت هم پیمانها با تعداد زیادی از سازمان ها، بهترین مدل است.

زبان علامت گذاری تایید امنیت 2.0 (SAML) Security Assertion Markup Language یک استاندارد SAML است که داده‌های احراز هویت و مجوز را بین سازمان‌ها یا حوزه‌های امنیتی مبادله می‌کند. از یک پروتکل مبتنی بر XML برای انتقال اطلاعات یک مدیر بین یک اعتبار SAML و یک سرویس وب از طریق توکن‌های امنیتی استفاده می‌کند. در SAML 2.0 سه نقش وجود دارد: مدیر یا کاربر، ارائه دهنده هویت و ارائه دهنده خدمات. ارائه دهنده خدمات تأیید هویت را از ارائه دهنده هویت درخواست می‌کند. SAML بسیار انعطاف پذیر است زیرا مبتنی بر XML می‌باشد. اگر یک سازمان، هویت هم پیمان SAML ساختاری را پیاده سازی کند، سازمان می‌تواند ویژگیهای هویتی را برای اشتراک با سازمان دیگر انتخاب کند.

دامنه‌های امنیتی Security Domains

دامنه مجموعه‌ای از منابع است که از طریق شبکه در دسترس یک موضوع Subject است. موضوعاتی که به یک دامنه دسترسی دارند شامل کاربران، فرآیندها و اپلیکیشن‌ها هستند. دامنه امنیتی مجموعه‌ای از منابع است که از همان سیاست‌های امنیتی پیروی می‌کند و در دسترس یک موضوع است. دامنه‌ها معمولاً در یک ساختار سلسله مراتبی حوزه‌های والدین و فرزندان مرتب می‌شوند.

توجه داشته باشید

شرط دامنه امنیتی Protection Domain را با دامنه حفاظت Protection Domain اشتباه نگیرید. اگرچه یک دامنه امنیتی معمولاً شامل یک شبکه است، یک دامنه حفاظت در یک منبع واحد قرار دارد. دامنه حفاظت، گروهی از فرآیندهایی می‌باشد که دسترسی به همان منبع را به اشتراک می‌گذارند.

مدیریت جلسه Session Management

مدیریت جلسه تضمین می‌کند که هر نمونه از شناسایی و احراز هویت به یک منبع به درستی مدیریت می‌شود، که شامل مدیریت جلسات دسکتاپ و جلسات از راه دور است. جلسات Desktop باید از طریق مکانیسم‌های مختلفی مدیریت شوند. محافظ صفحه نمایش Screensaver اجازه می‌دهد رایانه‌ها در صورت عدم فعالیت برای مدت معینی قفل شوند. برای فعال کردن مجدد رایانه، کاربر باید به سیستم وارد شود. محافظ صفحه نمایش مکانیزم زمان بندی است و سایر ویژگی‌های زمان بندی نیز ممکن است از قبیل خاموش کردن یا قرار دادن

رایانه در Hibernation که بعد از مدت معینی فعال شود. محدودیت های جلسه یا ورود به سیستم به سازمان ها اجازه می دهند تا چند جلسه همزمان یک کاربر را پیکربندی کنند. محدودیت های برنامه زمانی به سازمان ها امکان پیکربندی زمانی را می دهد که کاربر در آن می تواند به رایانه دسترسی پیدا کند.

جلسات از راه دور معمولاً برخی از مکانیسم های مشابه جلسات دسکتاپ را شامل می شوند. با این حال، جلسات از راه دور در خود رایانه رخ نمی دهند. در عوض، از طریق اتصال به شبکه انجام می شوند. جلسات از راه دور همیشه باید از پروتکل های اتصال امن استفاده کنند. علاوه بر این، اگر کاربران فقط از راه دور از طریق رایانه های معینی متصل شوند، سازمان ممکن است بخواهد نوعی دسترسی مبتنی بر قاعده Rule-based access را اجرا کند که فقط با اتصالات خاصی امکان پذیر است.

ثبت نام و اثبات هویت Registration and Proof of Identity

اثبات فرآیند هویت شامل جمع آوری و تأیید صحت اطلاعات در مورد یک فرد برای اثبات این است که شخصی که دارای یک حساب معتبر است، کسی است که ادعا می کند وجود دارد. ابتدایی ترین روش اثبات هویت، ارائه گواهینامه رانندگی، گذرنامه یا سایر شناسنامه های صادر شده دولتی است. اثبات هویت قبل از ایجاد حساب کاربری انجام می شود. پس از تکمیل اثبات هویت، برای کاربر اعتبارنامه صادر می شود و عوامل احراز هویت تعیین و ثبت می شود. از آن نقطه به بعد، هر بار کاربر با توجه به اعتبارنامه ای که صادر شده، احراز هویت می شود. انستیتوی ملی استاندارد و فناوری (NIST) اسنادی را منتشر کرده است که راهنمایی های مربوط به اثبات هویت را ارائه می دهد:

- **نشریه FIPS 201.2، تأیید هویت شخصی PIV کارمندان و پیمانکاران فدرال**
FIPS Publication 201.2, Personal Identity Verification (PIV) of Federal Employees and Contractors:
 این سند معماری و الزامات فنی استاندارد شناسایی مشترک برای کارمندان و پیمانکاران فدرال را مشخص می کند. این نشریه شامل نیازهای شناسایی، امنیت و حفظ حریم خصوصی و دستورالعمل های سیستم تأیید هویت شخصی است.
- **NIST 800-79-2، دستورالعمل های مربوط به مجوز صدور کارت های احراز هویت شخصی (PCI) و صادرکنندگان اعتبار PIV مشتق شده (DPCI)**

NIST 800-79-2, Guidelines for the Authorization of Personal Identity Verification Card Issuers (PCI) and Derived PIV Credential Issuers

(DPCI): این سند شامل دستورالعمل‌های تهیه، دستورالعمل‌های اجرای کنترل

صادرکننده و دستورالعمل‌های چرخه عمر کنترل صادرکننده است.

هر دو نشریه NIST در نظر دارد تا سازمان‌های دولتی فدرال را در اثبات هویت خود هدایت کرده و همچنین می‌تواند از سازمان‌های خصوصی برای کمک به پیشرفت سیستم‌های خود استفاده کند.

سیستم‌های مدیریت اعتبارنامه Credential Management Systems

کاربران اغلب موظف هستند نامهای کاربری، گذرواژه‌ها و سایر اطلاعات احراز هویت را برای انواع مختلف سازمان به خاطر بسپارند. آنها غالباً از همان اعتبارنامه احراز هویت در چندین سیستم عامل استفاده می‌کنند که این امر باعث می‌شود سرقت هویت آنلاین و کلاهبرداری آسان تر شود. هنگامی که مجموعه‌ای از اعتبارنامه‌های موجود در یک سیستم آنلاین کشف شد، مهاجمان اغلب از همان مجموعه مدارک معتبر در سیستم‌های سازمان دیگر استفاده می‌کنند تا ببینند آیا می‌توانند دسترسی پیدا کنند. در کنار این مشکل، مسئله داخلی سازمان برای حفظ اعتبارنامه‌های مختلف برای کاربران نیاز به دسترسی به چندین سیستم با سیستم‌های مختلف اعتبار سنجی بوجود می‌آید. افزایش فزاینده استفاده از دستگاه‌های سیار باعث یک گزارش فاجعه می‌شود.

سیستم‌های مدیریت اعتبارنامه به سازمان‌ها اجازه می‌دهند چارچوب احراز هویت و مجوز کاربر را در سراسر سازمان ایجاد کنند. سازمانها باید از متخصصان امنیت برای طراحی، استقرار و مدیریت سیستمهای مدیریت اعتبارنامه معتبر استفاده کنند. الزامات کسب و کار برای یک سیستم مدیریت اعتبارنامه باید شامل دستورالعمل‌های محافظت از حریم خصوصی فردی، راه حل‌های هویت خودکار، امنیت و نوآوری باشد. برخی از دستورالعمل‌های یک سیستم مدیریت اعتبارنامه شامل موارد زیر است:

- ✓ از گذرواژه قوی استفاده می‌شود.
- ✓ به طور خودکار گذرواژه‌های عبور پیچیده تولید می‌کنند.
- ✓ سابقه گذرواژه پیاده سازی شود.

- ✓ از مکانیسم های کنترل دسترسی استفاده کرده، از جمله (افرادی که، چه چیزی، چگونه و چه موقع دسترسی) استفاده شود.
 - ✓ ممیزی اجرا شود.
 - ✓ تهیه نسخه پشتیبان و بازیابی مکانیسم هایی برای یکپارچگی داده ها.
 - ✓ پیاده سازی سیستم های اضافی در سیستم های مدیریت اعتبارنامه برای اطمینان از دسترسی ۲۴/۷/۳۶۵.
 - ✓ سیاست های گروه مدیریت اعتبارنامه یا سایر مکانیزم های ارائه شده توسط سیستم عامل ها پیاده سازی شود.
- هنگامی که یک سازمان سیستم مدیریت اعتبارنامه را اجرا می کند، تفکیک وظایف از اهمیت بیشتری برخوردار می شود زیرا سیستم متمرکز مدیریت اعتبارنامه می تواند برای ارتکاب کلاهبرداری استفاده شود. متخصصان امنیت باید راهنمایی هایی در مورد چگونگی وقوع تفکیک برای محافظت از سازمان و دارایی های آن ارائه دهند.

مسئولیت Accountability

- مسئولیت توانایی سازمانی، که کاربران را باید برای عملکردهایی که انجام می دهند مسئول باشند. برای اطمینان از مسئولیت کاربران نسبت به اقدامات خود، سازمانها باید ممیزی و سایر مکانیزم های مسئولیت را پیاده سازی کنند.
- برای اطمینان از اینکه مسئولان در قبال اقدامات خود مسئول هستند، سازمانها می توانند ترکیبی از اجزای زیر را پیاده سازی کنند:
- ✓ **شناسایی قوی Strong identification:** هر کاربر باید حساب کاربری خود را داشته باشد. حساب های گروه یا نقش را نمی توان در یک فرد مجزا جستجو کرد.
 - ✓ **احراز هویت قوی Strong authentication:** احراز هویت چند عاملی بهتر می باشد. حداقل باید احراز هویت دو عاملی را انجام داد.
 - ✓ **نظارت Monitoring:** اقدامات کاربر باید مورد نظارت قرار گیرد، از جمله ورود به سیستم، استفاده از امتیاز و سایر اقدامات. به کاربران باید به عنوان بخشی از عدم توافق نامه حفظ حریم خصوصی، هشدار داده شود که امکان نظارت بر همه اقدامات وجود دارد.

✓ **گزارشهای ممیزی Audit Logs:** گزارشهای ممیزی باید مطابق با سیاستهای امنیتی سازمانی حفظ و ذخیره شوند. ادمین‌ها باید به صورت دوره‌ای این گزارش‌ها را بررسی کنند.

اگرچه سازمانها باید این سازوکارهای مسئولیت را به صورت داخلی پیاده سازی کنند، اما باید به طور دوره‌ای توسط شخص ثالث نیز ممیزی و آزمایش انجام شود. این عمل به این دلیل مهم است که شخص ثالث خارجی می‌تواند عینیتی را ارائه دهد که کارکنان داخلی غالباً قادر به ارائه آن نیستند.

ممیزی و گزارشگیری Auditing and Reporting

ممیزی و گزارش گیری اطمینان می‌دهد که کاربران در قبال اقدامات خود مسئول هستند، ولی یک مکانیزم ممیزی فقط می‌تواند از وقایعی که برای نظارت تنظیم شده است گزارش دهد. باید رخدادهای شبکه، رخدادهای سیستم، رخدادهای اپلیکیشن، رخدادهای کاربر و فعالیت ضربه زدن را تحت نظر داشته باشید. به خاطر داشته باشید که هرگونه فعالیت ممیزی بر عملکرد سیستم تحت نظارت تأثیر خواهد گذاشت. سازمانها باید بین ممیزی رخدادهای و فعالیتهای مهم و اطمینان از حفظ عملکرد دستگاه در سطح قابل قبول، تعادل ایجاد کنند. همچنین، سازمانها باید مطمئن شوند که هرگونه نظارتی که رخ می‌دهد مطابق با کل قوانین قابل اجرا است. در هنگام طراحی مکانیزم ممیزی، متخصصان امنیت باید دستورالعمل‌های زیر را به خاطر بسپارند:

- یک برنامه مدیریت log ممیزی تهیه کنید که شامل مکانیزمهایی برای کنترل اندازه Log ها، فرآیندهای پشتیبان گیری و طرح‌های بررسی دوره‌ای باشد.
- اطمینان حاصل کنید که امکان حذف یک ممیزی براساس یک کنترل دو نفره می‌باشد که نیاز به همکاری حداقل دو ادمین دارد، که تضمین می‌کند که یک ادمین واحد قادر به حذف Log های مربوط به شواهد جعلی نیست.
- نظارت بر همه حساب‌های دارای امتیاز بالا (از جمله کلیه کاربران اصلی و حساب‌های سطح ادمین).
- اطمینان حاصل کنید که دنباله ممیزی شامل: چه کسی تراکنش را پردازش می‌کند، چه تراکنشی رخ داده است (تاریخ و زمان)، جایی که تراکنش رخ داده است (کدام سیستم)، و اینکه آیا تراکنش موفقیت آمیز بوده است یا خیر.

- مطمئن شوید که حذف log و حذف داده ها در داخل logها نمی تواند رخ دهد، مگر اینکه کاربر مجوزهای سطح ادمین مناسبی داشته باشد.

مسیرهای ممیزی نفوذهای رایانه را تشخیص داده و اقداماتی را نشان می دهد که سوء استفاده را شناسایی می کند. به عنوان یک متخصص امنیت، باید از مسیرهای ممیزی برای بررسی الگوهای دسترسی به اشیاء فردی استفاده کرد. برای شناسایی الگوهای ناهنجار رفتاری، ابتدا باید الگوهای عادی رفتار را مشخص کرد. همچنین، باید سطح برش Clipping level را تعیین کرده، که این یک خط مبنا برای خطاهای کاربر است که در بالای آن، تخلفات ثبت خواهد شد.

به عنوان مثال، ممکن است سازمان تصمیم بگیرد اولین تلاش نامعتبر ورود به سیستم را نادیده بگیرد، با دانستن اینکه تلاشهای اولیه ورود به سیستم شکست خورده اغلب به دلیل خطای کاربر می باشد. هر ورود نامعتبر پس از اولین ورود نامعتبر ثبت می شود زیرا می تواند نشانه حمله باشد. یک سطح برش رایج که استفاده می شود برابر با سه تلاش برای ورود به سیستم است که ناموفق است. هرگونه تلاش ناموفق برای ورود به سیستم بالاتر سه بار، مخرب تلقی می شود. در بیشتر موارد، سیاست به این صورت می باشد که حساب کاربر پس از رسیدن به این سطح برش، قفل می شود.

مسیرهای ممیزی مانع از تلاش مهاجم برای دور زدن مکانیسمهای حفاظتی است که در یک سیستم یا دستگاه پیکربندی شده اند. به عنوان یک متخصص امنیت، برای ردیابی حقوق یا امتیازات سیستم یا امتیازاتی که به کاربر (اضافه کردن داده ها، حذف ها، یا تغییرات داده ها) اعطا می شود، باید مسیرهای ممیزی بطور خاص پیکربندی شوند.

سرانجام، مسیرهای ممیزی باید کنترل شوند و اعلانهای (Notification) خودکار باید پیکربندی شوند. اگر هیچکس مسیر ممیزی را رصد نکند، داده های ثبت شده در مسیر ممیزی بی فایده است. اقدامات خاصی باید تنظیم شوند تا اعلان های خودکار را به وجود آورد. به عنوان مثال، ممکن است بخواهید یک هشدار ایمیل را پیکربندی کنید که بعد از تعداد مشخصی از تلاشهای ورود به سیستم، ورود نامعتبر Invalid login رخ دهد، زیرا تلاشهای نامعتبر ورود به سیستم ممکن است نشانه ای از حمله Brute-force گذر واژه باشد.

هویت به عنوان یک سرویس پیاده سازی Identity as a Service (IDaaS) Implementation

هویت به عنوان یک سرویس IDaaS مجموعه‌ای از عملکردهای مدیریت هویت و دسترسی را برای هدف قرار دادن سیستم‌ها در محل مشتری و یا در ابر Cloud فراهم می‌کند. IDaaS شامل ادمین و اداره هویت Identity governance and administration (IGA) است، که توانایی تهیه هویت‌هایی را که توسط این سرویس برای هدف قرار دادن اپلیکیشن‌ها وجود دارد فراهم می‌کند. همچنین شامل احراز هویت کاربر، ورود یکپارچه SSO و اجرای مجوز است. خدمات IDaaS به دو دسته تقسیم می‌شوند: نرم افزار دسترسی به وب برای اپلیکیشن‌های مبتنی بر ابر و خدمات مدیریت هویت میراث ابری Cloud-delivered legacy identity anagement services. اپلیکیشن‌های Web IDaaS با اپلیکیشن‌های داخلی کار نمی‌کنند. اکثر استقرارهای IDaaS احراز هویت SSO، هویت پیمان، مدیریت از راه دور و ادغام سرویس دایرکتوری داخلی را ارائه می‌دهند. IDaaS با راه حل‌های مدیریت هویت و دسترسی IAM متفاوت است، و از طریق شبکه خود سازمان که نرم افزار و سخت افزار در خودش تعبیه شده است، اداره می‌شوند. راه حل‌های IAM ممکن است از پروتکل دستیابی Active Directory و Lightweight Directory Access Protocol (LDAP) استفاده کنند.

اگر سازمان‌ها استقرار IDaaS را در نظر بگیرند، در درجه اول باید نگران در دسترس بودن سرویس، محافظت از داده‌های هویت و اعتماد به شخص ثالث با عملکردی مهم در کسب و کار باشند، و همچنین باید نگران رعایت مقررات باشند. انتقال مدیریت هویت به ابر، سوالات زیادی را برای سازمان در مورد ممیزی، اطمینان از رعایت مقررات و آنچه در صورت افشا اتفاق می‌افتد، ایجاد می‌کند.

یک سازمان قبل از استقرار هرگونه سرویس IDaaS باید تجزیه و تحلیل جامع ریسک را انجام دهد. پس از انجام تحلیل ریسک، سازمان باید تعیین کند که کدام هویت باید به عنوان راه حل IDaaS قرار گیرد.

پیاده سازی خدمات هویت شخص ثالث Third-Party Identity Services Implementation

اگر یک سازمان تصمیم به استقرار یک سرویس هویت شخص ثالث بگیرد از جمله راه حل‌های رایانش ابری، کارکنان امنیت باید در یکپارچگی آن پیاده سازی با خدمات و منابع داخلی درگیر

شوند. این یکپارچگی می تواند پیچیده باشد، به خصوص اگر راه حل ارائه دهنده کاملاً با سیستم های داخلی موجود سازگار نباشد. بیشتر خدمات هویت شخص ثالث، هویت ابری، همگام سازی دایرکتوری و هویت هم پیمانی را ارائه می دهند. نمونه هایی از این خدمات عبارتند از سرویس وب سایت آمازون Amazon Web Services (AWS) هویت و مدیریت دسترسی Identity and Access Management (IAM) و مدیریت هویت اوراکل.

مکانیسم های مجوز Authorization Mechanisms

مکانیسم های مجوز سیستم هایی می باشد که یک سازمان برای کنترل سیستم هایی که کاربر یا دستگاه می تواند به آن دسترسی داشته باشد، مستقر می شود. مکانیسم های مجوز شامل مدل های کنترل دسترسی و سیاست های کنترل دسترسی است.

مدل های کنترل دسترسی Access Control Models

یک مدل کنترل دسترسی توصیف رسمی از سیاست امنیتی یک سازمان است. مدل های کنترل دسترسی برای ساده سازی مدیریت کنترل دسترسی با گروه بندی اشیاء و افراد اجرا می شوند. موضوع ها Subjects هویت هایی هستند که درخواست دسترسی به یک شی یا داده های موجود در یک شی را دارند. کاربران، برنامه ها و فرایندها موضوع هستند. اشیاء Objects موجودیت هایی هستند که حاوی اطلاعات یا عملکرد هستند. رایانه ها، بانکهای اطلاعاتی، فایل ها، برنامه ها، دایرکتوری ها و زمینه ها اشیاء هستند. یک مدل کنترل دسترسی امن باید تضمین کند که اشیاء امن نمی توانند به سمت موضوعی با امنیت کمتر حرکت کنند. مدل ها و مفاهیم کنترل دسترسی موارد زیر را شامل می شود:

- ✓ کنترل دسترسی اختیاری Discretionary access control
- ✓ کنترل دسترسی اجباری Mandatory access control
- ✓ کنترل دسترسی مبتنی بر نقش Role-based access control
- ✓ کنترل دسترسی مبتنی بر قانون Rule-based access control
- ✓ کنترل دسترسی وابسته به محتوا در مقابل وابسته به متن Content-dependent versus context-dependent access control
- ✓ ماتریس کنترل دسترسی Access control matrix
- ✓ جدول قابلیت ها Capabilities table

ACL ✓

• کنترل دسترسی اختیاری Discretionary access control

در کنترل دسترسی اختیاری DAC، صاحب شی مشخص می‌کند که افراد می‌توانند به منابع دسترسی پیدا کنند. DAC معمولاً در موقعیت‌های محلی و پویا استفاده می‌شود. دسترسی مبتنی بر هویت موضوع، پروفایل یا نقش است. DAC به عنوان یک کنترل نیاز به دانستن Need-to-know در نظر گرفته شده است.

DAC می‌تواند یک مسئولیت مدیریتی باشد زیرا نگهبان داده یا مالک داده امتیازات دسترسی را به کاربران اعطا می‌کند. براساس DAC، وقتی موضوع از سازمان خارج شود، باید حقوق موضوع خاتمه یابد. کنترل دسترسی مبتنی بر هویت زیر مجموعه‌ای از DAC است و مبتنی بر هویت کاربر یا عضویت گروهی است.

کنترل دسترسی غیر اختیاری برعکس DAC است. در کنترل دسترسی غیر اختیاری، کنترل‌های دسترسی توسط یک ادمین امنیتی یا مقامات دیگر پیکربندی می‌شوند. قدرت مرکزی تصمیم می‌گیرد که موضوعات براساس سیاست سازمان، به چه اشیایی دسترسی داشته باشند. در کنترل دسترسی غیر اختیاری، سیستم هویت موضوع را با ACL اشیاء مقایسه می‌کند.

• کنترل دسترسی اجباری Mandatory Access Control

در کنترل دسترسی اجباری MAC، مجوز موضوع بر اساس برچسب‌های امنیتی است. MAC اغلب به دلیل اینکه مبتنی بر سیستم برچسب امنیتی Security Label است، به عنوان منع کننده توصیف می‌شود. تحت MAC، تمام آنچه صراحتاً مجاز نیست ممنوع است. فقط ادمین می‌تواند دسته یا گروه یک منبع را تغییر دهد.

MAC از DAC امن‌تر است. DAC نسبت به MAC انعطاف پذیرتر و مقیاس پذیرتر است. به دلیل اهمیت امنیت در MAC، برچسب زدن لازم است. طبقه بندی داده‌ها نشانگر حساسیت داده‌ها است. در سیستم MAC، اختیار امتیاز یک موضوع است. به هر موضوع و شی یک برچسب امنیتی یا برچسب حساسیت داده می‌شود. برچسب‌های امنیتی سلسله مراتبی هستند. برای سازمان‌های تجاری، سطح برچسب‌های امنیتی می‌تواند محرمانه، اختصاصی، شرکتی، حساس و عمومی باشد. برای نهادهای دولتی یا نظامی، سطح برچسب‌های امنیتی می‌تواند بالاترین سطح پنهانی، پنهانی، محرمانه و غیرقابل طبقه بندی باشد.

در MAC، سیستم هنگامی که اختیار موضوع را با برچسب امنیتی شیء مقایسه می کند، تصمیمات دسترسی را اتخاذ می کند.

• کنترل دسترسی مبتنی بر نقش Role-Based Access Control

در کنترل دسترسی مبتنی بر نقش RBAC، هر موضوع به یک یا چند نقش اختصاص داده می شود. نقش ها سلسله مراتبی هستند. کنترل دسترسی بر اساس نقش ها تعریف می شود. RBAC می تواند مورد استفاده قرار گیرد تا به راحتی حداقل امتیازات مربوط به افراد را اعمال کند. نمونه ای از RBAC اجرای یک سیاست کنترل دسترسی برای فروشندگان بانکی و سیاست دیگر برای ماموران وام است.

RBAC به اندازه مدل های کنترل دسترسی که قبلاً ذکر شد ایمن نیست زیرا امنیت بر اساس نقش ها است. RBAC معمولاً هزینه بسیار کمتری نسبت به سایر مدلها دارد و در اپلیکیشن های تجاری رایج است. این یک انتخاب عالی برای سازمان هایی است که کارمندان گردش مالی بالایی دارند. RBAC به طور مؤثر می تواند جایگزین DAC و MAC شود زیرا اجازه می دهد سیاست های امنیتی سازمان را به شکل نقشه بر ساختار سازمان تنظیم و اجرا شود.

RBAC به چهار روش اداره می شود. در Non-RBAC، هیچ نقشی استفاده نمی شود. در RBAC محدود، کاربران در نقش های اپلیکیشن منحصر به فرد نقشه برداری شده اند، اما برخی از اپلیکیشن ها از RBAC استفاده نمی کنند و نیاز به دسترسی به هویت دارند. در RBAC هیبریدی، هر کاربر نقش واحدی را ترسیم می کند که به آنها اجازه می دهد تا به چندین سیستم دسترسی پیدا کنند، اما هر کاربر می تواند در نقش های دیگری که به سیستم های منحصر به فرد دسترسی دارند، نقشه برداری کند. RBAC کامل، کاربران برای نقش واحدی ترسیم شده اند که توسط سیاست امنیتی سازمان تعریف شده است و دسترسی به سیستم ها از طریق نقش های سازمانی مدیریت می شود.

• کنترل دسترسی مبتنی بر قانون Rule-Based Access Control

کنترل دسترسی مبتنی بر قانون، تغییرات مکرر به مجوزهای داده را تسهیل می کند و در RFC 2828 تعریف شده است. با استفاده از این روش، یک سیاست امنیتی مبتنی بر قوانین سراسری است که برای همه کاربران وضع شده است. از پروفایل ها برای کنترل دسترسی استفاده می کنند. بسیاری از روترها و فایروال ها از این نوع کنترل دسترسی استفاده می کنند و تعریف می کنند که

کدام نوع بسته‌ها در یک شبکه مجاز است. قوانینی را می‌توان نوشت که اجازه دسترسی یا عدم دسترسی را براساس نوع بسته، شماره پورت مورد استفاده، آدرس MAC و پارامترهای دیگر می‌دهد.

• محتوا-وابسته در مقابل متن وابسته Content-Dependent Versus Context-Dependent

کنترل دسترسی وابسته به محتوا، تصمیمات دسترسی را براساس داده‌های موجود در شی اتخاذ می‌کند. با استفاده از این کنترل دسترسی، داده‌هایی که کاربر می‌بیند ممکن است بر اساس سیاست و قوانین دسترسی اعمال شده تغییر کند.

کنترل دسترسی وابسته به متن مبتنی بر ویژگی‌های موضوع یا هدف یا ویژگی‌های محیطی است. این خصوصیات می‌تواند شامل محل یا زمان یا روز باشد. نمونه‌ای از این موارد در صورتی است که ادمین‌ها یک سیاست امنیتی را اجرا می‌کنند که تضمین می‌کند کاربر فقط در ساعات مشخصی از روز از یک ایستگاه کاری workstation خاص وارد شود.

کارشناسان امنیتی واسط کاربری محدود را به عنوان روش دیگر کنترل دسترسی در نظر می‌گیرند. نمونه‌ای از واسط کاربری محدود شده، یک پوسته Shell است، که یک واسط نرم در یک سیستم عامل است که کنترل دسترسی را با محدود کردن فرمان‌های سیستم موجود انجام می‌دهد. مثال دیگر نمایه‌های View پایگاه داده است که بر اساس معیارهای سیستم یا کاربر فیلتر می‌شوند. واسط‌های کاربر محدود می‌توانند بستگی به محتوا و یا بستگی به متن و به چگونگی محدود کردن واسط توسط ادمین داشته باشند.

• ماتریس کنترل دسترسی Access Control Matrix

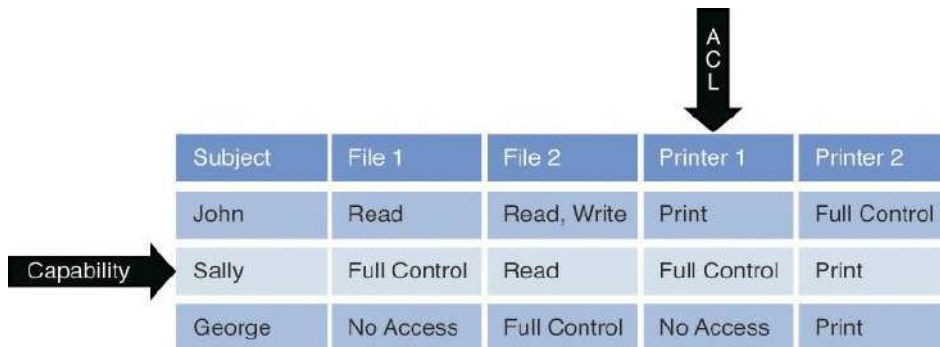
یک ماتریس کنترل دسترسی یک جدول است که شامل لیستی از موضوعات، لیستی از اشیاء و لیست کارهایی است که یک موضوع می‌تواند بر روی هر شی انجام دهد. ردیف‌های موجود در ماتریس، موضوعات هستند و ستون‌های موجود در ماتریس، اشیاء هستند. اجرای مشترک یک ماتریس کنترل دسترسی شامل یک جدول قابلیت‌ها و یک ACL است.

• جدول قابلیت ها Capabilities Table

یک قابلیت با ردیف یک موضوع در یک ماتریس کنترل دسترسی مطابقت دارد. یک جدول قابلیت ها حقوق دسترسی که یک موضوع خاص برای اشیاء دارد، را فهرست می کند. جدول قابلیت ها در مورد موضوع است.

• ACL

ACL با ستون یک شی از یک ماتریس کنترل دسترسی مطابقت دارد. ACL تمام حقوق دسترسی موضوعات به یک شی خاص را فهرست می کند. ACL در مورد شی است. شکل ۳-۵ ماتریس کنترل دسترسی و چگونگی قابلیت و ACL که بخشی از آن است، را نشان می دهد.



	Subject	File 1	File 2	Printer 1	Printer 2
John	Read	Read, Write	Print	Full Control	
Sally	Full Control	Read	Full Control	Print	
George	No Access	Full Control	No Access	Print	

شکل ۳-۵: ماتریس کنترل دسترسی

سیاست های کنترل دسترسی Access Control Policies

سیاست کنترل دسترسی روش شناسایی و تأیید هویت کاربران و سطح دسترسی مفروض به کاربران را تعریف می کند. سازمانها باید سیاست های کنترل دسترسی را به کار گیرند تا اطمینان حاصل شود که تصمیمات کنترل دسترسی برای کاربران براساس دستورالعمل های رسمی است. اگر سیاست کنترل دسترسی اتخاذ نشود، سازمانها در اختصاص دادن، مدیریت و مدیریت اداره کردن دسترسی مشکل خواهند داشت.

تهدیدات کنترل دسترسی Access Control Threats

تهدیدات کنترل دسترسی مستقیماً بر محرمانه بودن، یکپارچگی و در دسترس بودن داراییهای سازمان تأثیر می‌گذارد. هدف اکثر تهدیدات کنترل دسترسی آسیب زدن به یک سازمان است. از آنجا که آسیب رساندن به یک سازمان از درون شبکه خود آسانتر است، افراد خارجی معمولاً ابتدا سعی می‌کنند به هر کنترل دسترسی که در سازمان وجود دارد حمله کنند. تهدیدهای کنترل دسترسی عبارتند از:

- تهدیدهای گذرواژه Password threats
- تهدیدهای مهندسی اجتماعی Social engineering threats
- DoS / DDoS
- سرریزی بافر Buffer overflow
- کد سیار Mobile code
- بد افزار Malicious software
- جعل Spoofing
- خرابکاری و استراق سمع Sniffing and Eavesdropping
- ساطع (انتشار) Emanating
- Backdoor/trapdoor

✓ تهدیدات گذرواژه Password Threats

تهدید گذرواژه هرگونه حمله‌ای است که سعی در کشف گذرواژه‌های کاربر دارد. دو تهدید رایج گذرواژه حملات فرهنگ لغت Dictionary و حملات بی رحمانه Brute-force است. بهترین اقدامات متقابل در برابر تهدیدات گذرواژه، اجرای سیاستهای پیچیده گذرواژه، کاربران را ملزم می‌کند که به طور مرتب گذرواژه را تغییر دهند، استفاده از سیاست‌های قفل کردن حساب، رمزگذاری فایل‌های گذرواژه و استفاده از ابزارهای گذرواژه برای کشف گذرواژه‌های ضعیف است.

حمله فرهنگ لغت Dictionary Attack

هنگامی رخ می‌دهد که مهاجمان برای کشف گذرواژه‌ها از فرهنگ لغات مشترک استفاده می‌کنند. یک برنامه خودکار از هش کلمه فرهنگ لغت استفاده می‌کند و این مقدار هش را با ورودی‌های

موجود در فایل گذرواژه سیستم مقایسه می کند. اگرچه این برنامه با فرهنگ لغت همراه است، اما مهاجمان همچنین از فرهنگ لغات اضافی استفاده می کنند که در اینترنت یافت می شوند. باید یک قانون امنیتی را اجرا کرده که می گوید گذرواژه نباید کلمه ای باشد که در فرهنگ لغت یافت شود تا در برابر این حملات محافظت شود. همچنین می توان یک سیاست بستن حساب را به گونه ای اجرا کرد که یک حساب پس از تعداد مشخصی از ورود نامعتبر به سیستم قفل شود.

حمله بی رحمانه Brute-Force

حملات بی رحمانه انجام آنها دشوارتر است زیرا آنها در تمام ترکیبات ممکن از اعداد و کاراکترها کار می کنند. از حمله بی رحمانه نیز به عنوان یک حمله کامل استفاده می شود. تا زمان یافتن یک گذرواژه صحیح، جستجوهای گذرواژه را ادامه می دهد. این حملات همچنین بسیار زمان بر می باشد.

✓ تهدیدات مهندسی اجتماعی Social Engineering Threats

حملات مهندسی اجتماعی زمانی اتفاق می افتد که مهاجمان برای بدست آوردن اعتبارنامه Credentials کاربر یا برخی اطلاعات محرمانه دیگر از زبان باورپذیری و ساده لوحی کاربر استفاده می کنند. تهدیدهای مربوط به مهندسی اجتماعی که باید درک شود شامل Phishing/Pharming، گشت و گذار شانه ای Shoulder Surfing، سرقت هویت و جستجوی سطل آشغال است. بهترین اقدامات متقابل در برابر تهدیدهای مهندسی اجتماعی، ارائه آموزش آگاهی درباره امنیت کاربر است. این آموزش مورد نیاز بوده و باید بطور منظم انجام شود زیرا تکنیک های مهندسی اجتماعی به طور مداوم تکامل می یابد.

• Phishing/Pharming

فیشینگ یک حمله مهندسی اجتماعی است که در آن مهاجمان سعی می کنند اطلاعات شخصی از جمله اطلاعات کارت اعتباری و داده های مالی را کشف کنند. این نوع حمله معمولاً با پیاده سازی یک وب سایت جعلی انجام می شود که بسیار شبیه به یک وب سایت قانونی است. کاربران داده هایی را از جمله اعتبارنامه موجود را در وب سایت جعلی وارد می کنند و به مهاجمان امکان می دهند هرگونه اطلاعات وارد شده را ضبط کنند. نیزه فیشینگ یک حمله است که با آگاهی از عادات و علایق هدف مورد نظر علیه یک هدف خاص انجام می شود. به دلیل اطلاعاتی که باید

جمع شود، حملات نیزه فیشینگ بیشتر از حملات فیشینگ انجام می‌شود. Whaling نوعی فیشینگ است که بطور خاص مدیران سطح بالا یا سایر افراد دارای مشخصات سطح بالا را هدف قرار می‌دهد. Vishing نوعی فیشینگ است که از یک سیستم تلفن یا فن آوری‌های VoIP استفاده می‌کند. کاربر در ابتدا تماس، متن یا ایمیل دریافت می‌کند که می‌گوید با یک شماره خاص تماس بگیرید و اطلاعات شخصی مانند نام، تاریخ تولد، شماره تأمین اجتماعی و اطلاعات کارت اعتباری را وارد کند.

Pharming شبیه به فیشینگ است، ولی در واقع محتوای حافظه کش DNS رایانه را آلوده می‌کند، به طوری که درخواست‌ها به جای یک سایت قانونی به یک سایت جایگزین منتقل می‌شوند.

کاربران باید در مورد استفاده از لینک‌های تعبیه شده در پیام‌های ایمیل احتیاط کنند، حتی اگر به نظر می‌رسد این پیام از یک نهاد مشروع دریافت شده باشد. کاربران همچنین باید هر بار که به یک سایت دسترسی پیدا می‌کنند در جایی که اطلاعات شخصی آنها لازم است برای اطمینان از صحت سایت و استفاده از SSL، نوار آدرس را بررسی کنند، که در ابتدای آدرس URL یک مشخصه HTTPS وجود داشته باشد.

• گشت و گذار شانه‌ای Shoulder Surfing

زمانی اتفاق می‌افتد که یک مهاجم هنگام وارد کردن اطلاعات برای ورود کاربر یا ورود اطلاعات محرمانه، آنها را مشاهده می‌کند. کاربران را ترغیب کرده تا همیشه از اینکه چه کسی اقدامات وی را مشاهده می‌کند، آگاه باشند. پیاده سازی صفحه نمایش‌های خصوصی اطمینان می‌دهد که نمی‌توان ورود اطلاعات را ضبط کرد.

• سرقت هویت Identity Theft

سرقت هویت هنگامی اتفاق می‌افتد که فردی اطلاعات شخصی از جمله شماره گواهینامه راننده، شماره حساب بانکی و شماره تأمین اجتماعی را بدست می‌آورد و از این اطلاعات به جای هویت شخصی که اطلاعات وی به سرقت رفته استفاده می‌کند. پس از سرقت هویت، حمله می‌تواند از هر جهت پیش برود. در بیشتر موارد، مهاجمان حساب‌های مالی را به نام کاربر باز می‌کنند. مهاجمان همچنین می‌توانند به حساب‌های معتبر کاربر دسترسی پیدا کنند.

• جستجوی سطل آشغال Dumpster Diving

هنگامی اتفاق می افتد که مهاجمان برای دستیابی به اطلاعات محرمانه، زباله ها را بررسی می کنند و شامل اطلاعات مربوط به پرسنل، اطلاعات ورود به حساب، نمودارهای شبکه و داده های مالی سازمانی است. سازمان ها باید سیاست هایی را برای خرد کردن اسناد حاوی این اطلاعات پیاده سازی کنند.

✓ DoS / DDoS

حمله انکار سرویس DoS هنگامی رخ می دهد که مهاجمان با درخواست های کافی برای تخریب عملکرد دستگاه مورد نظر، دستگاه را غرق Flood می کنند. برخی از حملات رایج DoS شامل Flood SYN و حملات Teardrop است.

حمله توزیع شده DoS (DDoS) یک حمله DoS است که از چندین مکان حمله انجام می شود. دستگاه های آسیب پذیر آلوده به عامل های نرم افزاری هستند که زامبی نامیده می شوند، و دستگاه های آسیب پذیر را تبدیل به بات نت می کند و سپس حمله را انجام می دهد. به دلیل توزیع ماهیت حمله، شناسایی همه بات نت های حمله کننده تقریباً غیرممکن است. بات نت ها همچنین به مخفی کردن منبع اصلی حمله کمک می کنند.

✓ سرریز بافر Buffer Overflow

بافرهای بخشی از حافظه سیستم هستند که برای ذخیره اطلاعات استفاده می شوند. سرریز بافر هنگامی اتفاق می افتد که مقدار داده هایی که به اپلیکیشن ارسال شده زیاد تر از بافر باشد که بتواند رسیدگی کند. به طور معمول، این نوع حمله به دلیل ضعف برنامه نویسی یا کد سیستم عامل امکان پذیر است. این نوع حمله می تواند به تزریق کد مخرب منجر شود.

برای محافظت در برابر این مسئله، سازمانها باید مطمئن شوند که همه سیستم عامل ها و اپلیکیشن ها با جدیدترین بسته های خدماتی، بروزرسانی ها و پچ ها به روز شده اند. علاوه بر این، برنامه نویسان باید تمام اپلیکیشن ها را به درستی تست کنند تا شرایط سرریز بررسی شود. سرانجام، برنامه نویسان باید از اعتبار ورودی استفاده کنند تا تضمین شود که داده های ارسالی برای بافر خیلی زیاد نیستند.

✓ کد سیار Mobile Code

کد سیار هر نرم افزاری است که از طریق شبکه منتقل می شود تا بر روی یک سیستم محلی پیاده سازی شود. نمونه هایی از کد سیار شامل اپلت های جاوا، کد اسکریپت جاوا و کنترل های ActiveX است. کد سیار شامل کنترل های امنیتی، جعبه شنی جاوا Java sandbox و امضاهای کد دیجیتال ActiveX است. برای دور زدن کنترل های دسترسی می توان از کد سیار مخرب استفاده کرد.

سازمان ها باید مطمئن شوند که کاربران دغدغه های امنیتی درباره کد سیار مخرب را درک می کنند. کاربران فقط باید کد سیار را از سایت های مجاز و فروشندگان مجاز دانلود کنند.

✓ بد افزار Malicious Software

نرم افزارهای مخرب که به آن بد افزار نیز می گویند، هر نرم افزاری است که برای انجام اعمال مخرب طراحی شده است.

به پنج کلاس بد افزارها اشاره می کنیم:

- ۱- ویروس: هر بد افزار که برای تکثیر یا توزیع، خود را به اپلیکیشن دیگری متصل می کند.
- ۲- Worm: هر بد افزاری که خودش را تکرار کند، به این معنی که نیازی به اپلیکیشن یا تعامل انسانی برای انتشار ندارد.
- ۳- اسب تروجان: هر بد افزاری که هنگام انجام اقدامات مخرب خود را به عنوان یک اپلیکیشن مورد نیاز تبدیل می کند.
- ۴- Spyware: هر بد افزاری که داده های کاربر خصوصی از جمله سابقه مرور Browsing History یا ورودی صفحه کلید را جمع می کند.
- ۵- Ransomware: هر بد افزاری که مانع یا باعث محدود کردن دسترسی کاربر به سیستم یا دستگاهش شود و معمولاً قربانیان را مجبور می کند تا برای دوباره بدست آوردن دسترسی سیستم پرداختی را انجام دهند (باج گیری).

بهترین دفاع در برابر نرم افزارهای مخرب اجرای نرم افزارهای آنتی ویروس و ضد بد افزار است، که امروزه بیشتر فروشندگان این دو نوع نرم افزار را در همان آنتی ویروس و ضد بد افزار بسته بندی می کنند. به روز ماندن نرم افزارهای آنتی ویروس و ضد بد افزار بسیار مهم است، که شامل اطمینان از نصب آخرین تعریف ویروس و بد افزار است.

✓ جعل Spoofing

جعل، همچنین به آن تغییر قیافه Masquerading نیز گفته می شود، هنگامی که به نظر می رسد ارتباط یک مهاجم از منابع معتبر حاصل می شود. نمونه های جعل شامل جعل IP و جعل لینک می باشد. هدف از این نوع حمله دستیابی به اطلاعات معتبر یا سایر اطلاعات شخصی است. یک حمله Man-in-the-Middle، از جعل به عنوان بخشی از حمله استفاده می کند. برخی از متخصصان امنیت حملات فیشینگ را نوعی حمله جعل Spoofing قلمداد می کنند.

✓ خرابکاری و استراق سمع Sniffing and Eavesdropping

Sniffing، همچنین به عنوان استراق سمع از آن یاد می شود، وقتی مهاجمی وسیله یا نرم افزاری را در رسانه ارتباطی وارد کرده و تمام اطلاعات منتقل شده از طریق رسانه را جمع آوری کند. اسنیفرهای شبکه توسط متخصصان قانونی و مهاجمین استفاده می شوند. سازمان ها باید نظارت داشته باشد و استفاده از اسنیفرها را محدود کنند. برای محافظت در برابر استفاده از آنها، باید تمام ترافیک موجود در شبکه رمزگذاری شود.

✓ ساطع (انتشار) Emanating

سیگنال های الکترومغناطیسی هستند که توسط یک دستگاه الکترونیکی ساطع می شوند (انتشار می یابند). مهاجمان می توانند برخی از وسایل یا رسانه انتقال را هدف قرار دهند تا بدون دسترسی فیزیکی به دستگاه و یا رسانه، ارتباط برقرار کنند. برنامه TEMPEST که توسط ایالات متحده و انگلیس آغاز شد، روشهای محدود کردن انتشار و استاندارد سازی فن آوری های مورد استفاده را بررسی می کند. هرگونه تجهیزات مطابق با استانداردهای TEMPEST، انتشار سیگنال را با استفاده از مواد محافظ سرکوب می کند. دستگاه هایی که مطابق با استانداردهای TEMPEST هستند، معمولاً یک مانع بیرونی یا روکش را، به نام قفس فارادی Faraday cage یا محافظ فارادی Faraday shield اجرا می کنند. دستگاه های TEMPEST اغلب در دولت، ارتش یا اجرای قانون استفاده می شوند.

Backdoor / Trapdoor ✓

مکانیزمی است که در بسیاری از دستگاه‌ها یا اپلیکیشن‌ها اجرا می‌شود و به کاربری داده می‌شود که از دسترسی نامحدود به دستگاه یا اپلیکیشن استفاده می‌کند. حساب‌های اختصاصی رایج ترین روش Backdoor است که امروزه مشاهده می‌شود. بیشتر فروشندگان مقرر دستگاه یا اپلیکیشن‌هایی را با این مشکل امنیتی منتشر نمی‌کنند. باید توجه داشت همیشه باید از پشتیبان شناخته شده در دستگاه‌ها یا اپلیکیشن‌های مدیریتی خود آگاه باشید.

جلوگیری یا کاهش تهدیدات کنترل دسترسی Prevent or Mitigate Access Control Threats

از آنجا که تهدیدات کنترل دسترسی بسیار گسترده است، سازمان‌ها باید تمام تلاش خود را برای محافظت از سیستم‌های کنترل دسترسی انجام دهند، از جمله استقرار ضد بدافزار، فایروال‌ها، تشخیص و جلوگیری از نفوذ و سایر ابزارهای دفاعی. متخصصان امنیت باید سازمان‌های خود را ترغیب کنند تا اقدامات زیر را برای جلوگیری یا کاهش تهدیدهای کنترل دسترسی اعمال کنند:

- کنترل‌های دسترسی فیزیکی برای همه سیستم‌ها و دستگاه‌ها مستقر شود.
- کنترل و نظارت بر دسترسی به فایل‌های گذرواژه.
- رمزگذاری فایل‌های گذرواژه.
- استقرار یک سیاست گذرواژه قوی در سراسر شرکت.
- در تمام سیستم عامل‌ها و اپلیکیشن‌ها، ماسک یا روکش گذرواژه نصب شود.
- احراز هویت چند عاملی.
- استقرار قفل حساب.
- استقرار ممیزی را برای کنترل دسترسی.
- برای اطمینان از ایجاد و حذف حساب‌های کاربری در صورت لزوم، از یک سیاست مدیریت حساب کاربری استفاده شود.
- آموزش آگاهی درباره امنیت کاربر ارائه شود که به طور خاص روی کنترل دسترسی متمرکز است.

فصل ۶

ارزیابی و آزمون امنیت
(Security Assessment and Testing)

این فصل موضوعات زیر را در بر می گیرد:

- ❖ استراتژی های ارزیابی و آزمون Assessment and Testing Strategies: استفاده از استراتژی های ارزیابی و آزمون را توضیح می دهد.
 - ❖ آزمون کنترل امنیت Security Control Testing: مفاهیم مورد بحث شامل فرآیند آزمون کنترل امنیتی، از جمله ارزیابی آسیب پذیری، تست های نفوذ، بررسی log، تراکنش های مصنوعی، بررسی و تست کد، تست موارد سوءاستفاده، تجزیه و تحلیل پوشش تست و تست واسط است.
 - ❖ جمع آوری داده های فرآیند امنیت Collect Security Process Data: مفاهیم مورد بحث شامل NIST SP 800-137، مدیریت حساب، بررسی مدیریت، عملکرد اصلی و شاخص های ریسک، داده های تأیید نسخه پشتیبان، آموزش و آگاهی، بهبود فاجعه و تداوم کسب و کار است.
 - ❖ تجزیه و تحلیل و گزارش نتایج آزمون Analyze and Report Test Outputs: اهمیت تحلیل و گزارش خروجی های آزمون از جمله گزارش های خودکار و دستی را توضیح می دهد.
 - ❖ ممیزی داخلی و شخص ثالث Internal and Third-Party Audit: روند ممیزی و سه نوع گزارش SOC را توصیف می کند.
- ارزیابی و آزمون امنیت شامل طراحی، انجام و تجزیه و تحلیل تست های امنیتی است. متخصصان امنیت برای محافظت از دارایی های خود در برابر حملات باید این فرایندها را درک کنند.
- ارزیابی و آزمون امنیت برای تعیین آسیب پذیری ها و ریسک های سازمان به تعدادی روش آزمون نیاز دارد. این ارزیابی و آزمون امنیت، یک سازمان را در مدیریت ریسک ها در برنامه ریزی، استقرار، بهره برداری و نگهداری سیستم ها و فرایندها یاری می کند. هدف آن شناسایی هرگونه نقص فنی، نقص عملیاتی و نقص سیستم در اوایل مراحل، قبل از استقرار این نقص ها می باشد.
- هرچه زودتر بتوانید آن نواقص را کشف کنید، رفع آنها ارزان تر است.
- در این فصل استراتژی های ارزیابی و آزمون، آزمون کنترل امنیت، جمع آوری داده های فرآیند امنیت، تجزیه و تحلیل و گزارش نتایج آزمون ها و ممیزی های داخلی و شخص ثالث مطرح شده است.

استراتژی‌های ارزیابی و آزمون Assessment and Testing Strategies

متخصصان امنیت باید مطمئن شوند که سازمان طرح‌ها، طراحی‌ها، اجراها و راهکارهای ارزیابی و آزمون مناسب را تأیید می‌کند تا از کاهش ریسک‌ها مطمئن شوند. متخصصان امنیت باید نقش اصلی را در کمک به سازمان در اجرای استراتژی‌های آزمون و ارزیابی امنیتی مناسب داشته باشند. سازمان باید به بهترین شیوه‌های صنعت، استانداردهای ملی و بین‌المللی و رویه‌ها و دستورالعمل‌هایی که از طرف فروشندگان توصیه می‌شود، تکیه کند. تا استراتژی‌ها بطور مناسب برنامه ریزی و اجرا شوند.

سازمانها به احتمال زیاد تیمی را تشکیل می‌دهند که مسئولیت اجرای هرگونه استراتژی ارزیابی و آزمون را بر عهده خواهد داشت. این تیم باید از افرادی تشکیل شده باشد که ارزیابی و آزمون امنیت را درک می‌کنند و باید نمایندگانی از سایر مناطق سازمان نیز حضور داشته باشند. تأیید و اعتبار سنجی امنیت یک فعالیت در حال انجام است که هرگز متوقف نمی‌شود. اما متخصصان امنیت باید از نظر زمانی که نوع خاصی از ارزیابی یا آزمون که به بهترین نحو انجام می‌شود، سازمان را راهنمایی کنند.

آزمون کنترل امنیت Security Control Testing

سازمانها باید آزمون کنترل امنیت را که انجام می‌شود، کنترل کنند تا مطمئن شوند که کلیه کنترل‌های امنیتی توسط افراد مجاز آزمایش شده است. جنبه‌های آزمون کنترل امنیتی که سازمان‌ها باید شامل آن‌ها باشند شامل ارزیابی آسیب پذیری، تست‌های نفوذ، بررسی‌های ورود به سیستم، تراکنش‌های مصنوعی، بررسی و تست کد، تست موارد سوءاستفاده، تجزیه و تحلیل پوشش تست و تست واسط هستند.

ارزیابی آسیب پذیری Vulnerability Assessment

ارزیابی آسیب پذیری به شناسایی مناطق ضعیف در یک شبکه کمک می‌کند. همچنین می‌تواند به تعیین اولویت بندی دارایی در سازمان کمک کند. ارزیابی جامع آسیب پذیری بخشی از فرآیند مدیریت ریسک است. اما برای کنترل دسترسی، متخصصان امنیت باید از ارزیابی آسیب پذیری استفاده کنند که به طور خاص مکانیسم‌های کنترل دسترسی را هدف قرار می‌دهد. ارزیابی آسیب پذیری معمولاً در یکی از سه دسته زیر قرار می‌گیرد:

✓ آزمون پرسنل Personnel testing: شیوه های استاندارد و رویه هایی را که کاربران دنبال می کنند بررسی می کند.

✓ آزمون های فیزیکی Physical testing: بررسی امکانات و حفاظت از محیط.

✓ تست سیستم و شبکه System and network testing: سیستم ها، دستگاه ها و توپولوژی شبکه را بررسی می کند.

تحلیلگر امنیت Security analyst که ارزیابی آسیب پذیری را انجام خواهد داد، باید سیستم ها و دستگاه های موجود در شبکه و کارهایی که انجام می دهد را درک کند. تحلیلگر به این اطلاعات نیاز دارد تا بتواند آسیب پذیری سیستم ها و دستگاه ها را بر اساس تهدیدهای شناخته شده و احتمالی سیستم ها و دستگاه ها ارزیابی کند.

پس از کسب دانش در مورد سیستم ها و دستگاه ها، تحلیلگر امنیت باید کنترل های موجود را بررسی کرده و هرگونه تهدید علیه این کنترل ها را شناسایی کند. سپس تحلیلگر امنیت می تواند از تمام اطلاعات جمع آوری شده برای تعیین اینکه کدام ابزار خودکار برای جستجوی آسیب پذیری ها بکار برده می شود، استفاده کند. پس از اتمام تجزیه و تحلیل آسیب پذیری، تحلیلگر امنیت باید نتایج را تأیید کند تا از صحت آنها مطمئن شود و سپس یافته ها را با پیشنهادات مربوط به اقدامات چاره ساز به مدیریت گزارش دهد. با استفاده از این اطلاعات، تحلیلگر باید مدل تهدید را پیش برده تا بتواند تهدیداتی که بر سیستم ها و دستگاه ها و روشهای حمله ای که می تواند مورد استفاده قرار بگیرد و تأثیر منفی بگذارد، را شناسایی کند.

اپلیکیشن های ارزیابی آسیب پذیری شامل Nessus، سیستم ارزیابی آسیب پذیری باز Vulnerability Assessment System (OpenVAS)، Core Impact، Nexpose، GFI، LanGuard، QualysGuard و Analyser Security Baseline Security (MBSA) هستند. از بین این اپلیکیشن ها، OpenVAS و MBSA رایگان هستند.

هنگام انتخاب ابزار ارزیابی آسیب پذیری، باید معیارهای زیر را مورد بررسی قرار دهید: دقت Accuracy، قابلیت اطمینان Reliability، مقیاس پذیری Scalability و گزارش دهی Reporting. دقت مهمترین معیار می باشد. مثبت کاذب False positiv به طور کلی منجر به صرف زمان تحقیق در مورد موضوعی می شود که وجود ندارد. یک منفی کاذب False negative جدی تر است، زیرا این بدان معنی است که اسکنر نتوانسته است مسئله ای که ریسک های امنیتی جدی را در پی دارد، شناسایی کند.

تست نفوذ Penetration Testing

هدف از تست نفوذ، که به عنوان یک اخلاقی نیز شناخته می‌شود، شبیه سازی یک حمله برای شناسایی تهدیداتی است که می‌تواند ناشی از برنامه ریزی منابع داخلی یا خارجی برای بهره برداری از آسیب پذیری‌های یک سیستم یا دستگاه باشد.

مراحل انجام تست نفوذ به شرح زیر است:

- ۱- اطلاعات مربوط به سیستم یا دستگاه مورد نظر را مستند کنید.
 - ۲- اطلاعات در مورد روش‌های حمله در برابر سیستم یا دستگاه هدف را جمع آوری کنید، که شامل انجام اسکن پورت می‌باشد.
 - ۳- نقاط ضعف شناخته شده سیستم یا دستگاه هدف را شناسایی کنید.
 - ۴- برای بدست آوردن دسترسی کاربر و دسترسی ممتاز، حملات را علیه سیستم یا دستگاه هدف انجام دهید.
 - ۵- نتایج تست نفوذ را مستند سازی کنید و یافته‌ها را به مدیریت گزارش دهید، اقدامات احتمالی را برای اقدامات چاره ساز انجام دهید.
- هر دو تست داخلی و خارجی باید انجام شود. تست‌های داخلی از درون شبکه اتفاق می‌افتد، در حالی که تست‌های خارجی در خارج از شبکه منشا گرفته و سرورها و دستگاه‌هایی را که در معرض دید عموم قرار دارند هدف قرار می‌دهند.
- استراتژی‌های تست نفوذ مبتنی بر اهداف تست تعریف شده توسط سازمان است. راهکارهایی که باید با آنها آشنا باشید شامل موارد زیر است:

- تست کور Blind test: تیم تست، دانش محدودی در مورد سیستم‌ها و دستگاه‌های شبکه را از اطلاعات در دسترس عموم فراهم کرده است. تیم امنیت سازمان می‌داند که حمله در حال وقوع است. این تست به تلاش بیشتری توسط تیم تست نیاز دارد و تیم باید یک حمله واقعی را شبیه سازی کند.
- تست کوردوگانه Double-blind test: این تست مانند یک تست کور است به جز تیم امنیتی سازمان هیچکس نمی‌داند که حمله‌ای انجام شده است. فقط تعداد معدودی از افراد سازمان از این حمله خبر دارند و آنها این اطلاعات را با تیم امنیت به اشتراک نمی‌گذارند. این تست معمولاً نیاز به تلاش مساوی تیم تست و تیم امنیت سازمان دارد.

- تست هدف Target test: به تیم تست و تیم امنیت سازمان حداکثر اطلاعات در مورد شبکه و نوع حمله‌ای که رخ خواهد داد، داده می‌شود. این ساده ترین تست برای تکمیل شدن است اما تصویر کاملی از امنیت سازمان ارائه نمی‌دهد.
- تست نفوذ نیز بر اساس میزان اطلاعاتی که باید ارائه شود، به دسته بندی هایی تقسیم می‌شود. دسته‌های اصلی که باید با آنها آشنا شوید شامل موارد زیر است:
 - آزمون دانش صفر Zero-knowledge test: به تیم تست، اطلاعاتی درباره شبکه سازمان داده نمی‌شود. تیم تست می‌تواند از هر وسیله موجود برای بدست آوردن اطلاعات در مورد شبکه سازمان استفاده کند. همچنین به این تست بسته یا جعبه سیاه نیز گفته می‌شود.
 - آزمون دانش جزئی Partial-knowledge test: به تیم تست دانش عمومی در مورد شبکه سازمان ارائه می‌شود. ممکن است مرزها برای این نوع تست تعیین شود.
 - آزمون آگاهی کامل Full-knowledge test: به تیم تست دانش کلی در مورد شبکه سازمان ارائه می‌شود. این تست بیشتر بر روی حملات متمرکز است.
- اپلیکیشن‌های تست نفوذ شامل Nessus، Core Impact، Wireshark، Metasploit، BackTrack، Cain & Abel، Kali Linux، John Ripper هستند. هنگام انتخاب یک ابزار تست نفوذ، ابتدا باید سیستم هایی که می‌خواهید تست کنید، مشخص شوند. سپس درمورد ابزارهای مختلف تحقیق کرده تا بفهمید که آیا می‌توانید تست هایی را برای آن سیستم‌ها انجام دهید و اصول ابزار برای تست را جستجو کنید. علاوه بر این، سازمان برای انجام تست باید فرد صحیحی را انتخاب کند. به خاطر داشته باشید که تست‌های نفوذ باید شامل روش‌های دستی و همچنین روش‌های خودکار باشند زیرا اتکا تنها به یکی از این دو مورد نتیجه کاملی از حمله را نخواهد داد. این ساده ترین تست برای تکمیل شدن می‌باشد اما تصویر کاملی از امنیت سازمان ارائه نمی‌دهد.
- جدول ۶-۱ ارزیابی آسیب پذیری و تست‌های نفوذ را مقایسه می‌کند.

	Vulnerability Assessment	Penetration Test
Purpose	Identifies vulnerabilities that may result in compromise of a system.	Identifies ways to exploit vulnerabilities to circumvent the security features of systems.
When	After significant system changes. Schedule at least quarterly thereafter.	After significant system changes. Schedule at least annually thereafter.
How	Use automated tools with manual verification of identified issues.	Use both automated and manual methods to provide a comprehensive report.
Reports	Potential risks posed by known vulnerabilities, ranked using base scores associated with each vulnerability. Both internal and external reports should be provided.	Description of each issue discovered, including specific risks the issue may pose and specifically how and to what extent it may be exploited.
Duration	Typically several seconds to several minutes per scanned host.	Days or weeks, depending on the scope and size of the environment to be tested. Tests may grow in duration if efforts uncover additional scope.

جدول ۶-۱: مقایسه ارزیابی‌های آسیب‌پذیری و تست‌های نفوذ

بررسی‌های log

log ضبط وقایعی است که در یک دارایی سازمانی رخ می‌دهد، از جمله سیستم‌ها، شبکه‌ها، دستگاه‌ها و تاسیسات.

هر ورودی در یک Log یک رخداد واحد Single event را پوشش می‌دهد که روی دارایی رخ می‌دهد. در بیشتر موارد، log‌های جداگانه‌ای برای انواع مختلف رخدادها، از جمله log‌های مربوط به امنیت، log‌های مربوط به سیستم عامل و log‌های مربوط به اپلیکیشن وجود دارد. از آنجا که بسیاری از log‌ها، بر روی یک دستگاه واحد ایجاد می‌شود، بسیاری از سازمان‌ها برای اطمینان از بررسی log‌های به موقع، مشکل دارند. با این حال، بررسی log‌ها احتمالاً یکی از مهمترین اقداماتی است که یک سازمان می‌تواند برای اطمینان از شناسایی موضوعات قبل از تبدیل شدن به مشکلات اساسی، انجام دهد.

Logهای امنیتی رایانه از اهمیت ویژه‌ای برخوردار هستند زیرا می‌توانند به یک سازمان در شناسایی حوادث امنیتی، نقض خط مشی و کلاهبرداری کمک کنند. مدیریت logها اطمینان می‌دهد که logهای مربوط به امنیت رایانه برای یک دوره زمانی مناسب با جزئیات کافی ذخیره می‌شوند تا ممیزی، تجزیه تحلیل قانونی، تحقیقات، خط مبنا ها، روندها و مشکلات بلند مدت مشخص شوند.

انستیتوی ملی استاندارد و فناوری یا National Institute of Standards and Technology (NIST) دو نشریه ویژه ارائه داده است که مربوط به مدیریت ورود به سیستم هستند: NIST SP 800-92، "راهنمای مدیریت ورود به سیستم امنیت رایانه"، و NIST SP 800-137، "نظارت مداوم بر امنیت اطلاعات" یا Information Security Continuous Monitoring (ISCM) برای سیستم‌ها و سازمان‌های اطلاعاتی فدرال (هم پیمان). در حالی که هر دو انتشارات ویژه در درجه اول توسط سازمانها و سازمانهای دولتی فدرال مورد استفاده قرار می‌گیرند، سازمانهای دیگر ممکن است بخاطر سرمایه اطلاعاتی که ارائه می‌دهند بخواهند آن دو نشریه را بکار گیرند. بخش زیر NIST SP 800-92 را پوشش می‌دهد، و NIST SP 800-137 بعداً در این فصل مورد بحث خواهد گرفت.

NIST SP 800-92 برای مدیریت کارآمدتر و موثرتر log توصیه‌های زیر را ارائه می‌دهد:

- سازمان‌ها باید سیاست‌ها و رویه‌هایی را برای مدیریت log ایجاد کنند. به عنوان بخشی از فرایند برنامه ریزی، یک سازمان باید:
 - ✓ شرایط و اهداف log را تعریف کنند.
 - ✓ سیاست‌هایی را تدوین کنند که الزامات اجباری را به روشنی تعریف کرده و توصیه‌هایی را برای فعالیت‌های مدیریت logهای مربوط ارائه دهد.
 - ✓ اطمینان حاصل کنند که سیاست‌ها و رویه‌های مربوطه الزامات و توصیه‌های مربوط به مدیریت log را گنجانیده و پشتیبانی می‌کند.
 - ✓ مدیریت باید پشتیبانی لازم را برای اقدامات مربوط به برنامه ریزی، مدیریت سیاست‌ها و تدوین مراحل مدیریت انجام دهد:
- سازمانها باید مدیریت log را در کل سازمان به طور مناسب در اولویت قرار دهند.
- سازمانها باید زیرساختهای مدیریت log را ایجاد و حفظ کنند.
- سازمانها باید برای کلیه کارکنان دارای مسئولیت‌های مدیریت log، پشتیبانی مناسب را ارائه دهند.

- سازمانها باید فرآیندهای عملیاتی مدیریت log استاندارد را ایجاد کنند، که شامل اطمینان از این است که ادمین ها:
 - نظارت بر وضعیت log از تمام منابع log.
 - فرآیندهای چرخش log و بایگانی را کنترل کنند.
 - برای بروزرسانی نرم افزار و بدست آوردن، تست و استقرار آنها، بروزرسانی ها و پچ ها را بررسی کنند.
 - اطمینان حاصل کنند که ساعت میزبان log همزمان با یک منبع زمان مشترک است.
 - در صورت لزوم بر اساس تغییرات سیاست، تغییرات فناوری و سایر عوامل، log را مجدداً پیکربندی کنند.
 - ناهنجاری ها را در تنظیمات log، پیکربندی های log و فرآیندهای log گزارش کنند.
- مطابق با این انتشار، مؤلفه های زیرساخت مدیریت log رایج شامل کارکرد کلی (تجزیه log، فیلتر کردن رخداد و جمع آوری رخداد)، ذخیره سازی (چرخش log، بایگانی log، کاهش log، تبدیل log، نرمال سازی log و بررسی یکپارچگی فایل log)، تجزیه و تحلیل log (همبستگی رخداد، مشاهده log و گزارش log) و دفع log (پاکسازی log).
- Syslog یک چارچوب ساده برای تولید، ذخیره سازی و ورود log را برای سیستم فراهم می کند که هر سیستم عامل، نرم افزار امنیتی یا اپلیکیشن در صورت طراحی برای انجام این کار می تواند استفاده کند. بسیاری از منابع log یا از syslog به عنوان فرمت log محلی خود استفاده می کنند و یا ویژگی هایی را ارائه می دهند که باعث می شود فرمت های log آنها به فرمت syslog تبدیل شوند. هر پیام syslog تنها سه بخش دارد. بخش اول تاسیسات و شدت را به عنوان مقادیر عددی مشخص می کند. بخش دوم پیام حاوی یک زمان سنج و نام میزبان یا آدرس IP منبع گزارش است. بخش سوم محتوای پیام واقعی log است.
- هیچ فیلد استاندارد در محتوای پیام تعریف نشده است و اینگونه در نظر گرفته شده است که قابل خواندن توسط انسان باشد و به راحتی قابل تجزیه و تحلیل ماشین نیست. این قابلیت انعطاف پذیری بسیار بالایی را برای تولید کنندگان log فراهم می کند، که می تواند اطلاعاتی را که از نظر آنها مهم تلقی می شود در قسمت محتوا قرار دهند، اما تجزیه و تحلیل خودکار داده های log را بسیار چالش برانگیز می کند. ممکن است یک منبع واحد از فرمت های مختلفی برای محتوای پیام log استفاده کند، بنابراین یک برنامه تجزیه و تحلیل باید با هر فرمت آشنا باشد و بتواند معنی داده ها را در قسمت های هر فرمت استخراج کند. وقتی پیام های log توسط بسیاری

از منابع ایجاد می شوند، این مشکل بسیار چالش برانگیز می شود. ممکن است درک معنای همه پیام های log امکان پذیر نباشد، بنابراین ممکن است تجزیه و تحلیل به جستجوی کلمات کلیدی و الگو محدود شود. برخی سازمانها زیرساخت های syslog خود را به گونه ای طراحی می کنند که انواع مشابهی از پیامها در کنار هم گروه بندی شده یا کدهای مشابهی را به آنها اختصاص می دهند، که می تواند اتوماسیون تجزیه و تحلیل log را آسانتر کند.

از آنجا که امنیت log تبدیل به دغدغه بیشتری شده است، چندین پیاده سازی syslog ایجاد شده اند که تأکید بیشتری بر امنیت می کند. بیشتر اینها براساس IETF's RFC 3195 ساخته شده است، که به طور خاص برای بهبود امنیت syslog طراحی شده است. پیاده سازی مبتنی بر این استاندارد می تواند محرمانه بودن، یکپارچگی و در دسترس بودن log را از طریق چندین ویژگی از جمله تحویل معتبر log، حفاظت از محرمانه بودن انتقال و حفاظت از یکپارچگی انتقال و تأیید صحت انتقال پشتیبانی کند.

اطلاعات مربوط به مدیریت رخداد و اطلاعات امنیت Security information and event management (SIEM) به ادمین ها اجازه می دهد تا همه Log های اطلاعات امنیتی را متحد کنند. این اتحاد تضمین می کند که ادمین ها بتوانند به جای اینکه مجبور به تجزیه و تحلیل هر یک از منابع روی منابع جداگانه خود باشند، بر روی تمام log های مربوطه تجزیه و تحلیل انجام دهند. بیشتر محصولات SIEM از دو روش جمع آوری log های مربوط به ژنراتورهای log پشتیبانی می کنند:

✓ بدون عامل Agentless سرور SIEM داده ها را از میزبان های شخصی دریافت می کند بدون اینکه نیازی به نصب نرم افزار خاصی روی آن میزبان ها باشد. بعضی از سرورها log های مربوط به میزبان ها را می کشند یا هل می دهند، که این کار معمولاً با احراز هویت سرور به هر میزبان انجام می شود و مرتباً log های مربوط به آن را بازایی می کنند. در موارد دیگر، میزبان ها log های مربوط به خود را به سمت سرور سوق می دهند، که معمولاً شامل هر میزبان است که سرور احراز هویت کرده و به طور مرتب log های خود را منتقل می کند. صرف نظر از اینکه log ها را هل داده یا کشیده، سرور سپس عملیات فیلتر کردن رخداد و جمع کردن را انجام می دهد و نرمال سازی و تجزیه و تحلیل log ها را از روی log های مربوطه جمع آوری می کند.

✓ مبتنی بر عامل Agent-based یک برنامه عامل برای انجام فیلترگذاری رخداد و جمع آوری رخداد و نرمال سازی log برای نوع خاصی از log روی میزبان نصب می شود.

میزبان سپس اطلاعات log نرمال را به سرور SIEM، معمولاً به صورت زمان واقعی یا نزدیک به زمان واقعی برای تجزیه و تحلیل و ذخیره، انتقال می‌دهد. میزبان در صورت داشتن انواع مختلفی از علائم مورد علاقه، ممکن است لازم باشد چندین عامل نصب کند. برخی از محصولات SIEM همچنین نماینده‌هایی برای فرمت‌های عمومی مانند syslog و پروتکل مدیریت شبکه ساده یا SNMP ارائه می‌دهند. یک عامل عمومی در درجه اول برای بدست آوردن اطلاعات log از منبعی استفاده می‌کند، که یک عامل با فرمت خاص و یک روش بدون عامل در دسترس نیست. برخی از محصولات همچنین به ادمین‌ها این امکان را می‌دهند تا عوامل مربوط به منابع log را پشتیبانی نکنند.

برای هر روش مزایا و مضراتی وجود دارد. مزیت اصلی رویکرد بدون عامل این است که عامل‌ها لازم نیست که روی هر میزبان log، نصب، پیکربندی و نگهداری شوند. نقطه ضعف اصلی، عدم فیلتر و جمع شدن در سطح میزبان فردی است که می‌تواند باعث انتقال مقادیر قابل توجهی داده‌ها از طریق شبکه‌ها شود و مدت زمان لازم برای فیلتر و تجزیه و تحلیل logها را افزایش دهد. یکی دیگر از معایب احتمالی روش بدون عامل این است که سرور SIEM ممکن است برای احراز هویت برای هر میزبان log، به اعتبارنامه نیاز داشته باشد. در برخی موارد، تنها یکی از دو روش امکان پذیر است. به عنوان مثال، ممکن است بدون نصب عامل Agent روی آن، راهکاری برای جمع‌آوری logها از یک میزبان خاص وجود نداشته باشد.

محصولات SIEM معمولاً شامل پشتیبانی از دهها منبع log مانند OS، نرم افزارهای امنیتی، سرورهای اپلیکیشن (مانند سرورهای وب، سرورهای ایمیل) و حتی دستگاههای کنترل امنیت فیزیکی مانند نشانه خواننده Badge Reader می‌باشند. برای هر نوع منبع log پشتیبانی شده، به جز فرمت‌های عمومی مانند syslog، محصولات SIEM به طور معمول می‌دانند که چگونه مهمترین فیلدهای وارد شده را طبقه بندی کنند.

این امر به طور قابل توجهی نرمال سازی، تجزیه و تحلیل و همبستگی داده‌های log را با درک کمتری از منابع و فرمت‌های log خاص انجام می‌دهد. همچنین، نرم افزار SIEM می‌تواند با عدم توجه به فیلدهای داده که برای امنیت رایانه دارای اهمیت نیستند، کاهش رخداد را انجام دهد که به طور بالقوه باعث کاهش پهنای باند شبکه نرم افزار SIEM و استفاده از ذخیره سازی داده‌ها می‌شود.

به طور معمول، ادمین‌های سیستم، ادمین‌های شبکه و ادمین‌های امنیت مسئولیت مدیریت log بر روی سیستم‌های خود، انجام تجزیه و تحلیل منظم داده‌های log، اسناد و گزارش نتایج

فعالیت های مدیریت log خود را دارند و تضمین می کنند که داده های log به زیرساخت های مدیریت log در سازمان ارائه می شود. مطابق با سیاست های سازمان علاوه بر این، برخی از ادمین های امنیت سازمان به عنوان مدیر زیرساخت های مدیریت log مسئولیت هایی مانند موارد زیر را پوشش می دهند:

- برای بدست آوردن اطلاعات بیشتر در مورد یک رخداد یا درخواست تحقیق درباره یک رخداد خاص، با ادمین های سطح سیستم تماس می گیرند.
- تغییرات مورد نیاز برای پیکربندی های log را مشخص می کنند (به عنوان مثال، ورودی ها و فیلدهای داده به سرورهای ثبت متمرکز ارسال می شوند که از چه روشی باید استفاده شود) و تغییرات لازم را به ادمین های سطح سیستم اطلاع می دهند.
- پاسخ به رخدادها، از جمله رسیدگی به حادثه و مشکلات عملیاتی را شروع می کنند (به عنوان مثال، عدم موفقیت یک مؤلفه زیرساخت مدیریت log).
- اطمینان حاصل می کنند که داده های log قدیمی بایگانی شده در رسانه ها قابل جابجایی بوده و پس از آنکه دیگر نیازی به آن نباشد، به درستی آنها را از خود دور می کنند.
- با درخواست های مشاور حقوقی، ممیزان و دیگران همکاری می کنند.
- نظارت بر وضعیت زیرساخت های مدیریت log (به عنوان مثال، عدم موفقیت در ورود به نرم افزار یا رسانه بایگانی log، عدم موفقیت سیستم های محلی برای انتقال داده های log آنها) و در صورت بروز مشکلات پاسخ های مناسب بدهند.
- برورسانی ها و بهبودهای مؤلفه های زیرساخت مدیریت log را تست و پیاده سازی می کنند.
- حفظ امنیت زیرساخت های مدیریت log.

سازمانها باید سیاستی را تدوین کنند که به طور واضح الزامات اجباری را مشخص کند و توصیفاتی را برای چندین جنبه از مدیریت log ارائه دهند، از جمله تولید log، انتقال log، ذخیره سازی و دفع log و تجزیه و تحلیل log در جدول ۶-۲ نمونه هایی از تنظیمات پیکربندی log که یک سازمان می تواند از آنها استفاده کند، آورده شده است. انواع مقادیر تعریف شده در جدول ۶-۲ فقط باید برای میزبان ها و اجزای میزبان که قبلاً توسط سازمان مشخص شده، به عنوان مواردی که باید وقایع مربوط به امنیت log باشند اعمال شده است.

Category	Low-Impact Systems	Moderate-Impact Systems	High-Impact Systems
Log retention duration	1–2 weeks	1–3 months	3–12 months
Log rotation	Optional (if performed, at least every week or every 25 MB)	Every 6–24 hours or every 2–5 MB	Every 15–60 minutes or every 0.5–1.0 MB
Log data transfer frequency (to SIEM)	Every 3–24 hours	Every 15–60 minutes	At least every 5 minutes
Local log data analysis	Every 1–7 days	Every 12–24 hours	At least 6 times a day
File integrity check for rotated logs?	Optional	Yes	Yes
Encrypt rotated logs?	Optional	Optional	Yes
Encrypt log data transfers to SIEM?	Optional	Yes	Yes

جدول ۶-۲: نمونه هایی از گزارشات تنظیمات ورود به سیستم

تراکنشهای مصنوعی Synthetic Transactions

نظارت بر تراکنشهای مصنوعی، که نوعی نظارت فعال است، اغلب برای وب سایتها و اپلیکیشنها ترجیح داده می شود. قبل از اینکه کاربران از تخریب رفتار اپلیکیشن استفاده کنند، این بینش در دسترس بودن و عملکرد یک اپلیکیشن فراهم می شود و درباره هر مسئله بالقوه هشدار می دهد. و از عوامل خارجی برای اجرای تراکنشهای نوشته شده در برابر یک اپلیکیشن استفاده می کند. به عنوان مثال، مدیر عملیات مرکز سیستم مایکروسافت از تراکنشهای مصنوعی برای نظارت بر پایگاه داده ها، وب سایتها و استفاده از پورت TCP استفاده می کند.

در مقابل، نظارت کاربر واقعی (Real User Monitoring (RUM)، که نوعی نظارت منفعل Passive Monitoring است، هر تراکنش از هر اپلیکیشن یا کاربر وب سایت را ضبط و تجزیه و تحلیل می کند. بر خلاف نظارت مصنوعی، که سعی می کند با آزمایش منظم تراکنشهای مصنوعی، بینش عملکردی بدست آورد، RUM با دیدن دقیقاً نحوه تراکنشهای کاربران با اپلیکیشن، حدس و گمان را کاهش می دهد.

تست و بررسی کد Code Review and Testing

تست و بررسی کد باید در کل چرخه حیات توسعه سیستم یا اپلیکیشن انجام شود. هدف از تست و بررسی کد شناسایی الگوهای بد برنامه نویسی، تنظیمات غلط امنیتی، اشکالات عملکردی و نقص منطقی است.

در مرحله برنامه ریزی و طراحی، تست و بررسی کد شامل بررسی های امنیتی معماری و مدل سازی تهدید است. در مرحله توسعه، تست و بررسی کد شامل تجزیه و تحلیل کد منبع ایستا Static source code analysis، بررسی کد دستی Manual code review، تجزیه و تحلیل کد باینری استاتیک یا ایستا و بررسی باینری دستی است. پس از استقرار اپلیکیشن، تست و بررسی کد شامل تست نفوذ، اسکن آسیب پذیری و تست فازی می باشد.

بررسی کد رسمی Formal code review شامل یک فرایند دقیق همراه جزئیات با شرکت کنندگان و مراحل مختلف است. در این نوع بررسی کد، توسعه دهندگان نرم افزار در جلساتی شرکت می کنند که در آن هر خط کد بررسی می شود و معمولاً از نسخه های چاپی استفاده می شود. بررسی کد سبک Lightweight code review معمولاً نیاز به سر بار کمتری نسبت به بازرسی های کد رسمی دارد، اگرچه در صورت انجام صحیح می تواند به همان اندازه مؤثر باشد و موارد زیر را شامل می شود:

- روی شانه Over-the-shoulder: وقتی کدنویس از طریق کد حرکت می کند، یکی از توسعه دهنده ها از نمای روی شانه کدنویس مشاهده می کند.
 - عبور از گذر ایمیل Email pass-around: کد منبع پس از بررسی کد به صورت خودکار به بازرسان ارسال می شود.
 - برنامه نویسی زوجی Pair programming: دو کدنویس در یک ایستگاه کاری یک کد را با هم تهیه می کنند.
 - بررسی کد به کمک ابزار Tool-assisted code review: کدنویسان و بررسی کنندگان از ابزارهایی استفاده می کنند که برای بررسی کد یکسان طراحی شده اند.
- تست جعبه سیاه Black-box وقتی انجام می شود که هیچ جزئیات داخلی سیستم مشخص نیست. تست جعبه سفید White-box در صورت شناخته شدن کد منبع انجام می شود. انواع دیگر تستها شامل تست پویا در مقابل تست ایستا و تست دستی در مقابل تست خودکار می باشد.

تست حالت سوء استفاده Misuse Case Testing

تست حالت سوء استفاده، به آن تست منفی نیز گفته می‌شود، یک اپلیکیشن را آزمایش کرده تا مطمئن شد که اپلیکیشن می‌تواند ورودی نامعتبر یا رفتار غیر منتظره را برطرف کند. این تست به منظور اطمینان از خرابی اپلیکیشن و بهبود کیفیت اپلیکیشن با مشخص کردن نقاط ضعف آن، به پایان می‌رسد. هنگامی که تست حالت سوء استفاده انجام می‌شود، سازمان‌ها باید انتظار داشته باشند که مسائلی را پیدا کنند. تست سوء استفاده باید شامل تست هایی باشد که موارد زیر را دنبال کند:

- فیلدهای مورد نیاز باید جمع آوری شوند.
- فیلد هایی با یک نوع داده تعریف شده فقط می‌توانند داده هایی را که نوع داده مورد نیاز است، بپذیرند.
- فیلدها با کاراکتر محدود فقط به تعدادی کاراکترهای پیکربندی شده اجازه می‌دهد.
- فیلد هایی با دامنه داده تعریف شده فقط داده‌ها را در آن محدوده می‌پذیرند.
- فیلدها فقط داده‌های معتبر را می‌پذیرند.

تجزیه و تحلیل پوشش تست Test Coverage Analysis

تجزیه و تحلیل پوشش تست از حالت‌های تست استفاده می‌کند که براساس مشخصات الزامات اپلیکیشن نوشته شده است. افراد درگیر در این تحلیل نیازی به دیدن کد برای نوشتن حالت‌های تست ندارند. پس از نوشتن سندی که تمام موارد تست را تشریح می‌کند، گروه‌های تست درصدی از موارد زیر می‌باشد:

تستی که اجرا شده، تستی که گذشته، تستی که شکست خورده، تستی که ادامه دارد (run, passed, failed, so on). توسعه دهنده اپلیکیشن معمولاً تجزیه و تحلیل پوشش تست را به عنوان بخشی از تست واحد انجام می‌دهد. گروه‌های تضمین کیفیت از تجزیه و تحلیل پوشش کلی تست برای نشان دادن معیارهای تست و پوشش طبق برنامه ریزی تست استفاده می‌کند. تجزیه و تحلیل پوشش تست، حالت‌های تست اضافی را برای افزایش پوشش ایجاد می‌کند. این امر به توسعه دهندگان کمک می‌کند مناطقی از اپلیکیشن را که توسط مجموعه‌ای از حالت‌های تست استفاده نشده است، پیدا کنند. همچنین کمک می‌کند تا اندازه گیری کمی از پوشش کد، که به طور غیر مستقیم کیفیت اپلیکیشن یا محصول را اندازه گیری می‌کند، تعیین شود.

یکی از معایب اندازه گیری پوشش کد این است که آنچه کد را پوشش می دهد را اندازه گیری می کند اما نمی تواند آنچه را که کد را پوشش نمی دهد یا آنچه که نوشته نشده است را تست کند. علاوه بر این، این تجزیه و تحلیل به ساختار یا عملکردی که از قبل وجود دارد، نگاه می کند، نه آنهایی که هنوز وجود ندارند.

تست واسط Interface Testing

تست واسط ارزیابی می کند که آیا سیستم ها یا مؤلفه های اپلیکیشن به درستی داده ها و کنترل را به یکدیگر منتقل می کنند. این مسئله تأیید می کند که آیا فعل و انفعالات مازول به درستی کار می کنند یا خطاها به درستی اداره می شوند. واسط هایی که باید مورد آزمایش قرار بگیرند شامل واسط های مشتری، واسط های سرور، واسط های از راه دور، واسط های کاربر گرافیکی یا GUI، واسط های برنامه نویسی اپلیکیشن یا API، واسط های خارجی و داخلی و واسط های فیزیکی هستند.

تست GUI محصول برای اطمینان از مطابقت مشخصات آن با استفاده از حالت های تست است. تست API تست های API را بطور مستقیم در ایزوله سازی Isolation و به عنوان بخشی از تراکنش های End-to-End انجام شده در امتداد تست یکپارچه سازی برای تعیین اینکه آیا API پاسخ های صحیح را برگردانده اند، آزمایش می کند.

داده های فرایند امنیت را جمع آوری کنید Collect Security Process Data

پس از تست کنترل های امنیتی، سازمان ها باید مطمئن شوند که داده های مربوط به فرایند امنیت را جمع آوری می کنند. NIST SP 800-137 دستورالعمل هایی را برای تهیه یک برنامه نظارت مداوم بر امنیت اطلاعات (Information security continuous monitoring program) ارائه می دهد. متخصصان امنیت باید مطمئن شوند که داده های فرایند امنیت که جمع آوری شده شامل مدیریت حساب، بررسی مدیریت، شاخص های کلیدی عملکرد و ریسک، داده های تأیید نسخه پشتیبان، آموزش و آگاهی، و بهبود فاجعه و تداوم کسب و کار، می باشد.

NIST SP 800-137

مطابق با NIST SP 800-137، ISCM به عنوان حفظ آگاهی مداوم از امنیت اطلاعات، آسیب پذیری‌ها و تهدیدهای مربوط به پشتیبانی از تصمیمات مدیریت ریسک سازمانی تعریف شده است. سازمان‌ها باید اقدامات زیر را برای ایجاد، پیاده سازی و حفظ ISCM انجام دهند:

- ۱- یک استراتژی ISCM بر اساس تحمل ریسک تعریف شود که دید روشنی از دارایی‌ها، آگاهی از آسیب پذیری‌ها، اطلاعات به روز در مورد تهدید و تأثیرات مأموریت و کسب و کار داشته باشد.
- ۲- یک برنامه ISCM ایجاد شود که شامل معیارها، فرکانس‌های نظارت بر وضعیت، فرکانس‌های کنترل، و یک معماری فنی ISCM باشد.
- ۳- پیاده سازی یک برنامه ISCM و جمع آوری اطلاعات مربوط به امنیت مورد نیاز برای معیارها، ارزیابی‌ها و گزارش‌ها. جمع آوری خودکار، تجزیه و تحلیل خودکار، گزارش خودکار داده‌ها در صورت امکان.
- ۴- تجزیه و تحلیل داده‌های جمع آوری شده، یافته‌های گزارش شده و پاسخ‌های مناسب تعیین شود. جمع آوری اطلاعات اضافی برای واضح بودن یا تکمیل داده‌های نظارت موجود ممکن است ضروری باشد.
- ۵- پاسخ به یافته‌های مربوط به فعالیت‌های فنی، مدیریتی و کاهش فعالیت‌های عملیاتی یا پذیرش، انتقال / به اشتراک گذاری یا اجتناب/ رد کردن.
- ۶- بررسی و بروزرسانی برنامه نظارت، تنظیم استراتژی ISCM و قابلیت اندازه گیری برای افزایش آشکار شدن دارایی‌ها و آگاهی از آسیب پذیری‌ها، امکان کنترل بیشتر داده محور از امنیت زیرساخت‌های اطلاعاتی سازمان و افزایش مقاومت در سازمان.

مدیریت حساب Account Management

مدیریت حساب از آن جهت اهمیت دارد زیرا شامل اضافه و حذف حسابهایی است که به آنها اجازه دسترسی به سیستم‌ها یا شبکه‌ها داده می‌شود. مدیریت حساب همچنین شامل تغییر مجوزها یا امتیازهای اعطا شده به آن حسابها است. در صورت عدم نظارت و مدیریت صحیح حساب، سازمانها ممکن است تشخیص دهند که حسابهایی با هدف انجام فعالیت‌های کلاهبرداری یا مخرب ایجاد شده اند. کنترل‌های دو نفره باید با مدیریت حساب استفاده شود، غالباً با یک

ادمین که حساب کاربری ایجاد می کند و دیگری که مجوزها یا امتیازات مناسب را به آنها اختصاص می دهد.

بالا بردن Escalation و ابطال Revocation دو اصطلاح برای متخصصان امنیت می باشد که اهمیت دارد. بالا بردن حساب در شرایطی اتفاق می افتد که یک حساب کاربری براساس وظایف شغلی جدید یا تغییر شغل کامل مجوز بیشتری دریافت می کند. متخصصان امنیت باید قبل از تغییر مجوزها یا امتیازات فعلی، نیازهای کاربر را به طور کامل تجزیه و تحلیل کنند، مطمئن شوند که فقط مجوزها یا امتیازهایی را که برای کار جدید لازم است اعطا شده و مواردی که دیگر نیازی به آن ندارند، اعطا نکنند. بدون چنین تحلیلی، ممکن است کاربران بتوانند مجوزهایی را که باعث بروز مشکلات امنیتی می شود، حفظ کنند زیرا جدایی وظایف حفظ نشده است. به عنوان مثال، فرض کنید یک کاربر در بخش حساب های قابل پرداخت استخدام شده است تا تمام چک های فروشنده را چاپ کند. بعداً این کاربر ترفیعی را برای تأیید پرداخت برای همان حساب دریافت می کند. اگر مجوز قدیمی این کاربر برای چاپ چک حذف نشود، این کاربر نه تنها می تواند چک ها را تأیید کند بلکه همچنین آنها را چاپ کند، که این یک نقض مستقیم تفکیک وظایف است.

ابطال Revocation حساب وقتی اتفاق می افتد که یک حساب کاربری ابطال شود زیرا کاربر دیگر با سازمان همکاری نمی کند. متخصصان امنیت باید در نظر داشته باشند که اشیایی (objectها) وجود خواهد داشت که به این کاربر تعلق دارند. اگر حساب کاربری به راحتی حذف شود، ممکن است دسترسی به اشیاء متعلق به کاربر از بین برود که ممکن است یک طرح بهتر برای غیرفعال کردن حساب برای یک دوره معین باشد. سیاست های ابطال حساب باید بین ابطال حساب کاربری که از سازمان استعفا می دهد و ابطال حساب کاربری که فسخ شده، تفاوت قائل باشد.

بررسی مدیریت Management Review

بررسی مدیریت داده های فرایند امنیت باید اجباری باشد. مهم نیست که سازمان چقدر فرآیندهای امنیت خود را جمع آوری می کند، اگر هیچگاه توسط یک مدیر مورد بررسی قرار نگیرد، داده ها بی فایده هستند. دستورالعمل ها و رویه ها باید تهیه شود تا تضمین شود که بررسی مدیریت به موقع اتفاق می افتد بدون بررسی منظم، حتی جزئی ترین مسئله امنیتی می تواند به سرعت به نقض مهم امنیتی تبدیل شود.

شاخص‌های کلیدی عملکرد و ریسک Key Performance and Risk Indicators

با استفاده از شاخص‌های کلیدی عملکرد و ریسک داده‌های فرآیند امنیت، سازمان‌ها تشخیص می‌دهند که احتمالاً چه ریسک‌های امنیتی رخ می‌دهد. شاخص‌های کلیدی عملکرد به سازمانها این امکان را می‌دهد تا تعیین کنند که سطح عملکرد پایین تر یا بالاتر از هنجارهای تعیین شده است. شاخص‌های اصلی ریسک به سازمان‌ها اجازه می‌دهد تا مشخص کنند که احتمالاً برخی از ریسک‌های خاص رخ می‌دهد یا خیر.

NIST چارچوبی برای بهبود امنیت زیرساختهای بحرانی منتشر کرده است، که در آن استفاده از درایورهای کسب و کار برای هدایت فعالیت‌های امنیت سایبری و در نظر گرفتن ریسک‌های امنیت سایبری به عنوان بخشی از فرآیندهای مدیریت ریسک سازمان متمرکز شده است. این چارچوب از سه بخش تشکیل شده است: هسته چهارچوب، مشخصات چارچوب، و ردیف‌های اجرای چارچوب.

هسته چارچوب Framework Core مجموعه‌ای از فعالیت‌های امنیت سایبری، پیامدها و مراجع آموزنده است که در میان بخش‌های مهم زیرساخت بوده و راهنمایی‌های دقیقی را برای توسعه مشخصات سازمان منحصر به فرد ارائه می‌دهد. چهارچوب اصلی از پنج عملکرد همزمان و مداوم تشکیل شده است - شناسایی، محافظت، تشخیص، پاسخ و بازیابی.

پس از شناسایی هر عملکرد، شاخه‌ها و زیر شاخه‌ها برای هر عملکرد ثبت می‌شوند. مشخصات چارچوب Framework Profiles بر اساس نیازهای کسب و کار شاخه‌ها و زیر شاخه‌ها توسعه می‌یابد. این چارچوب با استفاده از مشخصات چارچوب به سازمان کمک می‌کند تا فعالیت‌های امنیت سایبری خود را با الزامات کسب و کار، تحمل ریسک و منابع خود تراز کند. ردیف‌های چارچوب Framework Tiers مکانیسمی را برای سازمانها فراهم می‌کند تا ویژگیهای رویکرد خود در مدیریت ریسک امنیت سایبری را مشاهده و درک کنند. ردیف‌های زیر استفاده می‌شود: ردیف ۱، جزئی Partial، ردیف ۲، آگاهی از ریسک Risk informed، ردیف ۳، قابل تکرار Repeatable و ردیف ۴، تطبیقی Adaptive.

سازمانها همچنان ریسک‌های منحصر به فرد، تهدیدات مختلف، آسیب پذیری‌های مختلف، و تحمل ریسک‌های مختلف، و نحوه اجرای این شیوه‌ها را در چارچوب متفاوت خواهند داشت. درنهایت، این چارچوب با هدف کاهش و مدیریت بهتر ریسکهای امنیت سایبری انجام شده که یک رویکرد یک اندازه برای مدیریت امنیت سایبری نیست.

داده‌های تأیید نسخه پشتیبان Backup Verification Data

از داده‌های فرآیند امنیت که جمع آوری شده نیز باید نسخه پشتیبان تهیه شود. متخصصان امنیت باید مطمئن شوند که سازمان آنها از پشتیبان گیری مناسب برخوردار بوده و دستورالعمل‌های مربوط به همه داده‌های فرایند امنیت را بازیابی می‌کنند. اگر داده‌ها به درستی تهیه نشده باشند، یک خرابی می‌تواند منجر به از بین رفتن داده‌های حیاتی برای همیشه شود. علاوه بر این، پرسنل باید روند بازیابی را بطور منظم تست کنند تا مطمئن شوند که آن طور که باید عمل می‌کند. اگر یک سازمان نتواند یک پشتیبان را به درستی بازیابی کند، ممکن است سازمان نتواند از این نسخه پشتیبان استفاده کند.

آموزش و آگاهی Training and Awareness

کلیه پرسنل باید هرگونه استراتژی ارزیابی و تست امنیتی را که سازمان از آن استفاده می‌کند درک کنند. ممکن است پرسنل فنی در مورد جزئیات ارزیابی و تست امنیت از جمله تست کنترل امنیتی و جمع آوری داده‌های فرآیند امنیت نیاز به آموزش داشته باشند. با این حال، فقط سایر پرسنل نیاز به آموزش آگاهی بیشتر در این زمینه دارند. متخصصان امنیت باید به پرسنل کمک کنند که درک کنند چه نوع ارزیابی و تستی رخ داده، چه چیزی توسط این فرآیند بدست آورده می‌شود و چرا این فرایند برای سازمان مهم است. مدیریت باید استراتژی ارزیابی امنیتی و تست امنیتی را کاملاً پشتیبانی کند و باید اهمیت این برنامه را به کلیه پرسنل و ذینفعان اعلام کند.

بازیابی فاجعه و استمرار کسب و کار Disaster Recovery and Business Continuity

هرگونه طرح‌های بازیابی و تداوم فاجعه که یک سازمان ایجاد می‌کند، باید ارزیابی و تست امنیتی، تست کنترل امنیت و جمع آوری داده‌های فرآیند امنیت را در نظر بگیرد. اغلب وقتی یک سازمان به حالت بازیابی فاجعه می‌رود، پرسنل در مورد این فرآیندها نمی‌اندیشند. در حقیقت، کنترل‌های امنیتی معمولی در چنین مواقعی در کنار قرار دارند. یک متخصص امنیت وظیفه دارد مطمئن شود که این اتفاق نمی‌افتد. متخصصان امنیت درگیر در تهیه طرح‌های بهبود فاجعه و تداوم کسب و کار باید همه این مناطق را تحت پوشش قرار دهند.

تجزیه و تحلیل و گزارش نتایج آزمون Analyze and Report Test Outputs

پرسنل باید گزارش خودکار Automate و دستی Manual را که می‌تواند به عنوان بخشی از ارزیابی امنیتی و آزمایش انجام شود درک کنند. خروجی باید به موقع به مدیریت گزارش شود تا اطمینان حاصل شود که آنها ارزش این روند را درک می‌کنند. ممکن است تهیه گزارشات مختلف بسته به سطح درک مخاطبان ضروری باشد. به عنوان مثال، مدیریت سطح بالا فقط به خلاصه یافته‌ها نیاز دارند. اما پرسنل فنی جزئیات یافته‌ها را نیاز دارند تا اطمینان حاصل شود که آنها می‌توانند کنترل‌های مناسبی را برای کاهش یا جلوگیری از ریسک موجود در ارزیابی و تست امنیتی انجام دهند.

ممکن است پرسنل در مورد نحوه اجرای گزارش‌های دستی و چگونگی تجزیه و تحلیل خروجی‌های گزارش نیاز به آموزش ویژه داشته باشند.

ممیزی داخلی و شخص ثالث Internal and Third-Party Audits

سازمان‌ها باید به عنوان بخشی از هر استراتژی ارزیابی و تست امنیتی، ممیزی‌های داخلی و شخص ثالث را انجام دهند. این ممیزی‌ها باید تمام کنترل‌های امنیتی موجود را آزمایش کنند. موارد زیر چند دستورالعمل برای در نظر گرفتن بخشی از یک طرح ممیزی امنیت مناسب می‌باشد:

- ✓ حداقل، ممیزی‌های سالانه را برای ایجاد یک مبنای امنیتی انجام شود.
- ✓ اهداف سازمان خود را برای ممیزی تعیین کرده و با ممیزان به اشتراک گذاشته شود.
- ✓ قبل از شروع ممیزی، قوانین پایه ممیزی، از جمله تاریخ / زمان ممیزی تنظیم شود.
- ✓ ممیزانی را انتخاب کرده که تجربه امنیتی دارند.
- ✓ در مراحل اولیه مدیران واحد کسب و کار درگیر شوند.
- ✓ اطمینان حاصل شود که ممیزان متکی به تجربه هستند، نه فقط براساس چک لیست ها.
- ✓ اطمینان حاصل شود که گزارش ممیزی منعکس کننده ریسک‌های شناسایی شده سازمان است.
- ✓ اطمینان حاصل شود که ممیزی به درستی انجام شده است.

✓ اطمینان حاصل شود که ممیزی همه سیستم ها و کلیه سیاست ها و رویه ها را در بر می گیرد.

✓ وقتی ممیزی کامل است گزارش بررسی شود.

امروزه بسیاری از مقررات مستلزم وقوع ممیزی ها هستند. در گذشته سازمانها با تکیه بر بیانیه استانداردهای ممیزی 70 Statement on Auditing Standards (SAS) اعتماد می کردند، که به میزان اطلاعات و تأیید در رابطه با کنترل مراکز داده و فرآیندهای مربوط به کاربران مراکز داده و گزارش مالی آنها ارائه می داد. در واقع ممیزی SAS 70 تأیید کرد که کنترل ها و فرآیندهای تنظیم شده توسط یک مرکز داده دنبال می شوند. بیانیه های مربوط به استانداردهای مربوط به شرکت در آزمون سنجش 16 Standards for Attestation Engagement (SSAE) استاندارد جدیدتری است که کنترل ها و فرایندها را تأیید می کند و همچنین مستلزم اظهار نظر کتبی در مورد طراحی و کارایی عملکرد کنترل های مورد بررسی است.

ممیزی 16 SSAE در گزارش کنترل سازمان خدمات (SOC) Service Organization Control گزارش شده است. این گزارش بر کنترل داخلی روی گزارشگری مالی متمرکز است. دو نوع گزارش SOC 1 وجود دارد:

▪ گزارش SOC 1، نوع ۱: تمرکز خود را بر روی نظر میزان در مورد صحت و کامل بودن

طراحی مدیریت کنترل های مرکز داده، سیستم و / یا خدمات انجام می دهد.

▪ گزارش SOC 1، نوع ۲: شامل گزارش نوع ۱ و همچنین ممیزی اثربخش کنترلها در

یک بازه زمانی مشخص، بطور معمول بین شش ماه تا یک سال است.

دو نوع گزارش دیگر نیز موجود است: SOC 2 و SOC 3 هر دو این ممیزی ها معیارهای کنترل مربوط به امنیت، در دسترس بودن، یکپارچگی پردازش، محرمانه بودن یا حفظ حریم شخصی یک سیستم و اطلاعات آن را ارائه می دهند. گزارش SOC 2 شامل خدمات تست و نتایج شخص ممیز است و گزارش SOC 3 فقط توضیحات سیستم و نظر شخص ممیز را ارائه می دهد. گزارش SOC 3 برای استفاده عمومی است و سطح صدور گواهی نامه را برای اپراتورهای مرکز داده فراهم می کند که به کاربران مرکز داده، امنیت تاسیسات، در دسترس بودن زیاد و یکپارچگی فرآیند را اطمینان می دهد. جدول ۶-۳ به طور خلاصه سه نوع گزارش SOC را مقایسه می کند.

	What It Reports On	Who Uses It
SOC 1	Internal controls over financial reporting	User auditors and controller office
SOC 2	Security, availability, processing integrity, confidentiality, or privacy controls	Management, regulators, and others; shared under non-disclosure agreement (NDA)
SOC 3	Security, availability, processing integrity, confidentiality, or privacy controls	Publicly available to anyone

جدول ۶-۳: مقایسه گزارش SOC

فصل ٧

عمليات امنيت
(Security Operations)

این فصل موضوعات زیر را در بر می گیرد:

- ❖ **تحقیقات Investigations:** مفاهیم مورد بحث شامل تحقیقات دیجیتالی و جرم شناسی رایانه ای است.
- ❖ **انواع تحقیق Investigation Types:** مفاهیم مورد بحث شامل عملیات، تحقیقات جنایی، غیرنظامی، نظارتی، و کشف الکترونیک eDiscovery است.
- ❖ **فعالیت های ورود به سیستم و نظارت Logging and Monitoring Activities:** مفاهیم مورد بحث شامل بررسی و ممیزی، شناسایی و جلوگیری از نفوذ، اطلاعات امنیتی و مدیریت رخدادهای، نظارت مستمر و نظارت بر خروجی ها است.
- ❖ **تأمین منابع Resource Provisioning:** مفاهیم مورد بحث شامل فهرست دارایی، مدیریت پیکربندی، دارایی های فیزیکی، دارایی های مجازی، دارایی های ابری و برنامه های کاربردی است.
- ❖ **مفاهیم عملیات امنیتی Security Operations Concepts:** مفاهیم مورد بحث شامل مباحث مربوط به عملیات امنیتی، از جمله نیاز به دانستن / حداقل امتیاز می باشد. مدیریت حساب ها، گروه ها و نقش ها، تفکیک وظایف، چرخش کار، روش های حساس اطلاعات، حفظ رکورد، نظارت بر امتیازات ویژه، چرخه عمر اطلاعات، و توافق نامه های سطح خدمات (سرویس).
- ❖ **حمایت از منابع Resource Protection:** مفاهیم مورد بحث شامل حفاظت از دارایی های ملموس و ناملموس و مدیریت دارایی می باشد.
- ❖ **مدیریت حادثه Incident Management:** مفاهیم مورد بحث شامل رخداد در مقابل حادثه، تیم واکنش به حادثه و تحقیقات درباره حادثه، قوانین تعامل، مجوز، دامنه، رویه های واکنش به حادثه، مدیریت واکنش به حادثه و مراحل در فرایند واکنش به حادثه است.
- ❖ **اقدامات پیشگیرانه Preventive Measures:** مفاهیم مورد بحث شامل سطوح قطع، انحراف از استانداردها، حوادث غیرمعمول یا غیر قابل توضیح، راه اندازی مجدد بدون برنامه ریزی، افشای غیرمجاز، بازیابی مطمئن، مسیرهای اعتماد، کنترل های ورودی / خروجی، سخت شدن سیستم، سیستم های مدیریت آسیب پذیری، IDS / IPS، ضد

بدافزار / آنتی ویروس، فایروال ها، لیست سفید / لیست سیاه، خدمات امنیتی شخص ثالث، جعبه ماسه بازی Sandboxing، و Honeypot/honeynet ها.

❖ **مدیریت پچ Patch Management:** مفاهیم مورد بحث شامل فرایند مدیریت پچ سازمان می باشد.

❖ **فرآیند مدیریت تغییر Change Management Process:** مفاهیم مورد بحث شامل فرایند مدیریت تغییر هستند.

❖ **استراتژی های بازیابی Recovery Strategies:** مفاهیم مورد بحث شامل سیستم های افزونگی، تاسیسات و برق هستند. فن آوری های تحمل خطا، بیمه، فایل پشتیبانی اطلاعات، شناسایی آتش و سرکوب، در دسترس بودن بالا، کیفیت خدمات، مقاومت سیستم، و ایجاد استراتژی های بازیابی.

❖ **بهبود فاجعه Disaster Recovery:** مفاهیم مورد بحث شامل پاسخ، پرسنل، ارتباطات، ارزیابی، ترمیم و آموزش و آگاهی است.

❖ **تست برنامه های بازیابی Testing Recovery Plans:** مفاهیم مورد بحث شامل تست از طریق خواندن، تست چک لیست، عملکرد بالای جدول، تست از طریق ساختاری، تست شبیه سازی، تست موازی، تست کامل وقفه، تمرین کاربردی و ممارست تخلیه است.

❖ **برنامه ریزی و فعالیت های مداوم در کسب و کار Business Continuity Planning and Exercises:** مفاهیم مورد بحث شامل برنامه ریزی و فعالیت های مداوم است.

❖ **امنیت فیزیکی Physical Security:** مفاهیم مورد بحث شامل امنیت محیط و ساختمان و امنیت داخلی می باشد.

❖ **حریم شخصی و امن پرسنل Personnel Privacy and Safety:** مفاهیم مورد بحث شامل شدت، سفر و نظارت هستند.

عملیات امنیت شامل مفاهیم عملیات امنیتی بنیادی، تحقیقات، مدیریت حوادث و بهبود فاجعه است. همچنین امنیت فیزیکی و پرسنلی را نیز تحت پوشش خود قرار می دهد. متخصصان امنیت باید آموزش های لازم را در این مناطق دریافت کنند یا از متخصصانی در این مناطق بهره بگیرند تا از دارایی سازمان ها به درستی محافظت شود.

عملیات امنیت شامل تضمین اجرای کلیه عملیات درون سازمان با روشی امن است. دغدغه تحقیق، مدیریت و جلوگیری از وقایع یا حوادث است. این برنامه همچنین فعالیت های ورود به سیستم را در هنگام وقوع، تأمین و محافظت از منابع در صورت لزوم، مدیریت رخدادها و حوادث، بازیابی رخداد و بلایای طبیعی و تأمین امنیت فیزیکی را در بر می گیرد. عملیات امنیت شامل فعالیت روزانه یک سازمان است.

تحقیقات Investigations

تحقیقات باید به روشی مناسب انجام شود تا تضمین شود که هرگونه شواهد جمع آوری شده در دادگاه قابل استفاده است. بدون تحقیقات مناسب و جمع آوری شواهد، مهاجمان مسئولیت اقدامات خود را بر عهده نخواهند گرفت. در این بخش به بررسی و شواهد قانونی جرم شناسی رایانه ای و دیجیتالی می پردازیم.

تحقیقات دیجیتال و جرم شناسی رایانه ای Forensic and Digital Investigations

تحقیقات رایانه ای نسبت به تحقیقات عادی روش های متفاوتی را طلب می کند زیرا بازه زمانی مامور تحقیق فشرده است و ممکن است به یک متخصص برای کمک به تحقیقات لازم باشد. همچنین، اطلاعات رایانه ای ناملموس است و غالباً نیاز به مراقبت بیشتری برای اطمینان از حفظ اطلاعات در فرمت اصلی خود دارد. در نهایت، شواهد جمع آوری شده در یک جرم رایانه ای دشوارتر می باشد.

پس از اتخاذ تصمیمی برای تحقیق در مورد جرم رایانه، باید رویه های استاندارد شده از جمله موارد زیر را دنبال شود:

- شناسایی اینکه چه نوع سیستمی قابل توقیف است.
- اعضای تیم جستجو و توقیف شناسایی شوند.
- تعیین ریسک اینکه مضمون شواهد را از بین ببرد.

پس از اطلاع از اجرای قانون جرم رایانه ای، محدودیت های مامور تحقیق سازمان افزایش می یابد. برای اطمینان از حفظ صحیح شواهد، تحقیقات لازم برای اجرای قانون انجام می شود. هنگام تحقیق درباره یک جرم رایانه، باید قوانین اثبات گرای رعایت شود. شواهد رایانه ای باید واقعی را اثبات کنند که برای پرونده مهم است و باید قابل اعتماد باشد و زنجیره حضانة باید

حفظ شود. اگر فرآیند تولید آن مستند باشد، به احتمال زیاد مدارک رایانه‌ای در دادگاه به عنوان مدارک پذیرفته نمی‌شوند.

تحقیقات قانونی شامل مراحل زیر است:

۱- شناسایی Identification

۲- حفظ Preservation

۳- مجموعه Collection

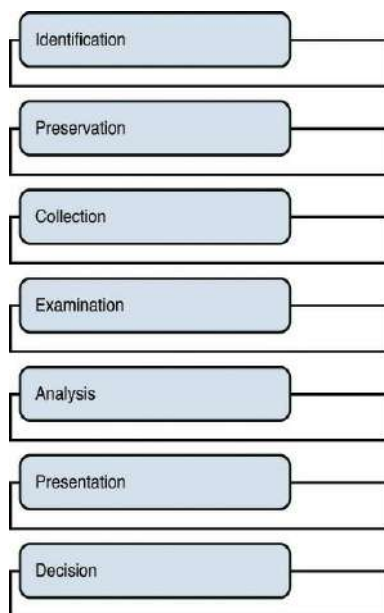
۴- امتحان Examination

۵- تجزیه و تحلیل Analysis

۶- ارائه Presentation

۷- تصمیم‌گیری Decision

روند تحقیقات قانونی در شکل ۷-۱ نشان داده شده است.



شکل ۷-۱: روند تحقیقات قانونی

در بخش‌های بعدی، مراحل تحقیقات جرم‌شناسی رایانه‌ای به طور مفصل و همچنین توضیح IOCE / SWGDE و NIST، صحنه جرم، MOM، زنجیره حفاظت و مصاحبه ارائه می‌شود.

شناسایی مدارک Identify Evidence

اولین قدم در هر تحقیقات جرم شناسی رایانه ای شناسایی و امنیت صحنه جرم و شناسایی شواهد است. شناسایی شواهد از طریق بررسی گزارش های ممیزی، سیستم های نظارت، تجزیه و تحلیل شکایات کاربر و تجزیه و تحلیل مکانیسم های تشخیص، انجام می شود. در ابتدا، ماموران تحقیق ممکن است از اهمیت مدارک مطمئن باشند. حفظ مدارک مبنی بر عدم نیاز، همیشه بهتر از آرزو داشتن مدارکی است که حفظ نشده است.

شناسایی صحنه جرم نیز بخشی از این مرحله است. در تحقیقات دیجیتالی، سیستم حمله شده صحنه جرم تلقی می شود. در برخی موارد، سیستمی که از آنجا حمله صورت گرفته نیز می تواند بخشی از صحنه جرم تلقی شود. با این حال، گرفتن کامل سیستم های مهاجم همیشه امکان پذیر نیست. به همین دلیل، باید اطمینان داشته باشید که از داده هایی که می توانند به یک سیستم خاص اشاره کنند، مانند گرفتن آدرس های IP، نام کاربری و سایر شناسه ها، عملیات ضبط صورت گرفته است.

حفظ و جمع آوری مدارک Preserve and Collect Evidence

مراحل بعدی در تحقیقات جرم شناسی رایانه ای شامل حفظ و جمع آوری شواهد است، که شامل ساختن تصاویر سیستم، اجرای زنجیره حضانة (که بعداً در بخش خود به تفصیل مورد بحث قرار می گیرد)، مستندسازی مدارک و ضبط زمان سنج ها است. قبل از جمع آوری هرگونه مدرک، ترتیب فراریت Volatility را در نظر بگیرید. این دستور تضمین می کند که محققان مدارکی را از مؤلفه هایی که در درجه اول فرار هستند جمع آوری کنند. ترتیب فراریت به شرح زیر است:

- ۱- محتویات حافظه Memory contents
- ۲- تعویض فایلها Swap files
- ۳- فرآیندهای شبکه Network processes
- ۴- فرآیندهای سیستم System processes
- ۵- اطلاعات سیستم فایل. File system information
- ۶- بلوک های دیسک خام Raw disk blocks

برای ساخت تصاویر Images سیستم، باید از ابزاری استفاده شود که یک نسخه بیتی از سیستم ایجاد کند. در بیشتر موارد، باید سیستم را جدا کرده و آن را از محصول حذف کند تا این نسخه سطح بیت ایجاد شود. باید اطمینان حاصل شود که دو نسخه از تصویر حفظ شده است. یک نسخه از تصویر ذخیره می‌شود تا مطمئن شود که یک نسخه دقیق آسیب دیده، به عنوان شواهد موجود است. نسخه دیگر در طی مراحل امتحان و تحلیل استفاده خواهد شد. برای اطمینان از یکپارچگی داده‌ها باید از خلاصه پیام استفاده شود.

اگرچه تصویر سیستم معمولاً مهمترین شواهد می‌باشد، ولی تنها مدارک مورد نیاز نیست. همچنین ممکن است لازم باشد داده‌هایی را که در کش حافظه، جداول پردازش، حافظه و رجیستری ذخیره می‌شوند، ضبط شوند. هنگام مستندسازی حمله به رایانه، باید از یک دفترچه مفید برای یادداشت کردن استفاده شود.

به خاطر داشته باشید که استفاده از متخصصان در تحقیقات دیجیتال برای اطمینان از صحت نگهداری و جمع‌آوری شواهد ممکن است ضروری باشد. ماموران تحقیق معمولاً یک کیت میدانی را برای کمک به روند تحقیقات جمع‌آوری می‌کنند. این کیت ممکن است شامل برچسب‌ها و تگ‌ها، ابزار جداسازی قطعات و بسته بندی مدارک باشد.

کیت‌های زمینه کسب و کار در دسترس هستند، یا می‌توان بر اساس نیازهای سازمانی، وسایل مورد نیاز خود را جمع‌آوری کنند.

بررسی و تجزیه و تحلیل مدارک Examine and Analyze Evidence

پس از حفظ و جمع‌آوری مدارک، ماموران تحقیق باید مدارک را بررسی و تجزیه و تحلیل کنند. در هنگام بررسی مدارک، باید هر ویژگی از جمله نشانگرهای زمانی (زمانسنجها) و خصوصیات شناسایی، تعیین و مستند شود. پس از آنکه مدارک با استفاده از روشهای علمی کاملاً مورد تجزیه و تحلیل قرار گرفت، باید حادثه کاملاً بازسازی و ثبت شود.

یافته‌های حاضر Present Findings

پس از بررسی و تحلیل شواهد، باید به عنوان شواهد در دادگاه ارائه شود. در بیشتر موارد هنگام ارائه مدارک در دادگاه، ارائه یافته‌ها با فرمی که مخاطب می‌تواند درک کند بهترین گزینه می‌باشد. اگرچه باید از یک متخصص برای شهادت در مورد یافته‌ها استفاده شود، اما مهم است که متخصص بتواند جزئیات شواهد را برای مخاطبان غیر فنی بیان کند.

تصمیم گیری Decide

در پایان مراحل دادگاه، تصمیمی در مورد گناه یا بی گناهی طرف متهم اتخاذ می شود. در آن زمان، دیگر نیازی به حفظ شواهد نخواهد بود. با این وجود، مستندسازی هر درس آموخته شده از حادثه مهم است. افراد درگیر در هر قسمت از تحقیقات باید بخشی از این جلسه آموخته شده باشند.

IOCE/SWGDE و NIST

سازمان بین المللی شواهد رایانه ای International Organization on Computer Evidence (IOCE) و کارگروه علمی شواهد دیجیتال Working Group on Digital Evidence (SWGDE) دو گروه هستند که جرم شناسی رایانه ای دیجیتال را مطالعه می کنند و به ایجاد استانداردهای تحقیق دیجیتال کمک می کنند. هر دو گروه در بسیاری از فرمت های اطلاعات دیجیتالی، از جمله داده های رایانه، داده های دستگاه سیار، داده های سیستم های رایانه ای خودرو و غیره، دستورالعمل هایی را منتشر می کنند. هر مامور تحقیق باید مطابق با اصول این گروه ها باشد. اصول اصلی که توسط IOCE مستند شده است به شرح زیر است:

- قوانین کلی شواهد باید برای کلیه مدارک دیجیتالی اعمال شود.
- پس از توقیف مدارک دیجیتالی، اقدامات انجام شده نباید این شواهد را تغییر دهد.
- هنگامی که یک فرد نیاز به دسترسی به شواهد دیجیتالی اصلی دارد، آن شخص باید برای این منظور آموزش دیده باشد.
- کلیه فعالیتهای مربوط به توقیف، دسترسی، ذخیره یا انتقال شواهد دیجیتالی باید کاملاً مستند، حفظ و برای بررسی در دسترس باشد.
- فرد، مسئول تمام اقدامات انجام شده با توجه به شواهد دیجیتالی است زمانی که شواهد دیجیتالی در اختیار اوست.
- هر آژانس که مدارک دیجیتالی را توقیف، دسترسی، ذخیره، یا انتقال می دهد، مسئول رعایت اصول IOCE است.

NIST SP 800-86، "راهنمای تحقیق در مورد تکنیک های جرم شناسی رایانه ای برای پاسخ به حوادث"، راهنمایی هایی را در مورد جمع آوری داده ها، بررسی، تجزیه و تحلیل و گزارش های مربوط به جرم شناسی دیجیتال ارائه می دهد. همچنین توضیح می دهد که استفاده از ماموران

تحقیق جرم شناسی رایانه ای، کارکنان فناوری اطلاعات و دست اندرکاران حادثه به عنوان بخشی از تحقیقات جرم شناسی رایانه ای هستند. این بحث در مورد چگونگی هزینه، زمان پاسخ و حساسیت داده ها باید بر تحقیقات جرم شناسی رایانه ای تأثیر بگذارد.

برای ایجاد توانایی قانونی سازمانی، NIST SP 800-86 دستورالعمل های زیر را ارائه می دهد:

- سازمان ها باید توانایی انجام جرم شناسی رایانه و شبکه را داشته باشند.
- سازمانها باید تعیین کنند که طرفین باید با هر جنبه جرم شناسی رایانه ای رفتار کنند.
- تیم های رسیدگی به حوادث باید از توانایی های جرم شناسی رایانه ای قوی برخوردار باشند.
- بسیاری از تیمهای یک سازمان باید در جرم شناسی رایانه ای شرکت کنند.
- ملاحظات جرم شناسی رایانه ای باید به روشنی در سیاستها مورد بررسی قرار گیرد.
- سازمانها باید دستورالعمل ها و روشهای انجام وظایف جرم شناسی رایانه ای را ایجاد کرده و حفظ کنند.

NIST SP 800-86 دستورالعمل استفاده از داده ها در فایل های داده، سیستم عامل ها، ترافیک شبکه و برنامه ها را ارائه می دهد. سازمان ها می توانند از این استاندارد استفاده کرده تا اطمینان حاصل شود که پرسنل از انجام دستورالعملهای مناسب در انجام تحقیقات جرم شناسی رایانه ای پیروی می کنند.

صحنه جرم Crime Scene

صحنه جرم، محیطی است که شواهد احتمالی در آن وجود دارد. پس از شناسایی صحنه جرم، باید اقدامات لازم جهت حراست از محیط، از جمله محیط فیزیکی و مجازی انجام شود. برای تأمین امنیت صحنه جرم فیزیکی، یک مامور تحقیق ممکن است با قطع کردن آنها از شبکه، سیستمهای درگیر را جدا کند. با این حال، سیستمها تا زمانی که مامور تحقیق مطمئن نشود که همه شواهد دیجیتالی توقیف شده است، نباید خاموش شود. به خاطر داشته باشید که اطلاعات رایانه ای زنده و پویا هستند و احتمالاً در چندین مکان فرار Volatile، ذخیره می شوند. هنگام پاسخ به یک جرم احتمالی، مهم است که با استفاده از مراحل زیر از محیط صحنه جرم محافظت شود:

- ۱- مشخص کردن صحنه جرم.
- ۲- محافظت کردن از کل صحنه جرم.

- ۳- شناسایی کردن هر قطعه شواهد یا منبع احتمالی شواهد که بخشی از صحنه جرم است.
 - ۴- جمع آوری تمام شواهد در صحنه جرم.
 - ۵- به حداقل رساندن آلودگی با ایمن سازی و حفظ همه شواهد.
- به خاطر داشته باشید که به ویژه در جرایم دیجیتال، بیش از یک صحنه جرم وجود دارد. اگر یک مهاجم شبکه یک سازمان را نقض کند، تمام دارایی‌ها که به خطر می‌افتد بخشی از صحنه جرم بوده و هر دارایی که مهاجم از آن استفاده می‌کند همچنین جزئی از صحنه جرم می‌باشد. دسترسی به صحنه جرم باید کاملاً کنترل شود و فقط در دسترس افرادی که برای تحقیقات حیاتی هستند، باشد. به عنوان بخشی از فرآیند مستندسازی، هر شخصی را که به صحنه جرم دسترسی دارد را، یادداشت کنید. پس از آلوده شدن صحنه جرم، راهی برای بازگرداندن آن به وضعیت اصلی وجود ندارد.

MOM

مستندسازی انگیزه، فرصت و ابزار (Motive, Opportunity, Means (MOM) اساسی ترین استراتژی برای تعیین مظنونان است. انگیزه، همه چیز در مورد اینکه چرا این جرم مرتکب شده و چه کسی مرتکب جرم شده است.

فرصت، در مورد محل و زمان وقوع جرم است. ابزار، همه چیز در مورد نحوه انجام این جرم توسط مظنون است. هر مظنون که مورد توجه قرار گیرد باید هر سه خصوصیات را داشته باشد. به عنوان مثال، یک مظنون ممکن است انگیزه ارتکاب جرم (اخراج از سازمان) و فرصتی برای ارتکاب جرم داشته باشد (حساب‌های کاربری به درستی غیرفعال نشده اند) اما ممکن است ابزاری برای انجام جرم نداشته باشد.

درک MOM می‌تواند به هر مامور تحقیق کمک کند تا لیست مظنونان را به حداقل برساند.

زنجیره‌ای از توقیف Chain of Custody

در ابتدای هر تحقیق، باید سؤالات چه کسی، چه چیزی، چه زمانی، کجا و چگونه است، مطرح شود. این سؤالات می‌توانند به دریافت کلیه داده‌های مورد نیاز برای زنجیره توقیف کمک کنند. زنجیره توقیف نشان می‌دهد که چه کسی شواهد را کنترل کرده، چه کسی شواهد را تضمین کرده است و چه کسی شواهد را بدست آورده است. برای پیگرد موفقیت آمیز یک مظنون، باید

یک زنجیره توقیف مناسب حفظ شود. برای حفظ زنجیره مناسب از توقیف، شواهد باید طبق مراحل از پیش تعیین شده مطابق با کلیه قوانین و مقررات جمع آوری شوند. هدف اصلی زنجیره توقیف اطمینان از پذیرش شواهد در دادگاه است. مأموران اجرای قانون در هرگونه تحقیق که انجام می‌دهند، بر زنجیره توقیف تأکید دارند. درگیر کردن اجرای قانون در مراحل اولیه در طی تحقیقات می‌تواند باعث اطمینان شود که زنجیره مناسب توقیف، دنبال شده است.

مصاحبه Interviewing

تحقیقات اغلب شامل مصاحبه با مظنونین و شاهدان است. یک نفر باید مسئول تمام مصاحبه‌ها باشد. از شواهد بدست آمده باید مطمئن شود که مصاحبه کننده می‌داند چه اطلاعاتی باید بدست آورد و همچنین همه سؤالات مهم را پوشش می‌دهد. اگر اجرای قانون انجام مصاحبه است، فقط خواندن حقوق یک مظنون لازم است. ضبط مصاحبه ممکن است ایده خوبی برای تأیید بعد از مصاحبه به عنوان شواهد باشد.

اگر یک کارمند مظنون به جرم رایانه‌ای باشد، نماینده اداره منابع انسانی باید در هر بازجویی از مظنون شرکت داشته باشد. کارمند فقط باید توسط فردی که ارشد آن کارمند است مصاحبه شود.

شواهد Evidence

برای اینکه شواهد قابل قبول باشد، باید مرتبط، از نظر قانونی مجاز، قابل اطمینان، به درستی شناسایی و به درستی حفظ شود. مرتبط Relevant به این معنی است که باید یک واقعیت مادی مربوط به جرم را اثبات کند که نشان می‌دهد جرم مرتکب شده است، می‌تواند اطلاعاتی را برای توصیف جرم ارائه دهد، می‌تواند اطلاعاتی را در مورد انگیزه‌های فرد مرتکب ارائه دهد، یا می‌تواند وقوع آن را تأیید کند. قابلیت اطمینان Reliability یعنی عدم دستکاری یا اصلاح آن. حفظ Preservation به معنی این است که مدارک در معرض خسارت یا تخریب قرار نگیرد. به همه شواهد باید تگ چسبیده شود. هنگام چسباندن تگ، حتماً نحوه انتقال و وسایل انتقال، توضیحات کاملی از شواهد از جمله کیفیت، کسانی که شواهد را دریافت کرده اند، و افرادی که به شواهد دسترسی داشته اند، مستند شود.

هر مامور تحقیق باید مطمئن شود که شواهد به پنج قاعده پایبند است. علاوه بر این، مامور تحقیق باید هر نوع شواهدی را که می توان بدست آورد و نحوه استفاده از هر نوع در دادگاه را درک کند. ماموران تحقیق باید دستورالعملهای نظارت، جستجو و توقیف را دنبال کنند. سرانجام، محققان باید تفاوت های بین رسانه، نرم افزار، شبکه، تجزیه و تحلیل سخت افزار / دستگاه تعبیه شده را درک کنند.

هنگام جمع آوری شواهد، یک مامور تحقیق باید مطمئن باشد که شواهد پنج قاعده حاکم بر آن را رعایت می کند:

- معتبر باشد. Be authentic
- صحت داشته باشد. Be accurate
- کامل باشد. Be complete
- قانع کننده باشد Be convincing
- قابل قبول است. Be admissible

از آنجا که شواهد دیجیتالی فراتر از سایر شواهد است، باید این پنج قانون رعایت شود.

انواع شواهد Types of Evidence

یک مامور تحقیق باید از انواع شواهدی که در دادگاه استفاده می شود آگاه باشد تا از اثبات پذیرش همه شواهد اطمینان یابد و گاهی اوقات نوع شواهد پذیرش آن را تعیین می کند. انواع شواهدی که باید درک شود به شرح زیر است:

- بهترین شواهد Best evidence
- شواهد ثانویه Secondary evidence
- شواهد مستقیم Direct evidence
- شواهد قطعی Conclusive evidence
- شواهد محرمانه Circumstantial evidence
- شواهد تأیید شده Corroborative evidence
- شواهد نظری Opinion evidence
- شواهد گفت و شنود Hearsay evidence

✓ بهترین شواهد Best Evidence

بهترین قاعده شواهد بیان می‌کند که وقتی شواهد، مانند سند یا رکوردی، ارائه می‌شود، فقط نسخه اصلی پذیرفته می‌شود، مگر اینکه دلیل موجهی برای استفاده از اصل وجود نداشته باشد. در بیشتر موارد، شواهد دیجیتالی بهترین شواهد به حساب نمی‌آیند زیرا ماموران تحقیق باید نسخه‌هایی از داده‌های اصلی را کپی کنند.

اما دادگاهها با توجه به شواهد و وضعیت می‌توانند بهترین قاعده شواهد را در مورد شواهد دیجیتالی به صورت موردی اعمال کنند. در این شرایط، نسخه باید توسط یک شاهد متخصص ثابت شود که می‌تواند در مورد مطالب شهادت داده و تأیید کند که این یک نسخه دقیق از اصل می‌باشد.

✓ شواهد ثانویه Secondary Evidence

شواهد ثانویه از یک نسخه اصلی تولید شده است یا جایگزین یک مورد اصلی است. کپی اسناد اصلی و شهادت شفاهی شواهد ثانویه محسوب می‌شوند.

✓ شواهد مستقیم Direct Evidence

شواهد مستقیم بر اساس اطلاعات جمع‌آوری شده از طریق حواس شاهد، یک واقعیت را از طریق شهادت شفاهی اثبات یا رد می‌کنند. شاهد می‌تواند آنچه را دیده، بو کرده، شنیده، مزه یا احساس کرده شهادت دهد که شواهد مستقیم تلقی می‌شود. فقط شاهد می‌تواند شواهد مستقیم ارائه دهد. هیچ کس دیگر نمی‌تواند گزارشی را که شاهد بیان کرده را گزارش کند زیرا این به عنوان شواهد محرمانه در نظر گرفته می‌شود.

✓ شواهد قطعی Conclusive Evidence

شواهد قطعی نیازی به تأیید دیگری ندارد و با هیچ شواهد دیگری قابل تضاد نیست.

✓ شواهد محرمانه Circumstantial Evidence

شواهد محرمانه استنباط اطلاعات از دیگر حقایق مربوط به واسطه را فراهم می‌کند. این شواهد باعث می‌شود هیئت منصفه با استفاده از یک واقعیت به این نتیجه برسند که واقعیت دیگری

صحیح یا نادرست است. مثال این مورد حاکی از این است که یک کارمند سابق به دلیل عدم تمایل به سازمان پس از عزل خود، برضد یک سازمان مرتکب عملی شود.

✓ شواهد تأیید شده Corroborative Evidence

شواهد تأیید کننده اثبات شواهد دیگری است. به عنوان مثال، اگر مظنون رسیدی را تهیه کند تا ثابت کند که در یک ساعت خاص در یک رستوران خاص بوده و سپس یک پیشخدمت به وی شهادت دهد که منتظر فرد مظنون بوده است، آنگاه پیشخدمت از طریق شهادت خود مدارکی تأیید کننده‌ای را ارائه داده است.

✓ شواهد نظری Opinion Evidence

شواهد نظری مبتنی بر آنچه شخص شاهد درباره واقعیت ها، فکر، احساس یا استنباط می‌کند. اما اگر از شاهد خبره استفاده شود، وی می‌تواند براساس دانش خود در یک منطقه خاص، بر واقعیت شهادت دهد. به عنوان مثال، روانپزشک می‌تواند نتیجه گیری در مورد وضعیت روانی یک فرد شهادت دهد. شهادت خبره به دلیل دانش و تجربه خبره، شواهد نظری محسوب نمی‌شود.

✓ شواهد گفت و شنود Hearsay Evidence

شواهدی می‌باشد که در درجه دوم قرار دارد که شخص شاهد، دانش مستقیمی از واقعیت ندارد، و فقط آنرا از کسی شنیده است. در برخی موارد، شواهد مبتنی بر رایانه شواهد گفت و شنود می‌باشد، به ویژه اگر یک خبره نتواند صحت و یکپارچگی شواهد را گواهی دهد.

نظارت، جستجو و توقیف Surveillance, Search, and Seizure

نظارت، جستجو و توقیف جنبه‌های مهم هر تحقیق و بررسی می‌باشد. نظارت، معمولاً در افراد عبارتند از عمل نظارت بر رفتار، فعالیت‌ها یا سایر اطلاعات در حال تغییر. جستجو عمل پیگیری اطلاعات است و توقیف، انجام حضانت اجزای فیزیکی یا دیجیتالی است.

توسط ماموران تحقیق دو نوع نظارت استفاده می‌شود: نظارت فیزیکی و نظارت رایانه. نظارت فیزیکی هنگامی رخ می‌دهد که اقدامات شخص با استفاده از دوربین، مشاهده مستقیم یا دوربین مدار بسته (Closed-Circuit TV (CCTV)) گزارش و ضبط میشود. نظارت رایانه هنگامی رخ

می‌دهد که اقدامات شخص با استفاده از اطلاعات دیجیتالی، مانند گزارش‌های ممیزی، گزارش یا ضبط می‌شود.

در بیشتر موارد برای جستجوی فعال در یک سایت خصوصی برای اثبات، مجوز تفتیش Search Warrant لازم است. برای صدور مجوز تفتیش، علت احتمالی ارتکاب جرم باید به قاضی ثابت شود و قاضی باید با توجه به وجود شواهد، آن را تأیید کند. تنها زمانی نیازی به صدور مجوز تفتیش نیست که شرایط اضطراری بوده و برای جلوگیری از آسیب فیزیکی، تخریب شواهد، ضروری باشد. فرار مظنون یا پیامد دیگر اقدامات اجرایی ناامیدکننده‌ای خواهد بود و زمانیکه این شواهد در دادگاه ارائه شود، باید شرایط بحرانی اثبات شود.

توقیف مدارک فقط در صورتی ممکن است رخ دهد که شواهد به طور مشخص به عنوان بخشی از مجوز تفتیش ذکر شده باشد، مگر اینکه شواهد به نظر ساده بیاید. شواهدی که به طور خاص در مجوز تفتیش ذکر شده است می‌تواند توقیف شود و جستجو فقط می‌تواند در مناطقی که به طور خاص در مجوز ذکر شده است، انجام شود.

قوانین جستجو و توقیف در مورد سازمانهای خصوصی و افراد صدق نمی‌کند. اکثر سازمانها به کارمندان خود تذکر می‌دهند که فایل‌های ذخیره شده در منابع سازمانی، دارایی سازمان محسوب می‌شوند. این معمولاً بخشی از هرگونه سیاست عدم انتظار برای حفظ حریم خصوصی است. بحث در مورد شواهد بدون بحث در مورد صلاحیت Jurisdiction، ناقص است. از آنجا که جرائم رایانه‌ای می‌تواند دارایی‌هایی را در بر داشته باشد که از مرزهای قضایی عبور می‌کنند، ماموران تحقیق باید درک کنند که قوانین مدنی و جزائی کشورها می‌توانند تفاوت‌های زیادی با یکدیگر داشته باشند. همیشه بهتر است برای هرگونه تحقیقات جنایی یا مدنی با پرسنل اجرای قانون محلی مشورت کرد و از هرگونه توصیه‌ای که برای تحقیقات مربوط به حوزه‌های قضایی انجام می‌شود، پیروی کرد.

تحلیل رسانه Media Analysis

ماموران تحقیق با توجه به نوع رسانه می‌توانند انواع مختلفی از تحلیل رسانه را انجام دهند. ممکن است یک متخصص بازبینی رسانه‌ها برای تهیه یک تصویر گواهی جرم شناسی رایانه‌ای، که یک فرآیند پرهزینه می‌باشد، به کار گرفته شود.

در تحلیل رسانه می‌توان از موارد زیر استفاده کرد:

- تصویربرداری/از دیسک *Disk imaging*: یک تصویر دقیق از محتویات هارد دیسک ایجاد می کند.
- تجزیه و تحلیل فضای خالی *Slack space analysis*: فضای خالی (مشخص شده به عنوان خالی یا قابل استفاده مجدد) فضای درایو را بررسی می کند تا ببیند آیا می توان داده های قدیمی (مشخص شده برای حذف) را بازیابی کرد.
- تجزیه و تحلیل محتوا *Content analysis*: محتویات درایو را تجزیه و تحلیل می کند و گزارشی از انواع داده ها را با درصد ارائه می دهد.
- تجزیه و تحلیل پنهان سازی یک پیام کوچک *Steganography analysis*: فایل های موجود در درایو را تجزیه و تحلیل می کند تا ببیند آیا فایل ها تغییر کرده اند یا رمزگذاری فایل را کشف کرده است.

تجزیه و تحلیل نرم افزار *Software Analysis*

تجزیه و تحلیل نرم افزار بسیار دشوارتر از تجزیه و تحلیل رسانه است زیرا اغلب نیاز به ورود یک متخصص کد نرم افزار، از جمله کد منبع، کد کامپایل شده یا کد دستگاه دارد، و اغلب شامل تجزیه یا مهندسی معکوس است. این نوع تحلیل اغلب در حین تحلیل بدافزارها و اختلافات مربوط به حق چاپ *Copyright* مورد استفاده قرار می گیرد.

تکنیک های تحلیل نرم افزار شامل موارد زیر است:

- تجزیه و تحلیل محتوا *Content analysis*: تجزیه و تحلیل محتوای نرم افزار، به ویژه نرم افزارهای مخرب، برای تعیین اینکه کدام نرم افزار ایجاد شده است.
- مهندسی معکوس *Reverse engineering*: کد منبع *Source Code* برنامه را بازیابی می کند تا نحوه عملکرد برخی از عملیات را مشخص کند.
- شناسایی نویسنده *Author identification*: تلاش برای شناسایی شخصی که نرم افزار را نوشته است.
- تجزیه و تحلیل زمینه *Context analysis*: برای کشف سرنخ هایی برای تعیین ریسک، محیطی که نرم افزار در آن یافت می شود را تجزیه و تحلیل می کند.

تجزیه و تحلیل شبکه Network Analysis

تجزیه و تحلیل شبکه شامل استفاده از ابزارهای شبکه برای حفظ logها و فعالیت برای شواهد است.

تکنیک‌های تحلیل شبکه شامل موارد زیر است:

- ✓ تجزیه و تحلیل ارتباطات *Communications analysis*: با بدست گرفتن تمام یا بخشی از ارتباطات و جستجوی انواع خاص فعالیت، ارتباطات را از طریق شبکه تحلیل می‌کند.
- ✓ تجزیه و تحلیل *log (Log analysis)*: به تجزیه و تحلیل logهای مربوط به ترافیک شبکه می‌پردازد.
- ✓ ردیابی مسیر *Path tracing*: ردیابی مسیر یک بسته یا ترافیک خاص برای کشف مسیری که توسط مهاجم استفاده شده است.

تجزیه و تحلیل دستگاه تعبیه شده / سخت افزار Hardware/Embedded Device Analysis

تجزیه و تحلیل دستگاه تعبیه شده / سخت افزار شامل استفاده از ابزارها و سیستم عامل‌های ارائه شده با دستگاه‌ها برای تعیین عملکردهایی که روی دستگاه انجام می‌شود. تکنیک‌های مورد استفاده برای تحلیل دستگاه تعبیه شده / سخت افزار بر اساس دستگاه متفاوت است. در بیشتر موارد، فروشنده دستگاه با توجه به اطلاعات مورد نیاز، می‌تواند در مورد بهترین تکنیک مورد استفاده، مشاوره ارائه دهد. تجزیه و تحلیل *log*، تجزیه و تحلیل سیستم عامل و تحقیقات حافظه برخی از تکنیک‌های کلی مورد استفاده هستند.

این نوع تحلیل هنگام تجزیه و تحلیل دستگاه‌های سیار استفاده می‌شود. برای انجام این نوع تحلیل، NIST توصیه‌های زیر را ارائه می‌دهد:

- هرگونه تجزیه و تحلیل نباید داده‌های موجود در دستگاه یا رسانه را تغییر دهد.
- فقط ماموران تحقیق شایسته باید به داده‌های اصلی دسترسی داشته باشند و باید کلیه اقدامات انجام شده را توضیح دهند.
- مسیرهای ممیزی یا سوابق دیگر باید در تمام مراحل تحقیق ایجاد و حفظ شوند.
- رهبر مامور تحقیق مسئولیت اطمینان از پیروی این مراحل را به عهده دارد.
- کلیه فعالیت‌های مربوط به شواهد دیجیتالی، از جمله توقیف آن، دسترسی به آن، ذخیره آن یا انتقال آن باید مستند سازی، حفظ و برای بررسی در دسترس باشد.

انواع تحقیق Investigation Types

از متخصصان امنیت خواسته شده است که هر حادثه‌ای را که رخ می‌دهد، تحقیق کنند. در نتیجه دارایی‌های مختلفی که تحت تأثیر قرار می‌گیرند، و همچنین باید بتوانند انواع مختلفی از تحقیقات از جمله عملیات، تحقیقات جنایی، مدنی، نظارتی و تحقیقات الکترونیکی را انجام دهند.

عملیات Operations

تحقیقات عملیات، تحقیقاتی است که منجر به بروز هیچ مسئله کیفری، مدنی یا نظارتی نمی‌شود. در بیشتر موارد، این نوع تحقیقات به منظور تعیین علت اصلی بروز یک حادثه به پایان رسیده است تا بتوان اقدامات لازم را برای جلوگیری از وقوع این حادثه در آینده انجام داد. این فرآیند را تجزیه و تحلیل علت ریشه‌ای Root-cause analysis می‌گویند. از آنجا که هیچ قانون کیفری، مدنی یا نظارتی نقض نشده است، مستندسازی مدارک مهم نیست. با این حال، متخصصان امنیت هنوز باید تدابیری را برای مستند کردن دروس آموخته شده به عمل آورند.

به عنوان نمونه‌ای از این نوع تحقیقات، به یک کاربر بر اساس نقش شغلی خود، مجوزهای نامناسب اختصاص داده شود. اگر نتیجه این عمل مجرمانه باشد، باید تحقیقات جنایی صورت گیرد. با این حال، می‌تواند به سادگی از طریق اشتباهاتی که توسط پرسنل انجام می‌شود، رخ دهد. از آنجا که یک متخصص امنیت علت مجوزهای نامناسب را نمی‌داند، وی باید تحقیقات را طبق دستورالعمل‌های جرم‌شناسی رایانه‌ای مناسب آغاز کند. با این حال، هنگامی که او تشخیص داد که این حادثه نتیجه یک تصادف است، دیگر نیازی به پیروی از آن دستورالعمل‌ها نیست. هر شخصی که این نوع تحقیقات را انجام می‌دهد، باید مطمئن شود که تغییرات مناسب برای جلوگیری از وقوع دوباره چنین حادثه‌ای، از جمله اعمال کنترل‌های امنیتی انجام شده است. در مورد مثال مجوزهای نامناسب، ممکن است متخصص امنیت متوجه شود که الگوی حساب کاربری که برای ایجاد حساب کاربری استفاده شده است به یک گروه نامناسب اختصاص داده شده است بنابراین باید از بازنگری در الگوی حساب کاربری مطمئن شود.

جنایی Criminal

تحقیقات جنایی تحقیقاتی است که به دلیل نقض قانون فدرال، ایالتی یا محلی انجام می‌شود. در این نوع تحقیقات، یک سازمان باید مطمئن شود که اجرای قانون در تحقیقات انجام شده تا

اطمینان حاصل شود که جرم به درستی قابل اثبات، بررسی و قابل محاکمه است. تحقیقات جنایی منجر به محاکمه کیفری می‌شود.

مدنی Civil

تحقیقات مدنی وقتی اتفاق می‌افتد که یک سازمان یا یک طرف به یک سازمان دیگر بخاطر اقدامات غیرنظامی مظنون شود. به عنوان مثال، اگر یک سازمان مظنون باشد به سازمان دیگری که کپی رایت را نقض کرده است، می‌تواند دادخواست مدنی در این فیلد تشکیل دهد، زمانی پرونده‌های کپی رایت غیرقانونی رخ می‌دهد، فقط توسط دادستان‌های دولتی قابل ارائه هستند. در یک پرونده مدنی، سازمان باید از پیروی کلیه قوانین شواهد اطمینان حاصل کند و نماینده قانونی به عنوان بخشی از تحقیقات درگیر می‌شود.

نظارتی Regulatory

یک تحقیق نظارتی زمانی اتفاق می‌افتد که یک نهاد نظارتی، سازمانی را برای نقض نظارتی بررسی می‌کند. اخیراً، کمیسیون بورس و اوراق بهادار Securities and Exchange Commission (SEC) تحقیقات نظارتی زیادی را در مورد سازمان‌ها و معاملات مالی آنها انجام داده است. مهم نیست که کدام نهاد نظارتی تحقیق را انجام می‌دهد، به سازمان مورد بررسی، اطلاع داده می‌شود که تحقیقات در حال انجام است. سازمان باید سیاست‌ها و دستورالعمل‌هایی را برای اطمینان از رعایت کامل تحقیقات انجام دهد. عدم رعایت چنین تحقیقاتی می‌تواند منجر به اتهاماتی برضد این سازمان و هرگونه پرسنل درگیر شود.

اکتشاف الکترونیکی eDiscovery

اکتشاف الکترونیکی به دادخواست یا تحقیقات دولتی اشاره دارد که به عنوان بخشی از فرایند کشف، با تبادل اطلاعات در قالب الکترونیکی سروکار دارد. این اکتشاف شامل اطلاعات ذخیره شده الکترونیکی (ESI) Electronically stored information است و شامل ایمیل، اسناد، سخنرانیها، بانک اطلاعاتی، پست صوتی، فایل‌های صوتی و تصویری، رسانه‌های اجتماعی و وب سایت‌ها می‌باشد. متخصصان امنیت باید مطمئن شوند که محتوای اصلی و (Meta Data) ابر داده‌های ESI حفظ شده است تا از ادعای جاسوسی یا دستکاری شواهد بعد دادخواست جلوگیری شود. پس از جمع‌آوری ESI مناسب، باید در یک محیط امن برای بررسی برگزار شود.

فعالیت های log و نظارت Logging and Monitoring Activities

به عنوان بخشی از امنیت عملیات، ادمین ها باید مطمئن شوند که فعالیت های کاربر به طور منظم وارد سیستم شده و نظارت می شود، همچنین شامل ممیزی و بررسی، شناسایی و جلوگیری از نفوذ، اطلاعات امنیتی و مدیریت رخدادها، نظارت مداوم و نظارت بر خروجی ها است.

ممیزی و بررسی Audit and Review

پاسخگویی بدون ثبت فعالیت ها و بررسی فعالیت ها غیرممکن است. ضبط و نظارت ممیزی بر log ها، اثبات دیجیتالی را در هنگام شناسایی شخصی که انجام فعالیت های خاص را ارائه می دهد، فراهم می کند، که هم برای افراد خوب و هم برای افراد بد انجام می شود. در بسیاری از موارد لازم است مشخص شود چه کسی چیزی را اشتباه تنظیم کرده است، نه اینکه چه کسی چیزی را به سرقت برده است. مسیرهای ممیزی بر اساس کدهای دسترسی و شناسایی، مسئولیت پذیری فردی را ایجاد می کند. سؤالاتی که هنگام بررسی سوابق ممیزی باید به آنها رسیدگی شود شامل موارد زیر است:

- آیا کاربران به اطلاعات دسترسی پیدا می کنند یا وظایفی را که برای شغل خود ضروری نیست انجام می دهند؟
- آیا اشتباهات تکراری (مانند حذف) انجام می شود؟
- آیا بسیاری از کاربران حق و امتیازات ویژه ای دارند؟

سطح و میزان ممیزی باید منعکس کننده سیاست امنیتی شرکت باشد. ممیزها می توانند خود کارممیزی را انجام دهند یا توسط شخص ثالث انجام شود. خود ممیزی ها همیشه خطر ذهنیت را به فرایند معرفی می کنند. log ها را می توان در دستگاه های مختلفی از جمله سیستم های تشخیص نفوذ IDS، سرورها، روترها و سوئیچ ها تولید کرد. در حقیقت، یک IDS مستقر در میزبان از log های سیستم عامل دستگاه میزبان استفاده می کند.

هنگام ارزیابی کنترل های مربوط به مسیرهای ممیزی یا log های مربوطه، سوالات زیر مطرح می شود:

- آیا مسیر ممیزی اثری از اقدامات کاربر است؟
- آیا دسترسی به گزارش های آنلاین به شدت کنترل می شود؟

- آیا بین کارمندان امنیتی که عملکرد کنترل دسترسی را کنترل می‌کنند و افرادی که دنباله ممیزی را انجام می‌دهند، تفکیک وظایف وجود دارد؟

logها مطابق با سیاست حفظ و بقای تعریف شده در سیاست امنیت سازمان، نگهداری و ذخیره شود، تا برای جلوگیری از اصلاح، حذف و نابودی ایمن شوند. وقتی ممیزی در یک نقش نظارتی فعالیت می‌کند، از عملکرد تشخیص امنیت در گروه فنی پشتیبانی می‌کند.

هنگامی که بررسی رسمی logهای ممیزی صورت می‌گیرد، نوعی کنترل اداری کارآگاهی Detective Administrative است. بررسی داده‌های ممیزی باید عملکردی جدا از اجرای روزانه سیستم باشد.

تشخیص نفوذ و پیشگیری Intrusion Detection and Prevention

سازمانهای هشدار دهنده IDS در هنگام دسترسی یا اقدامات غیرمجاز، وقتی که سیستم‌های پیشگیری از نفوذ Intrusion prevention systems (IPSs) بر این نوع فعالیت نظارت می‌کنند در واقع برای جلوگیری از موفقیت اقدامات آنها فعالیت می‌کنند. از دستگاه‌های IDS و IPS می‌توان در طول تحقیقات استفاده کرد تا اطلاعاتی در مورد الگوهای ترافیکی که درست قبل از حمله موفقیت آمیز رخ می‌دهد، فراهم کرد. متخصصان امنیت باید دائماً دستگاه‌های IDS و IPS را تنظیم کنند تا از شناسایی صحیح یا جلوگیری از فعالیت آنها اطمینان یابند. از آنجا که تغییراتی در شیوه انجام حملات ایجاد می‌شود، این سیستم‌ها باید پیکربندی و به روز شوند.

مدیریت رخداد و اطلاعات امنیتی Security Information and Event Management (SIEM)

SIEM می‌تواند log و اطلاعات سیستم را برای مطابقت با الزامات نظارتی جمع آوری کند، مسئولیت پذیری داخلی را فراهم کرده، مدیریت ریسک را ارائه داده و نظارت و روند را انجام دهد. SIEM اطلاعات خام را از سیستم‌ها و دستگاه‌های مختلف ذخیره می‌کند و آن اطلاعات را در یک پایگاه داده واحد ذخیره می‌کند. متخصصان امنیت باید همکاری کنند تا مطمئن شوند که اقدامات مناسب پایش خواهد شد و از بررسی سوابق اطمینان حاصل شود. از آنجا که سیستم‌های SIEM مخزن متمرکز اطلاعات امنیتی هستند، سازمان‌ها باید مراقبت ویژه‌ای را برای تأمین امنیت کافی برای این سیستم‌ها انجام دهند تا اطمینان حاصل شود که مهاجمان نمی‌توانند به سوابق موجود دسترسی پیدا کنند و یا تغییر دهند.

نظارت مداوم Continuous Monitoring

هرگونه فعالیت ورود به سیستم و نظارت باید جزئی از برنامه نظارت مداوم سازمانی باشد. برنامه نظارت مداوم باید به گونه ای طراحی شود که نیازهای سازمان را برآورده سازد و به درستی اجرا شود تا از زیرساخت های مهم سازمان محافظت شود. سازمانها ممکن است بخواهند به عنوان یک سرویس یا CMaaS که توسط ارائه دهندگان خدمات ابری مستقر شده اند، نظارت مداوم را جستجو کنند.

نظارت بر خروج Egress Monitoring

نظارت بر خروج زمانی اتفاق می افتد که یک سازمان جریان خروجی اطلاعات را از یک شبکه به شبکه دیگر نظارت می کند. رایجترین شکل نظارت بر خروجی با استفاده از فایروال هایی که نظارت و کنترل ترافیک خارجی را انجام می دهند.

نشت داده ها Data leakage هنگامی رخ می دهد که داده های حساس به صورت عمدی یا سهواً برای پرسنل غیرمجاز فاش شود. نرم افزار پیشگیری از دست دادن داده یا Data Loss Prevention (DLP) سعی در جلوگیری از نشت داده ها دارد. این کار را با حفظ آگاهی از اقداماتی که با توجه به یک سند امکان پذیر است و نمی توان انجام داد، انجام می دهد. به عنوان مثال، ممکن است اجازه چاپ یک سند فقط در دفتر کار شرکت باشد. همچنین ممکن است ارسال سند از طریق ایمیل مجاز نباشد. نرم افزار DLP از فیلترهای ورودی و خروجی برای شناسایی داده های حساس که در حال خارج شدن از سازمان هستند، استفاده می کند و می تواند از بروز چنین نشتی هایی جلوگیری کند.

سناریوی دیگر ممکن است انتشار برنامه های محصول باشد که فقط در دسترس گروه فروش باشد. یک متخصص امنیتی می تواند سیاستی مانند موارد زیر را برای آن سند تنظیم کند:

- این امر به غیر از اعضای گروه فروش نمی تواند به کسی ارسال شود.
- قابل چاپ نمی باشد.
- قابل کپی کردن نمی باشد.

دو مکان وجود دارد که DLP قابل پیاده سازی می باشد:

- شبکه DLP: نصب شده در نقاط خروجی شبکه در نزدیکی محیط، و ترافیک شبکه را تجزیه و تحلیل می کند.

- نقاط پایانی DLP در ایستگاه‌های کاری کاربر نهایی End-User یا سرورهای موجود در سازمان اجرا می‌شود.
- می‌توان از هر دو روش دقیق و غیردقیق برای تعیین حساسیت استفاده کرد:
- ✓ روش‌های دقیق *Precise Methods*: این روش‌ها شامل ثبت محتوا هستند و تقریباً حادثه مثبت کاذب را صفر می‌کنند.
- ✓ روش‌های غیردقیق *Imprecise Methods*: این روش‌ها می‌توانند شامل کلمات کلیدی، واژگان، عبارات رایج، عبارات رایج گسترده، برچسب‌های فوق داده Metadata tags، تجزیه و تحلیل بیضوی و تجزیه و تحلیل آماری باشند.
- ارزش یک سیستم DLP در میزان دقت آن است که می‌تواند نشت داده‌های حساس را پیدا کرده و از آن جلوگیری کند.
- توجه داشته باشید
- پنهان سازی Steganography و سایه‌گذاری دیجیتالی Watermarking بعضی اوقات بخشی از نظارت بر خروجی هستند.

تأمین منابع Resource Provisioning

تأمین منابع روندی در عملیات امنیت است که تضمین می‌کند که یک سازمان فقط دارایی مورد نیاز خود را مستقر می‌کند. تأمین منابع باید از چرخه حیات منابع سازمان پیروی کند. برای مدیریت صحیح چرخه عمر منابع، یک سازمان باید موجودی دقیق دارایی را حفظ کرده و از فرآیندهای مناسب مدیریت پیکربندی Configuration Management Prozesse استفاده کند. منابعی که در تهیه آن نقش دارند عبارتند از دارایی‌های فیزیکی، دارایی‌های مجازی، دارایی‌های ابری و اپلیکیشن‌ها.

فهرست موجودی دارایی Asset Inventory

دارایی، هر کالای با ارزش برای یک سازمان از جمله دستگاه‌های فیزیکی و اطلاعات دیجیتال است. اگر هیچ سیستم اعدادی یا فهرست موجودی وجود نداشته باشد یا اینکه موجودی به روز نباشد، تشخیص در زمان سرقت دارایی یا استقرار نادرست غیرممکن است. کلیه تجهیزات باید فهرست شوند و کلیه اطلاعات مربوط به هر دستگاه باید حفظ و به روز باشد. هر دارایی باید کاملاً مستند باشد، از جمله شماره سریال، شماره مدل، نسخه سفت ابزار Firmware، نسخه سیستم

عامل، پرسنل مسئول و غیره. سازمان باید این اطلاعات را هم به صورت الکترونیکی و هم به صورت کپی کاغذی حفظ کند. حفظ این فهرست موجودی در تعیین زمان استقرار دارایی های جدید یا داراییهایی که در حال حاضر مستقر هستند که باید از آنجا استفاده شود، کمک می کند. دستگاه های امنیتی، مانند فایروال ها، دستگاه های ترجمه آدرس شبکه Network Address Translation (NAT) و IDS و IPS ها باید بیشترین توجه را به خود جلب کنند، زیرا این امر به امنیت فیزیکی و منطقی مربوط می شود. فراتر از این، دستگاه هایی که به راحتی می توانند به سرقت بروند، مانند لپ تاپ، تبلت و تلفن های هوشمند، باید قفل شوند. اگر این کار عملی نیست، بنابراین قفل کردن این نوع دستگاه ها را روی اشیاء ثابت (مثلاً استفاده از کابل قفل دار متصل به لپ تاپ) را باید در نظر گرفت.

هنگامی که این فناوری موجود است، ردیابی دستگاه های کوچک می تواند به کاهش از بین رفتن هر دو دستگاه و داده های آنها کمک کند. بسیاری از تلفن های هوشمند اکنون شامل نرم افزار ردیابی هستند که به ما امکان می دهد دستگاه را بعد از سرقت یا از بین رفتن با استفاده از ردیابی برج سلولی یا GPS پیدا کنیم.

یکی دیگر از ویژگی های مفید موجود در بسیاری از تلفن های هوشمند و سایر دستگاه های قابل حمل، ویژگی پاک کردن از راه دور است. این امر به کاربر اجازه می دهد تا سیگنالی را به دستگاه دزدیده شده ارسال کند و به وی دستور می دهد داده های موجود در دستگاه را پاک کند. به طور مشابه، این دستگاه ها به طور معمول با قابلیت قفل شدن از راه دور در هنگام جابجایی نیز همراه هستند.

کنترل دقیق استفاده از دستگاه های رسانه قابل حمل می تواند به جلوگیری از خروج اطلاعات حساس از شبکه کمک کند، که شامل سی دی، دی وی دی، فلش مموری و هارد اکسترنال است. اگرچه قوانین کتبی باید در مورد استفاده از این دستگاه ها اعمال شود، اما استفاده از سیاست های امنیتی برای جلوگیری از کپی کردن داده ها در این نوع رسانه ها نیز امکان پذیر است. مجاز بودن کپی کردن داده ها در این نوع درایوها تا زمانی که داده ها رمزگذاری شوند نیز امکان پذیر است. اگر این وظایف توسط سیستم عامل شبکه ارائه شده است، باید آنها را مستقر کنید. برای افراد غیرمجاز نباید امکان دسترسی و دستکاری هر دستگاهی وجود داشته باشد. مداخله پیش فرض، آسیب رساندن یا تغییر پیکربندی یک دستگاه است. برنامه های تأیید یکپارچگی باید توسط نرم افزارها مورد استفاده قرار گیرد تا به دنبال شواهدی از دستکاری داده ها، خطاها و حذف ها باشند.

رمزگذاری داده‌های حساس ذخیره شده در دستگاه‌ها می‌تواند در جلوگیری از قرار گرفتن در معرض سرقت اطلاعات در رخداد سرقت یا جلوگیری از دسترسی نامناسب دستگاه به شما کمک کند.

مدیریت پیکربندی Configuration Management

اگرچه این زیر مجموعه‌ای از مدیریت تغییر است، مدیریت پیکربندی به طور خاص خود را به بیرون آوردن از هرج و مرج و ایجاد نظم متمرکز می‌کند که می‌تواند هنگامی رخ دهد که چندین مهندس و تکنسین دسترسی اداری به رایانه‌ها و دستگاه‌هایی داشته باشند که باعث فعالیت در شبکه می‌شوند. این فرآیند همان روند اساسی را دارد که تحت عنوان "فرآیندهای مدیریت تغییر" مورد بحث قرار گرفته است، اما با توجه به تأثیر تغییرات متضاد (و در بعضی موارد بلافاصله) در یک شبکه، می‌تواند اهمیت بیشتری را نیز در این جا به وجود آورد.

وظایف مدیریت پیکربندی عبارتند از:

- ✓ گزارش وضعیت فرایند تغییر.
- ✓ ویژگی‌های عملکردی و فیزیکی هر مورد پیکربندی مستند شود.
- ✓ انجام ضبط اطلاعات و کنترل نسخه.
- ✓ تغییرات در آیتم‌های پیکربندی کنترل شده و نسخه‌های موارد پیکربندی از کتابخانه نرم افزار صادر شود.

توجه داشته باشید

در زمینه مدیریت پیکربندی، یک نرم افزار کتابخانه‌ای Software Library یک منطقه کنترل شده است که فقط برای کاربران محدود به استفاده از یک روش تایید شده است. یک مورد پیکربندی Configuration Item (CI) یک زیر مجموعه منحصر به فرد قابل شناسایی از سیستم است که نشان دهنده کوچکترین بخشی است که باید تحت یک روش کنترل پیکربندی مستقل شود. هنگامی که یک عملیات به CIهای فردی شکسته می‌شود، این فرایند را شناسایی پیکربندی

Configuration Identification می‌نامند.

نمونه‌هایی از این نوع تغییرات عبارتند از:

- پیکربندی سیستم عامل
- پیکربندی نرم افزار
- پیکربندی سخت افزار

از دیدگاه CISSP، بزرگترین سهم کنترل های مدیریت پیکربندی تضمین می کند که تغییرات در سیستم باعث کاهش ناخواسته امنیت نمی شوند. به همین دلیل، باید تمام تغییرات را مستندسازی کرد و کلیه نمودارهای شبکه، از نظر منطقی و فیزیکی، باید مرتباً و به طور مداوم به روز شوند تا وضعیت هر پیکربندی را اکنون و نه آنطور که دو سال پیش بود، دقیقاً نشان دهند. تأیید اینکه تمام خط مشی های مدیریت پیکربندی دنبال می شوند باید یک فرایند مداوم باشد.

در بسیاری موارد، تشکیل یک صفحه (Board) کنترل پیکربندی مفید است. وظایف صفحه کنترل پیکربندی می تواند شامل موارد زیر باشد:

- اطمینان از اینکه تأیید، آزمایش، مستندسازی و تغییرات، صحیح پیاده سازی شده است.
- بطور دوره ای در مورد گزارش های حسابداری وضعیت پیکربندی جلسه بحث شود.
- حفظ مسئولیت و اطمینان از ایجاد تغییرات، صحت و درستی تأیید سیستم را به خطر نمی اندازد.

به طور خلاصه، مؤلفه های مدیریت پیکربندی عبارتند از:

- کنترل پیکربندی
- پیکربندی وضعیت حسابداری
- پیکربندی ممیزی

دارایی های فیزیکی Physical Assets

دارایی های فیزیکی شامل سرورها، رایانه های رومیزی، لپ تاپ ها، دستگاه های سیار و دستگاه های شبکه است که در شرکت مستقر هستند. دارایی های فیزیکی باید براساس نیاز سازمانی مستقر شده و از بین بروند. به عنوان مثال، فرض کنید سازمان یک نقطه دسترسی بی سیم را برای استفاده توسط ممیز شخص ثالث مستقر می کند. تأمین منابع مناسب باید اطمینان حاصل کند که هنگامی که ممیز شخص ثالث دیگر نیازی به دسترسی به شبکه نداشته باشد، نقطه دسترسی بی سیم وی حذف شود. بدون مدیریت فهرست موجودی و مدیریت پیکربندی صحیح، ممکن است نقطه دسترسی بی سیم مستقر شده در برخی از نقاط برای انجام حمله به شبکه بی سیم قابل استفاده باشد.

دارایی‌های مجازی Virtual Assets

دارایی‌های مجازی شامل شبکه‌های تعریف شده نرم افزاری Software-Defined Networks، شبکه‌های منطقه ذخیره سازی مجازی (VSANs) Virtual Storage-area Networks، سیستم عامل‌های مهمان مستقر در ماشین‌های مجازی (VMs) Virtual Machines و روترهای مجازی است. مانند دارایی‌های فیزیکی، استقرار و رد دارایی‌های مجازی باید به عنوان بخشی از مدیریت پیکربندی کاملاً کنترل شود زیرا دارایی‌های مجازی، دقیقاً مانند دارایی‌های فیزیکی، می‌توانند به خطر بیفتند. به عنوان مثال، یک ماشین مجازی ویندوز ۱۰ که در ویندوز سرور R2 ۲۰۱۲ مستقر است باید فقط تا زمانی که نیاز به آن می‌باشد، حفظ شود. تا زمانی که از ماشین مجازی استفاده می‌شود، مهم است که اطمینان حاصل شود که بروزرسانی‌های مناسب، پچ‌ها و کنترل‌های امنیتی به عنوان بخشی از مدیریت پیکربندی روی آن مستقر شده اند. هنگامی که کاربران دیگر به ماشین مجازی دسترسی ندارند، ماشین مجازی باید حذف شود.

ذخیره سازی مجازی هنگامی اتفاق می‌افتد که ذخیره سازی فیزیکی از چندین دستگاه ذخیره شبکه در یک فضای ذخیره سازی مجازی منفرد ساخته شود. بلوک مجازی سازی Block Virtualization ذخیره منطقی را از ذخیره فیزیکی تفکیک می‌کند. مجازی سازی فایل File Virtualization، وابستگی بین داده‌های قابل دسترسی در سطح فایل و محل ذخیره فیزیکی فایل‌ها را از بین می‌برد. حافظه مجازی مبتنی بر میزبان Host-Based Virtual Storage نیاز به اجرای نرم افزار بر روی هاست دارد. فضای مجازی مبتنی بر دستگاه ذخیره سازی Storage Device-Based Virtual Storage روی یک کنترلر ذخیره سازی کار می‌کند و به دیگر کنترلرهای ذخیره سازی اجازه می‌دهد تا متصل شوند.

ذخیره سازی مجازی مبتنی بر شبکه Network-Based Virtual Storage از دستگاه‌های مبتنی بر شبکه مانند iSCSI یا کانال فیبر نوری برای ایجاد یک راه حل ذخیره سازی استفاده می‌کند.

دارایی‌های ابری Cloud Assets

دارایی‌های ابری شامل خدمات ابری، ماشین‌های مجازی، شبکه‌های ذخیره سازی و سایر خدمات ابری است که از طریق ارائه دهنده خدمات ابری Cloud Service Provider منعقد می‌شوند. دارایی‌های ابری معمولاً مبتنی بر صورتحساب Billed Based می‌باشند و باید با دقت تهیه و نظارت شوند تا از پرداخت مبالغ خدماتی که نیازی به سازمان ندارند، جلوگیری شود. مدیریت

پیکربندی باید اطمینان داشته باشد که از سیاست های نظارت مناسب استفاده شده تا فقط منابعی که مورد نیاز هستند مستقر می شوند.

برنامه های کاربردی (اپلیکیشن ها) Applications

اپلیکیشن ها شامل برنامه های تجاری است که به صورت محلی نصب می شوند، سرویس های وب و هرگونه سرویس برنامه های کاربردی ابری مانند نرم افزار به عنوان یک سرویس (Such as Software as a Service (SaaS)). تعداد مناسب مجوزهای لیسانس باید برای کلیه برنامه های تجاری حفظ شود. یک سازمان باید به طور دوره ای نیازهای مجوز لیسانس خود را بررسی کند. برای استقرار ابری از خدمات نرم افزاری، باید از مدیریت پیکربندی استفاده شود تا تضمین شود که فقط پرسنلی که نیازهای معتبری به نرم افزار دارند، دسترسی پیدا می کنند.

مفاهیم عملیات امنیتی Security Operations Concepts

در طول این کتاب، شاهد مراجعه به سیاست ها و اصولی هستید که می توانند کلیه عملیات امنیتی را راهنمایی کنند. در این بخش، برخی مفاهیم را به طور کامل تر بررسی می کنیم که قبلاً به آنها پرداخته شده و برخی از موضوعات جدید مربوط به حفظ عملیات امنیتی را معرفی خواهیم کرد.

نیاز به دانستن / حداقل امتیاز Need to Know/Least Privilege

در رابطه با اجازه دسترسی به منابع و اختصاص حقوق برای انجام عملیات، همیشه مفهوم حداقل امتیاز (معروف به نیاز به دانستن) بکار برده می شود. در زمینه دسترسی به منابع، بدان معنی است که به طور پیش فرض نباید دسترسی داشته باشد. دسترسی کاربران فقط براساس منابع مورد نیاز برای انجام کارشان باشد و بعد از تأیید نیاز به دسترسی توسط یک سرپرست (Supervisor) به صورت اجرای دستی Manual می باشد.

کنترل دسترسی اختیاری (Discretionary Access Control (DAC) و کنترل دسترسی مبتنی بر نقش (Role-Based Access Control (RBAC) نمونه هایی از سیستم های مبتنی بر نیاز کاربر به دانستن هستند. برای اطمینان از حداقل امتیاز، مستلزم شناسایی شغل کاربر است و به هر کاربر حداقل میزان امتیاز لازم برای کارهایش اعطا می شود. مثال دیگر پیاده سازی View ها در یک پایگاه داده است. نیاز به دانستن مستلزم این است که اپراتور از سیستم لازم برای انجام وظیفه اش حداقل آگاهی را داشته باشد.

مدیریت حساب ها، گروه ها و نقش ها Managing Accounts, Groups, and Roles

دستگاه ها، رایانه ها و اپلیکیشن ها، حساب ها و نقش های کاربر و گروه را پیاده سازی می کنند تا دسترسی را مجاز یا رد کنند. حسابهای کاربری برای هر کاربر نیاز به دسترسی ایجاد می کند. حسابهای گروهی برای پیکربندی مجوزهای منابع استفاده می شوند. حسابهای کاربری به حسابهای گروه مناسب اضافه می شوند تا مجوزهای اعطاء شده آن گروه را به ارث ببرند. همچنین می توان حسابهای کاربری را به نقش ها اختصاص داد. نقش ها اغلب توسط اپلیکیشن ها استفاده می شوند.

متخصصان امنیت باید حساب های زیر را درک کنند:

✓ حساب ادمین داخلی یا ریشه *Root or built-in administrator account*

قدرتمندترین حسابهای سیستم هستند. بهتر است بعد از اینکه حساب دیگری با همین امتیازات ایجاد شد، اینگونه حساب کاربری قبلی غیرفعال شود زیرا بیشتر این نام ها به خوبی شناخته شده اند و می توانند توسط مهاجمان استفاده شوند. اگر تصمیم به نگهداری این حساب ها هست، بیشتر فروشندگان پیشنهاد می کنند نام حساب را تغییر داده و رمز عبور پیچیده ای به آن داده شود. حسابهای ریشه یا ادمین فقط هنگام انجام وظایف مدیریتی باید مورد استفاده قرار گیرند و همیشه باید این حسابها ممیزی شوند.

✓ حساب خدمات *Service account* از این حسابها برای اجرای سرویس ها و اپلیکیشن های سیستم استفاده می شود. بنابراین، متخصصان امنیت می توانند دسترسی حساب خدمات به سیستم را محدود کنند. همیشه حسابهای کاربری پیش فرض استفاده شده را مورد تحقیق قرار گیرند. مطمئن شوید که گذرواژه های این حسابها بطور منظم تغییر می کنند. استفاده از این حسابها باید همیشه ممیزی شوند.

✓ حسابهای ادمین عادی *Regular administrator accounts* این حسابهای ادمین فقط

برای یک فرد مجزا ایجاد و اختصاص داده می شوند. هر کاربر که دارای یک حساب کاربری ادمین می باشد نیز باید از این نوع حساب برای انجام کارهای روزمره و عادی داشته باشد. حسابهای ادمین فقط هنگام انجام وظایف در سطح ادمین باید مورد استفاده قرار گیرند و همیشه باید این حسابها ممیزی شوند.

✓ حسابهای کاربری قدرتمند *Power user accounts* این حسابها نسبت به حسابهای

عادی کاربر دارای امتیازات و مجوزهای بیشتری هستند. این حسابها باید بطور منظم

مورد بررسی قرار گیرند تا اطمینان حاصل شود که فقط کاربرانی که مجوزهای سطح بالاتری احتیاج دارند، دارای این حسابها هستند. اکثر سیستم عامل های مدرن توانایی کاربران قدرتمند را محدود می کنند یا حتی این نوع حساب را به طور کامل حذف می کنند.

✓ **حسابهای کاربر عادی** *Regular user accounts* حسابهایی است که کاربر در حین وظایف عادی روزمره خود از آنها استفاده می کند. این حسابها باید کاملاً از اصل حداقل امتیازات پیروی کنند.

تفکیک وظایف Separation of Duties

مفهوم تفکیک وظایف پیش بینی می کند که عملیات حساس بین چندین کاربر تقسیم می شود تا هیچ کس حق استفاده و حق دسترسی به این عملیات را به تنهایی برخوردار نباشد. تفکیک وظایف در جلوگیری از تقلب با اطمینان از اینکه هیچ یک از افراد نمی توانند یک سیستم را به خطر بیندازند بسیار ارزشمند است. تفکیک وظایف یک کنترل ادمین پیشگیرانه Preventive Administrative Control محسوب می شود. به عنوان نمونه یک شخص می تواند درخواست پرداخت را شروع کند و دیگری مجاز به پرداخت شود. این امر گاهی به کنترل دوگانه Dual control نیز معروف است.

چرخش شغل Job Rotation

از منظر امنیتی، چرخش شغل به آموزش چندین کاربر برای انجام وظایف در یک موقعیت برای کمک به جلوگیری از کلاهبرداری توسط هر یک از کارمندان اشاره دارد. ایده آن اینگونه است که با آشنا کردن چندین نفر با کارکردهای قانونی این موقعیت، احتمال اینکه فعالیتهای غیرمعمول توسط هر یک از افراد مشاهده شود، بیشتر می شود و اغلب در تعطیلات اجباری مورد استفاده قرار می گیرد، که در آن کلیه کاربران موظف هستند کار خود را تعطیل کرده و به دیگری اجازه می دهند موقعیتشان را پر کنند، که فرصتی برای کشف فعالیت غیرمعمول می باشد. فراتر از جنبه های امنیت چرخش شغل، مزایای دیگر شامل موارد زیر است:

- آموزش پشتیبان گیری در صورت بروز شرایط اضطراری
- محافظت در برابر کلاهبرداری
- آموزش متقابل کارمندان

- چرخش وظایف، تفکیک وظایف و تعطیلات اجباری همه کنترل‌های مدیریتی هستند.

رویه‌های حساس اطلاعات Sensitive Information Procedures

کنترل دسترسی و استفاده از آن در جلوگیری از دسترسی غیرمجاز به داده‌های حساس برای امنیت سازمان از اهمیت ویژه برخوردار است. از این رو، دستیابی امن به اطلاعات حساس بسیار مهم است. گرچه تمایل داریم که از دید اطلاعات شرکت بیندیشیم، اما بسیار مهم است که این شرکت از اطلاعات خصوصی مشتریان و کارمندان خود نیز محافظت کند. نشت اطلاعات شخصی کاربران و مشتریان حداقل باعث شرمساری برای شرکت و احتمالاً جریمه و دعوای قضایی می‌شود.

صرف نظر از این که آیا هدف، محافظت از داده‌های شرکت یا داده‌های شخصی است، مهم این است که اصول کنترل دسترسی در هر دو مجموعه داده اعمال شود. هنگام بررسی دسترسی به رویه‌ها و سیاست‌های کنترل دسترسی، باید به سؤالات زیر پاسخ داده شود:

- آیا داده‌هایی که برای وظیفه کاربر لازم نیست در اختیار کاربر قرار دارد؟
- آیا بسیاری از کاربران به داده‌های حساس دسترسی دارند؟

حفظ رکورد Record Retention

کنترل دسترسی مناسب بدون ممیزی امکان پذیر نیست، و این امکان را دارد تا قبل از تحقق کامل، فعالیت‌ها را ردیابی کرده و مشکلات را کشف کرد. از آنجا که این مسئله گاهی اوقات می‌تواند منجر به تجزیه و تحلیل داده‌های فراوانی شود، فقط بر حساس‌ترین فعالیت‌ها نظارت داشته و تمامی سوابق را حفظ و بررسی می‌کند. علاوه بر این، در بسیاری از موارد شرکت‌ها به موجب قانون یا مقررات مکلفند سوابق داده‌های خاص را حفظ کنند.

بیشتر سیستم‌های ممیزی امکان پیکربندی گزینه‌های حفظ و نگهداری داده را فراهم کنند. در برخی موارد عملیات پیش فرض، شروع به نوشتن روی سوابق قدیمی در log می‌کنند که log به طور کامل پر شده است. حتی توصیه می‌شود در موارد بسیار حساس، وقتی یک log امنیتی پر شده و هیچ رویداد دیگری را نمی‌توان ثبت کرد، سرور دسترسی را قطع کند.

نظارت بر امتیازات ویژه Monitor Special Privileges

به ناچار برخی از کاربران، به ویژه سرپرستان یا افرادی که در بخش پشتیبانی فناوری اطلاعات هستند، به حقوق و امتیازات ویژه‌ای احتیاج دارند که سایر کاربران از آن برخوردار نیستند. به عنوان مثال، ممکن است نیاز باشد که مجموعه‌ای از کاربرانی که در Help desk کار می‌کنند، قادر به تنظیم مجدد گذرواژه‌ها یا ایجاد تغییراتی در حساب کاربری باشند. این نوع حقوق مسئولیت، اعمال حقوق اخلاقی و مسئولیت پذیری را با خود به همراه دارد.

اگرچه در یک دنیای کامل فرض کنیم که می‌توانیم این انتظار را از همه کاربران داشته باشیم، اما در دنیای واقعی می‌دانیم که همیشه درست نیست. بنابراین، یکی از مواردی که باید نظارت شود استفاده از این امتیازات است. اگرچه ما باید به میزان نظارت انجام شده و میزان داده‌های حاصل از این نظارت توجه داشته باشیم، ضبط اعمال امتیازات ویژه نباید قربانی شود، حتی اگر این به معنای ذخیره منظم داده‌ها به عنوان فایل log و پاک سازی سیستم جمع آوری رخداده‌ها باشد.

چرخه عمر اطلاعات Information Life Cycle

در عملیات امنیتی، متخصصان امنیت باید چرخه عمر اطلاعات را درک کنند، که شامل ایجاد، توزیع، استفاده، نگهداری و دسترسی اطلاعات است. پس از جمع آوری اطلاعات باید طبقه بندی شود تا اطمینان حاصل شود که فقط پرسنل مجاز می‌توانند به اطلاعات دسترسی داشته باشند.

توافقنامه‌های سطح خدمات Service-Level Agreements

توافقنامه‌های سطح خدمات (SLAs) Service-Level Agreements توافق نامه هایی در مورد توانایی سیستم پشتیبانی برای پاسخگویی به مشکلات در یک بازه زمانی مشخص ضمن ارائه سطح خدمات توافق شده است. آنها می‌توانند بین بخش‌های داخلی یا خارج از شرکت ارائه دهنده خدمات باشند. با توافق در مورد سرعتی که در آن به مشکلات مختلفی رسیدگی می‌شود، مقدار پیش بینی شده‌ای برای پاسخ به مشکلات ارائه می‌شود که در نهایت از حفظ دسترسی به منابع پشتیبانی می‌کند.

SLA باید توضیحی در مورد خدمات ارائه شده و میزان خدمات و معیارهای مورد انتظار باشد که مشتری می‌تواند انتظار داشته باشد. همچنین وظایف و مسئولیتهای هر یک از طرفین SLA را

شامل می‌شود. این لیست مشخصات خدمات، استثنائات، سطح خدمات، مراحل افزایش سرعت و هزینه را نشان می‌دهد. این شرط باید در مورد پرداخت به مشتریان ناشی از نقض SLA باشد. زمانی که SLAها قابل انتقال هستند، طبق قانون قابل انتقال نیستند. معیارهایی که باید اندازه‌گیری شوند شامل در دسترس بودن سرویس، سطح خدمات، نرخ نقص، کیفیت فنی و امنیت می‌باشد. SLAها باید بطور دوره‌ای مورد بررسی قرار گیرند تا تضمین شود که نیازهای شغلی، محیط فنی یا بار کاری تغییر نکرده‌اند. علاوه، باید معیارها، ابزارهای اندازه‌گیری و فرآیندها مورد بررسی قرار گیرند تا ببینند که آیا بهبود یافته‌اند.

حفاظت از منابع Resource Protection

منابع سازمانی شامل دارایی که می‌توانیم ببینیم و لمس کنیم (ملموس Tangible) مانند رایانه‌ها و چاپگرها و دارایی‌هایی که نمی‌توانیم آنها را ببینیم و لمس کنیم (ناملموس Intangible) مانند اسرار تجاری و پردازش‌ها. اگرچه به طور معمول حمایت از منابع به خاطر، جلوگیری از فساد منابع دیجیتال و جلوگیری از آسیب رساندن به منابع فیزیکی استفاده می‌شود، این مفهوم همچنین شامل حفظ دسترسی منابع نیز می‌باشد. در این بخش، در مورد هر دو جنبه حمایت از منابع بحث می‌کنیم.

محافظت از دارایی‌های ملموس و ناملموس Protecting Tangible and Intangible Assets

در بعضی موارد از با ارزش ترین دارایی‌های یک شرکت موارد ناملموس مانند دستور العمل‌های مخفی، فرمول‌ها و اسرار تجاری است. در موارد دیگر، ارزش شرکت از دارایی‌های فیزیکی آن شرکت مانند تاسیسات، تجهیزات و استعدادهای افراد شرکت بدست می‌آید. همه منابع در نظر گرفته شده و باید در یک برنامه جامع حمایت از منابع درج شوند. در این بخش، برخی از دغدغه‌های خاص در مورد این نوع منابع مختلف مورد بررسی قرار گرفته است.

تاسیسات Facilities

معمولاً بزرگترین دارایی ملموس که یک سازمان دارد، ساختمانی است که در آن فعالیت می‌کند و زمین‌های اطراف آن می‌باشد. امنیت فیزیکی که بعداً در این فصل مطرح می‌شود، و تأکید

می کند که تست آسیب پذیری باید شامل کنترل های امنیتی خود تأسیسات باشد. برخی از نمونه های تست آسیب پذیری در ارتباط با تأسیسات عبارتند از:

- آیا درها به صورت خودکار بسته می شوند و در صورت باز بودن بیش از حد، زنگ هشدار به صدا در می آید؟
 - آیا مکانیسم های حفاظت از مناطق حساس مانند اتاق های سرور و کمدهای سیم کشی کافی و عملیاتی هستند؟
 - آیا سیستم مهار آتش کار می کند؟
 - آیا اسناد حساس بر خلاف انداختن در سطل زباله، خرد شده اند؟
- فراتر از مشکلات دسترسی، سیستم های اصلی مورد نیاز برای اطمینان از عدم قطع عملیات، عبارتند از: شناسایی آتش / مهار آتش، HVAC از جمله کنترل دما و رطوبت، سیستم های آب و فاضلاب، برق / پشتیبان برقی، تجهیزات ارتباطی و تشخیص نفوذ.

سخت افزار Hardware

یکی دیگر از دارایی های ملموس تر که باید از آن محافظت شود، تمام سخت افزاری است که باعث می شود شبکه کار کند. این دارایی ها نه تنها شامل رایانه ها و پرینترهایی است که کاربران با آنها مستقیماً در تماس هستند بلکه دستگاه های زیرساختی مانند روترها، سوئیچ ها و وسایل فایروال کابردی هستند که هرگز مشاهده نمی شوند.

از نظر مدیریتی، این دستگاه ها معمولاً از راه دور اداره می شوند. برای محافظت از دسترسی به این ویژگی های مدیریتی و همچنین محافظت از داده ها و دستوراتی که از طریق شبکه به این دستگاه ها منتقل می شود، باید توجه ویژه ای صورت گیرد. برخی از دستورالعمل های خاص شامل موارد زیر است:

- کلیه گذرواژه های پیش فرض سرور را در دستگاه ها تغییر دهید.
- تعداد کاربرانی که دسترسی از راه دور به این دستگاه ها دارند را محدود کنید.
- به جای Telnet (که دستورات را با متن واضح ارسال می کند) از یک ابزار خط فرمان رمزگذاری شده مانند Secure Shell (SSH) استفاده کنید.
- سیستم های مهم را به صورت محلی مدیریت کنید.
- دسترسی فیزیکی به این دستگاه ها را محدود کنید.

نرم افزار Software

دارایی‌های نرم افزار شامل اپلیکیشن‌های مناسب، اسکریپت‌ها یا فایل‌های دسته‌ای هستند که برای عملکرد سازمان بسیار مهم هستند. کدنویسی امن و انجام توسعه آن می‌تواند به جلوگیری از ضعف در این سیستم‌ها کمک کند. همچنین باید به جلوگیری از سرقت این دارایی‌ها نیز توجه داشت.

علاوه بر این، نظارت دقیق بر استفاده از اپلیکیشن‌های و سیستم‌های تجاری در شرکت می‌تواند از نقض غیر عمدی قراردادهای مجوزلیسانس جلوگیری کند. یکی از مزایای استفاده از اپلیکیشن‌های مورد نیاز کاربران برای انجام کار خود این است که تعداد کاربرانی که دارای اپلیکیشن هستند را محدود کرده و به جلوگیری از فرسودگی مجوزهای نرم افزار کمک می‌کند.

دارایی‌های اطلاعاتی Information Assets

دارایی‌های اطلاعاتی آخرین نوع دارایی است که باید مورد بحث قرار گیرد، اما به هیچ وجه کمترین اهمیت را ندارد. هدف اصلی امنیت عملیات، محافظت از داراییهای اطلاعاتی است که در سیستم مستقر هستند. این دارایی‌ها شامل دستور العمل‌ها، فرآیندها، اسرار تجاری، طرح‌های محصول و هر نوع اطلاعات دیگری است که به شرکت امکان می‌دهد تا رقابت خود را در صنعت حفظ کند. اصول طبقه بندی داده‌ها و کنترل دسترسی با شدت بیشتری روی این دارایی‌ها اعمال می‌شود. در بعضی موارد، ممکن است تعیین ارزش دلار این دارایی‌ها دشوار باشد، اگرچه ممکن است همه را درگیر کرده که دارایی بسیار مهم می‌باشد. به عنوان مثال فرمول مخفی کوکاکولا سالهاست که به دلیل ارزش آن برای شرکت، به طور دقیق محافظت می‌شود.

مدیریت دارایی Asset Management

در فرآیند مدیریت این دارایی‌ها باید به چندین موضوع رسیدگی شود. مطمئناً دسترسی به دارایی باید از نزدیک کنترل شود تا از حذف، سرقت یا فساد آن (در مورد دارایی‌های دیجیتال) و از آسیب‌های فیزیکی (در مورد دارایی‌های فیزیکی) جلوگیری شود. علاوه بر این، در صورت نیاز دارایی باید در دسترس باشد. این بخش روش‌های تضمین دسترسی، احراز هویت و یکپارچگی را در بر می‌گیرد.

افزونگی و تحمل خطا Redundancy and Fault Tolerance

یکی از راه‌های دسترسی بی وقفه به دارایی‌های اطلاعاتی، افزونگی و تحمل خطا است. افزونگی به ارائه چندین مورد از یک مولفه فیزیکی یا منطقی اشاره دارد به گونه‌ای که در صورت عدم موفقیت اولین مولفه، در دسترس می‌باشد. تحمل خطا مفهوم گسترده تری است که افزونگی را شامل می‌شود و به هر فرآیندی اشاره دارد که به یک سیستم اجازه می‌دهد در صورت عدم موفقیت، دارایی‌های اطلاعاتی را در دسترس قرار دهد.

در بعضی موارد، افزونگی در لایه فیزیکی اعمال می‌شود، مانند افزونگی شبکه که توسط ستون فقرات دوگانه Dual Backbone در محیط شبکه محلی یا با استفاده از چندین کارت شبکه در یک سرور مهم ایجاد می‌شود. در موارد دیگر، افزونگی به صورت منطقی اعمال می‌شود، مانند زمانی که روتر در صورت عدم موفقیت یک مسیر، مسیرهای مختلفی را برای رسیدن به مقصد شناسایی می‌کند.

اقدامات متقابل تحمل خطا برای طراحی قابلیت اطمینان و مبارزه با تهدیدات طراحی شده اند. اگرچه تحمل خطا می‌تواند افزونگی باشد، همچنین به سیستم هایی مانند آرایه‌های اضافی دیسک‌های مستقل Redundant Array of Independent Disks (RAID) اشاره دارد که در آن داده‌ها در چندین دیسک نوشته می‌شود به گونه‌ای که دیسک نتواند خراب شود و داده‌ها به سرعت از باقی مانده دیسک‌های موجود در آرایه بدون استفاده از نوار پشتیبان قابل تهیه باشند. آگاه باشید که تعدادی از انواع RAID تحمل خطا را ارائه نمی‌دهند. صرف نظر از تکنیک مورد استفاده برای تحمل خطا، یک سیستم باید قابلیت تشخیص و اصلاح خطا را داشته باشد.

پشتیبان گیری و بازیابی سیستم‌ها Backup and Recovery Systems

اگرچه در این فصل پوشش کاملی از سیستم‌های تهیه پشتیبان و بازیابی وجود دارد، ولی در اینجا می‌توان به نقش عملیات در انجام آن فعالیت‌ها تأکید کرد. پس از طراحی برنامه زمانی تهیه نسخه پشتیبان، کارهای روزانه‌ای در رابطه با اجرای طرح انجام می‌شود. یکی از مهمترین بخش‌های این سیستم یک فرایند تست مداوم می‌باشد تا مطمئن شود که در صورت نیاز به بازیابی، کلیه نسخه‌های پشتیبان قابل استفاده است. زمان کشف اینکه پشتیبان گیری موفقیت آمیز نیست، در طول تست انجام می‌شود نه در طی یک بازیابی زنده live recovery.

هویت و مدیریت دسترسی Identity and Access Management

از منظر عملیات، مهم این است که بدانیم که مدیریت این موارد یک فرایند مداوم است که ممکن است نیاز به ایجاد حساب، حذف حساب، ایجاد و پر کردن گروه‌ها و مدیریت مجوزهای مرتبط با همه این مفاهیم باشد. حصول اطمینان از اینکه حقوق انجام این اقدامات به شدت کنترل می‌شود و انجام یک فرایند رسمی برای از بین بردن مجوزها هنگامی که دیگر لازم نیستند و همچنین غیرفعال کردن حساب‌هایی که دیگر لازم نیستند.

یکی دیگر از نکات قابل توجه، کنترل استفاده از حسابهای ممتاز یا حسابهای دارای حقوق و مجوزهایی می‌باشد که از حسابهای یک کاربر معمولی فراتر رفته است. اگرچه این امر به وضوح در مورد حساب‌های ادمین، حساب‌های ریشه یا حساب‌های ادمین داخلی (که در برخی از سیستم عامل‌ها به عنوان حساب‌های ریشه نامیده می‌شوند) که دارای مجوزهای گسترده‌ای هستند، صدق می‌کند، بلکه در مورد هر حساب دیگری که امتیازات ویژه‌ای را نیز به کاربر اعطا می‌کند، صدق می‌کند.

علاوه بر این، باید کنترل شدید بر تعداد زیادی از گروههای داخلی موجود در ویندوز برای اعطای حقوق ویژه به اعضای گروه، حفظ شود. هنگام استفاده از این گروه‌ها، امکان دارد به امتیازات گروه‌های پیش فرض برای اهدافمان نیازی نداشته باشیم و بخواهیم برخی از امتیازات را از گروه‌های پیش فرض حذف کرده تا از مفهوم حداقل امتیاز حمایت شود.

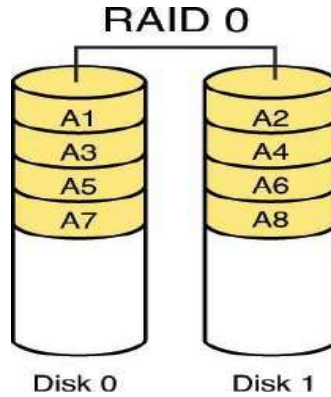
مدیریت رسانه Media Management

مدیریت رسانه بخش مهمی از امنیت عملیات است زیرا رسانه، مکانی می‌باشد که داده‌ها در آن ذخیره می‌شوند. مدیریت رسانه‌ها شامل RAID، SAN، NAS، HSM است.

آرایه‌های اضافی دیسک‌های مستقل Redundant Array of Independent Disks (RAID)

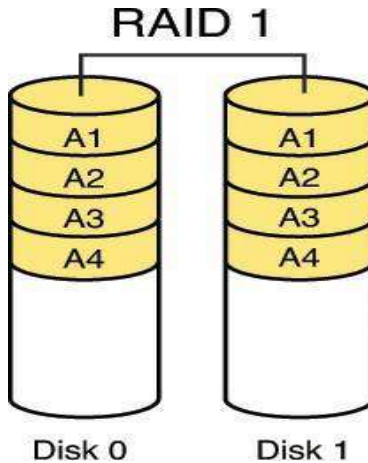
به سیستمی اطلاق می‌شود که در آن از چندین درایو سخت استفاده می‌شود تا یک تقویت عملکرد یا تحمل خطا برای داده‌ها فراهم شود. هنگامی که ما در مورد تحمل خطا در RAID صحبت می‌کنیم، منظور ما حفظ دسترسی به داده‌ها حتی در زمان خرابی درایو بدون بازیابی داده‌ها از رسانه پشتیبان است. موارد زیر انواع RAID می‌باشد که باید با آنها آشنا باشید.

RAID 0، که به آن نوار دیسک (Disk Striping) نیز گفته می شود، داده ها را در درایوهای مختلف می نویسد. اگر چه عملکرد را بهبود می بخشد، اما تحمل خطا را ارائه نمی دهد. شکل ۲-۷ RAID 0 را نشان می دهد.



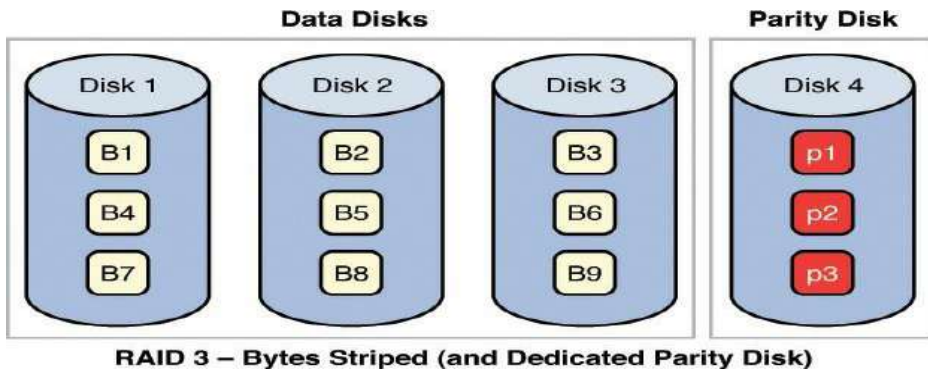
شکل ۲-۷: RAID 0

RAID 1، همچنین همانندسازی دیسک (Disk Mirroring) نامیده می شود، از دو دیسک استفاده می کند و یک نسخه از داده ها را در هر دو دیسک می نویسد و تحمل خطا را در صورت شکست یا خرابی یک درایو ارائه می کند. شکل ۳-۷ RAID 1 را نشان می دهد.



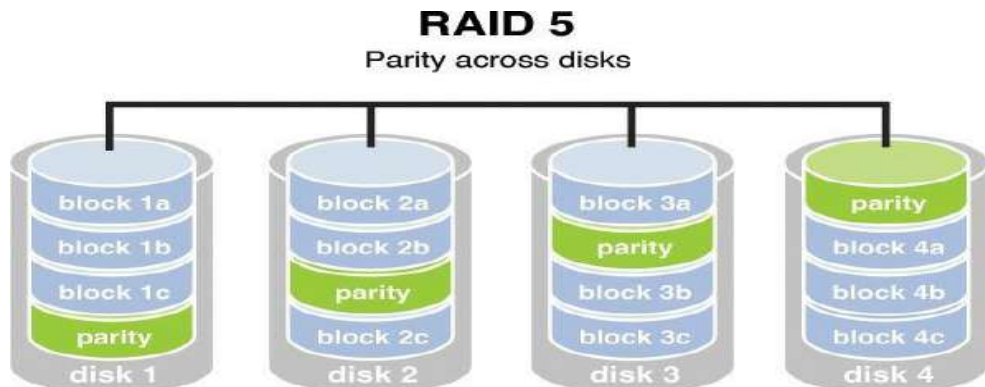
شکل ۳-۷: RAID 1

RAID 3، که نیاز به حداقل سه درایو دارد، همچنین نیاز دارد که داده‌ها در همه درایوها مانند نوار نوشته و سپس اطلاعات یکسان (Parity Information) در یک درایو اختصاصی نوشته شوند. از اطلاعات یکسان برای بازیابی اطلاعات در صورت خرابی تک درایو استفاده می‌شود. نقطه ضعف این است که درایو یکسان اگر بدعمل کند یا خراب شود یک نقطه شکست محسوب می‌شود. شکل ۷-۴ RAID 3 را نشان می‌دهد.



شکل ۷-۴: RAID3

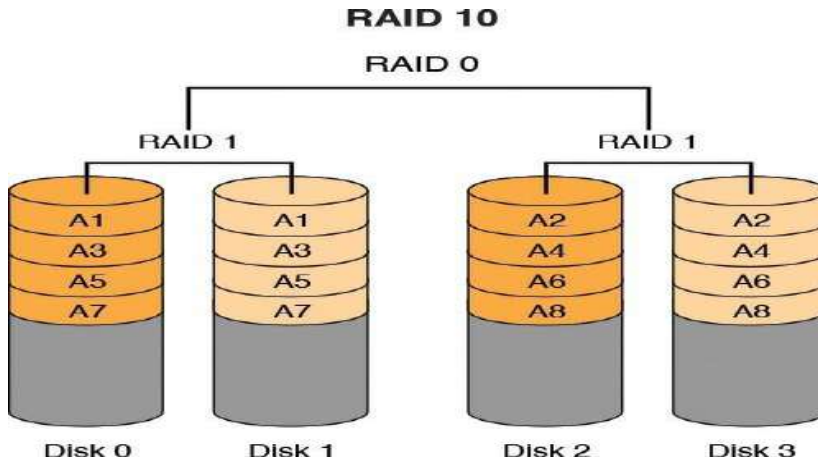
RAID 5، نیاز به حداقل سه درایو دارد، همچنین نیاز دارد که داده‌ها در تمام درایوها مانند نوار نوشته شوند و سپس اطلاعات یکسان در تمام درایوها نیز نوشته شود. اطلاعات یکسان به همان شیوه RAID 3 استفاده می‌شود، اما بر روی یک درایو منفرد ذخیره نمی‌شود، بنابراین هیچ نقطه‌ای از خرابی برای داده‌های یکسان وجود ندارد. با وجود سخت افزار RAID سطح ۵، درایوهای جایگزین (Spare Drives) که جایگزین درایوهای خراب شده می‌شوند معمولاً قابل تعویض هستند، به این معنی که در هنگام کار می‌توان آنها را روی سرور جایگزین کرد. شکل ۷-۵ تصویر RAID 5 را نشان می‌دهد.



شکل ۷-۵: RAID 5

RAID 7 که یک استاندارد نیست بلکه یک پیاده سازی اختصاصی است، همان اصول RAID 5 را در خود جای داده است اما در صورت عدم موفقیت هر دیسک یا هر راهی برای دیسک، آرایه را قادر به ادامه کار می کند. دیسک های چندگانه در آرایه به صورت یک دیسک مجازی عمل می کند.

RAID 10 ترکیبی از RAID 1 و RAID 0 است که حداقل به دو دیسک نیاز دارد و با انعکاس (Mirroring) دو درایو بوجود می آید سپس یک مجموعه نوار روی هر جفت منعکس می شود. با این حال، بسیاری از پیاده سازی RAID 10 دارای چهار یا درایوهای بیشتر هستند. استقرار RAID 10 حاوی یک نوار دیسک است که روی یک نوار دیسک جداگانه نشان داده شده است. شکل 7-۶ RAID 10 را نشان می دهد.



شکل ۷-۶: RAID 10

اگر چه RAID را می‌توان با نرم افزار یا سخت افزار پیاده سازی کرد، انواع خاصی از RAID با سخت افزار سریعتر اجرا می‌شوند. هنگام استفاده از RAID نرم افزار، که عملکردی از سیستم عامل می‌باشد. هر دو RAID 3 و RAID 5 نمونه‌ای از انواع RAID می‌باشد که سریعتر با سخت افزار اجرا می‌شوند. با این حال، (Mirroring, Striping) نوار کردن و یا همانندسازی (RAID 0 and 1) در نرم افزار به خوبی عمل می‌کند، زیرا آنها از درایوهای پارتیتی یا یکسان سخت افزاری استفاده نمی‌کنند. جدول ۷-۱ انواع RAID را خلاصه می‌کند.

RAID Level	Min. Number of Drives	Description	Strengths	Weaknesses
RAID 0	2	Data striping without redundancy	Highest performance	No data protection; one drive fails, all data is lost
RAID 1	2	Disk mirroring	Very high performance; very high data protection; very minimal penalty on write performance	High redundancy cost overhead; because all data is duplicated, twice the storage capacity is required
RAID 3	3	Byte-level data striping with dedicated parity drive	Excellent performance for large, sequential data requests	Not well-suited for transaction-oriented network applications; single parity drive does not support multiple, simultaneous read and write requests
RAID 5	3	Block-level data striping with distributed parity	Best cost/performance for transaction-oriented networks; very high performance, very high data protection; supports multiple simultaneous reads and writes; can also be optimized for large, sequential requests	Write performance is slower than RAID 0 or RAID 1
RAID 10	4	Disk mirroring with striping	Same fault tolerance as RAID 1; same overhead as with mirroring; provides high I/O rates; can sustain multiple simultaneous drive failures	Very expensive; all drives must move in parallel to properly track, which reduces sustained performance; very limited scalability at a very high cost

جدول ۷-۱: RAID

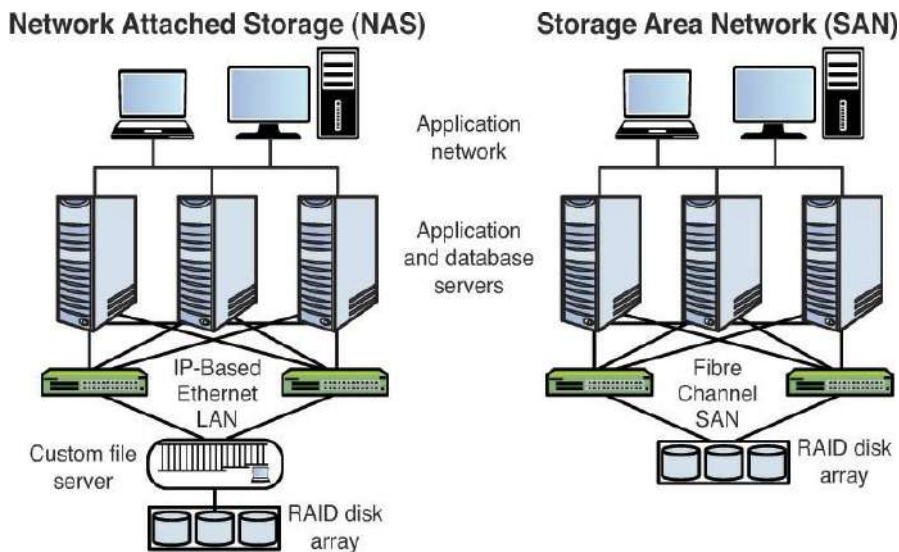
SAN

شبکه‌های ذخیره سازی منطقه‌ای (SAN) Storage-area networks شامل دستگاه‌های ذخیره سازی با ظرفیت بالا هستند که توسط یک شبکه خصوصی با سرعت بالا (جدا از شبکه LAN) با استفاده از سوئیچ‌های ذخیره سازی خاص متصل می‌شوند. این معماری اطلاعات ذخیره سازی، جمع آوری داده ها، مدیریت داده‌ها و استفاده از داده‌ها را پاسخ می‌دهد.

NAS

ذخیره سازی ضمایم شبکه (NAS) Network-attached storage همانند SAN عمل می‌کند، اما مشتریان یا (Clients) به شیوه‌ای دیگر به ذخیره سازی دسترسی پیدا می‌کنند. در یک NAS،

تقریباً هر دستگاهی که می‌تواند به LAN متصل شود (یا از طریق یک شبکه WAN به شبکه متصل شود) می‌تواند از پروتکل‌هایی مانند NFS، CIFS، HTTP برای اتصال به NAS استفاده کند و فایل‌ها را به اشتراک بگذارد. در SAN فقط دستگاه‌ها می‌توانند از طریق کانال فیبرنوری، ATA، iSCSI از اترنت استفاده کنند، یا از طریق شبکه HyperSCSI به داده‌ها دسترسی پیدا کنند، بنابراین به طور معمول هر سرور با این قابلیت انجام می‌شود. شکل ۷-۷ مقایسه دو سیستم را نشان می‌دهد.



شکل ۷-۷: NAS و SAN

HSM

سیستم مدیریت ذخیره سازی سلسله مراتبی Hierarchical Storage Management یک نوع سیستم مدیریت پشتیبان است که یک پشتیبان آنلاین مستمر را با استفاده از دستگاه‌های jukeboxهای نوری (Optical) یا نواری (Tape) فراهم می‌کند. این دستگاه با حرکت خودکار داده‌ها بین رسانه‌های ذخیره سازی با هزینه بالا و هزینه پایین به عنوان عمر داده‌ها عمل می‌کند. زمانیکه در دسترس بودن مداوم (پردازش ۲۴ ساعته روزانه) مورد نیاز می‌باشد، HSM یک جایگزین مناسب برای پشتیبان گیری نوار (Tape) است و همچنین از رسانه مناسب برای این سناریو استفاده می‌کند. به عنوان مثال، دیسک‌های نوری دیجیتال (DVD) گاهی برای پشتیبان

گیری استفاده می‌شوند که برای داده‌های قابل تغییر نیاز به ذخیره سازی کوتاه مدت دارند و دسترسی سریعتر فایل نسبت به نوار را دارند.

تاریخچه رسانه Media History

logهای مربوط به کتابخانه رسانه را بطور دقیق حفظ کرده تا تاریخچه رسانه‌ها ردیابی شود. از این جهت مهم است که کلیه انواع رسانه حداکثر تعداد دفعات استفاده از آن را دارند. یک log باید توسط یک کتابخانه رسانه نگه داشته شود. این رسانه باید تمام رسانه‌ها (پشتیبان گیری و انواع دیگر مانند دیسک‌های نصب سیستم عامل) را ردیابی کند. با توجه به رسانه پشتیبان، از دستورالعمل‌های زیر استفاده می‌شود:

- تمام موارد دسترسی به رسانه ردیابی شود.
- تعداد و محل پشتیبان گیری‌ها ردیابی شود.
- برای جلوگیری از دست رفتن داده‌ها از طریق تخریب رسانه، سن رسانه‌ها ردیابی شود.
- رسانه‌ها به طور منظم در لیست موجودی قرار گیرند.

برچسب زدن رسانه‌ها و ذخیره سازی Media Labeling and Storage

به طور ساده انواع رسانه‌های ذخیره سازی (نوار، نوری و غیره) را برچسب زده و با خیال آسوده ذخیره می‌شود. برخی از دستورالعمل‌ها در زمینه کنترل رسانه‌ها شامل:

- با دقت و به موقع تمام رسانه‌های ذخیره داده علامت گذاری شود.
- از ذخیره سازی مناسب محیط رسانه اطمینان حاصل شود.
- برخورداری از درست بودن و امنیت رسانه، تضمین شود.
- برای ارائه یک کنترل موجودی فیزیکی، داده در رسانه وارد شود.

محیطی که رسانه در آن ذخیره خواهد شد نیز دارای اهمیت است. به عنوان مثال، آسیب دیدن رسانه مغناطیسی، بالای ۱۰۰ درجه شروع می‌شود. کتاب جنگل سبز Forest Green Book یک کتاب از سری کتاب‌های رنگین کمان است که قابلیت استفاده امن از حافظه سیستم اطلاعات خودکار و حساس طبقه بندی شده و رسانه‌های ذخیره سازی ثانویه مانند دزدگیرها، نوارهای مغناطیسی، هارد دیسک‌ها و کارت‌ها را تعریف می‌کند.

پاکسازی و دفع رسانه Sanitizing and Disposing of Media

در حین دفع رسانه، باید تضمین شود که هیچ داده‌ای روی رسانه‌ها باقی نمی‌ماند. مطمئن‌ترین و امن‌ترین وسیله برای حذف داده‌ها از رسانه‌های ذخیره سازی مغناطیسی، مانند کاست نوار مغناطیسی، جدا سازی یا تفکیک می‌باشد که رسانه‌ها را در معرض یک میدان مغناطیسی قدرتمند و متناوب قرار می‌دهند، و داده‌های قبلی را که قبلاً نوشته شده است حذف می‌کند و رسانه‌ها را در حالت تصادفی مغناطیسی (خالی) قرار می‌دهند. برخی دیگر از اصطلاحات و مفاهیم دفع انباشت که باید با آنها آشنا باشید.

- **پاکسازی داده‌ها Data purging**: با استفاده از روشی مانند Degaussing، داده‌های قدیمی حتی با در اختیار واحد جرم شناسی رایانه‌ای قرار گرفتن نیز در دسترس نخواهد بود. پاکسازی باعث می‌شود در مقابل حملات آزمایشگاهی (جرم شناسی رایانه‌ای) اطلاعات غیر قابل برگشت نباشد.
- **تسویه داده Data Clearing**: اطلاعات غیر قابل بازیابی را توسط یک صفحه کلید ارائه می‌دهد. این حمله با اجرای برنامه‌های نرم افزاری، فشار کلیدها یا سایر منابع سیستم که از یک صفحه کلید اجرا می‌شوند، اطلاعات را از رسانه ذخیره سازی داده استخراج می‌کند.
- **باقیمانده Remanence**: هر گونه داده‌ای که پس از پاک کردن رسانه‌ها باقی مانده است.

مدیریت شبکه و منابع Network and Resource Management

اگرچه عملیات امنیتی بر تأمین محرمانه بودن و یکپارچگی داده‌ها تمرکز دارد اما در دسترس بودن داده‌ها نیز یکی از اهداف آن می‌باشد، و به معنای طراحی و نگهداری فرایندها و سیستمهایی است که با عدم وجود سخت افزار یا نرم افزار در محیط، دسترسی به منابع را حفظ می‌کنند. اصول و مفاهیم زیر برای کمک به حفظ دسترسی به منابع موجود می‌باشند:

- ✓ **افزونگی سخت افزاری Redundant hardware**: خرابی مؤلفه‌های فیزیکی مانند هارد دیسک‌ها و کارت شبکه می‌تواند دسترسی به منابع را مختل کند. ارائه موارد اضافی از این مؤلفه‌ها می‌تواند به اطمینان از بازگشت سریع تر دسترسی‌ها کمک کند. در بعضی حالات، تغییر کردن یک مؤلفه ممکن است نیاز به مداخله دستی داشته باشد، اما در بسیاری حالات این آیتم‌ها قابل جابجایی هستند (آنها را می‌توان با دستگاه و کار با

دستگاه تغییر داد)، در این حالت ممکن است کاهش لحظه ای عملکرد به جای یک اختلال کامل دسترسی رخ دهد.

✓ فن آوری های تحمل خطا Fault-tolerant technologies: تحقق ایده افزونگی به سطح بعدی، فناوری هایی هستند که مبتنی بر چندین سیستم محاسباتی هستند که با هم کار می کنند و حتی در صورت خرابی یکی از سیستم ها، دسترسی بی وقفه را فراهم می کنند. خوشه بندی سرورها Clustering of server و محاسبات شبکه هر دو نمونه ای عالی از این رویکرد هستند.

✓ MTBF و MTTR: اگرچه SLAها برای خدماتی که ارائه می شوند مناسب هستند، با توجه به مولفه های فیزیکی خریداری شده، می توان از رویکرد کمی متفاوت برای معرفی پیش بینی استفاده کرد. فروشندگان به طور معمول مقادیری را برای میانگین زمان بین محصول (MTBF) منتشر می کنند، که توصیف می کند که اغلب یک مولفه به طور متوسط چگونه از کار می افتد. یک متریک یا معیار با ارزش دیگر که به طور معمول ارائه می شود، میانگین زمان برای تعمیر (MTTR) است که میانگین مدت زمان لازم برای دریافت دستگاه را به صورت ثابت و برگشت به صورت آنلاین توصیف می کند.

✓ تنها نقطه شکست: Single point of failure (SPOF) اگرچه یک استراتژی نیست، اما لازم به ذکر است که هدف نهایی هر یک از این رویکردها جلوگیری از شکست SPOF در یک سیستم است. برای شناسایی هر عنصر واحد که می تواند دسترسی به منابع را در صورت بروز خرابی دچار وقفه کند، باید کلیه مؤلفه ها و گروه های قطعات و دستگاه ها مورد بررسی قرار گیرد. سپس هر SPOF باید به نوعی کاهش یابد.

مدیریت حادثه Incident Management

واکنش به حادثه برای هر سازمان به خاطر اطمینان از شناسایی، کنترل و بررسی هرگونه حادثه امنیتی بسیار حیاتی است. واکنش به حادثه آغاز هرگونه تحقیقات است. پس از کشف یک حادثه، پرسنل واکنش به حادثه وظایف خاصی را انجام می دهند. در امتداد کل واکنش به حادثه، تیم واکنش به حادثه باید اطمینان حاصل کنند که از اقدامات صحیح پیروی می کنند تا از حفظ شواهد مطمئن شوند.

به عنوان بخشی از واکنش به حادثه، متخصصان امنیت باید تفاوت بین رخدادها (Event) و حوادث (Incident) را درک کنند. تیم واکنش به حادثه باید اقدامات مناسب برای واکنش به

حادثه انجام دهند تا از رسیدگی به این حادثه اطمینان حاصل شود، اما رویه‌ها نباید مانع از تحقیقات جرم‌شناسی رایانه‌ای باشد که ممکن است برای اطمینان از اینکه طرفین در قبال هرگونه اقدامات غیرقانونی مسئولیت داشته باشند، مانع شود. متخصصان امنیت باید قوانین درگیری و مجوز و دامنه تحقیقات مربوط به حادثه را درک کنند.

رخداد در مقابل حادثه Event Versus Incident

در رابطه با واکنش به حادثه، تفاوت اساسی بین رخدادها و حوادث وجود دارد. یک رخداد تغییر حالتی است که رخ می‌دهد. در حالی که حوادث شامل رخداد‌های منفی و مثبت است، واکنش حوادث بیشتر به رخداد‌های منفی متمرکز می‌شود - رخداد‌هایی که به نظر منفی می‌باشند بر سازمان تأثیر می‌گذارند. یک حادثه مجموعه‌ای از رخداد‌هایی است که بر عملکرد و امنیت یک سازمان تأثیر منفی می‌گذارد.

رخدادها فقط در صورتی قابل شناسایی هستند که سازمان مکانیزم‌های مناسب برای ممیزی و امنیتی را برای نظارت بر فعالیت ایجاد کرده باشد. یک رخداد منفی منفرد ممکن است رخ دهد. به عنوان مثال، ورود به ممیزی ممکن است نشان دهد که یک تلاش نامعتبر برای ورود به سیستم رخ داده است. این تلاش ورود به سیستم به خودی خود دغدغه امنیتی نیست. اما اگر بسیاری از تلاش‌های نامعتبر ورود به مدت چند ساعت انجام شوند، سازمان ممکن است مورد حمله قرار گیرد. ورود نامعتبر اولیه یک رخداد در نظر گرفته می‌شود، اما مجموعه‌ای از تلاش‌های ورود نامعتبر طی چند ساعت، یک حادثه است، به خصوص اگر مشخص شود که تلاش‌های ورود نامعتبر همه از یک آدرس IP سرچشمه می‌گیرد.

تیم واکنش به حادثه و تحقیقات حادثه Incident Response Team and Incident Investigations

هنگام تشکیل تیم واکنش به حادثه، سازمان‌ها باید دانش فنی هر فرد را در نظر بگیرند. اعضای تیم باید سیاست‌های امنیتی سازمان را درک کنند و مهارت‌های ارتباطی خوبی داشته باشند. اعضا همچنین باید در زمینه واکنش و تحقیقات در مورد حادثه آموزش دیده باشند. وقتی حادثه‌ای رخ داده است، هدف اصلی تیم مهار حمله و ترمیم هرگونه خسارت ناشی از این حادثه است. ایزوله کردن (عایق سازی) امنیتی صحنه حادثه باید بلافاصله با کشف رخداد آغاز شود. شواهد باید حفظ شود و به مقامات ذیربط اطلاع داده شود.

تیم واکنش به حادثه باید به نقشه (Plan) واکنش به حادثه دسترسی داشته باشند. این نقشه باید شامل لیست مسئولان برای تماس، نقش ها و مسئولیت های تیم، لیست تماس داخلی، تضمین و حفظ روال شواهد و لیستی از کارشناسان تحقیقات باشد که می توانند برای کمک، با آنها تماس گرفته شود. باید یک کتابچه راهنمای مرحله به مرحله ایجاد شود که تیم واکنش به حادثه از آن پیروی کنند تا از عدم استفاده از این مراحل اطمینان حاصل شود. پس از انجام فرآیند واکنش به حادثه، کلیه اقدامات واکنش به حادثه باید مستندسازی شود. اگر تیم واکنش به حادثه تشخیص دهند که جرم مرتکب شده است، باید با مدیریت ارشد و مقامات مناسب بلافاصله تماس گرفته شود.

قواعد اشتغال، مجوز و حوزه Rules of Engagement, Authorization, and Scope

یک سازمان باید تیم های مربوط به مشارکت، مجوز و محدوده تیم واکنش به حادثه را مستند سازی کند. قوانین مربوط به تعامل تعریف می کنند که در صورت وقوع یک حادثه کدام یک از اقدامات قابل قبول و کدام یک غیرقابل قبول است. مجوز و حوزه اختیار تیم واکنش به حادثه برای انجام تحقیقات با توجه به محدوده مجاز تحقیقاتی که باید انجام دهند، ارائه می شود. قوانین درگیر این موضوع به عنوان راهنما برای تیم واکنش به حادثه عمل می کنند تا از عدم عبور از مسیر به دام افتادن، مطمئن شوند. فریب خوردن (Enticement) در شرایطی رخ می دهد که فرصت انجام اقدامات غیرقانونی فراهم شود (فریبنده) و مهاجم تصمیم خود را برای انجام عمل می گیرد، به دام افتادن (Entrapment) به معنای تشویق کسی به ارتکاب جرمی است که ممکن است فرد قصد آن را نداشته باشد. ابتکار عمل Enticement قانونی می باشد اما استدلال های اخلاقی را مطرح می کند و ممکن است در دادگاه قابل قبول نباشد و در مقابل، به دام افتادن که غیرقانونی می باشد.

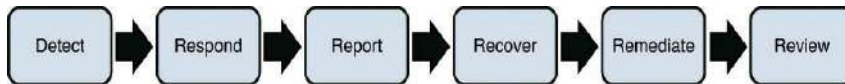
روشهای واکنش حادثه Incident Response Procedures

هنگام انجام واکنش به حادثه، مهم است که تیم پاسخگویی به حادثه روشهای واکنش حادثه را دنبال کنند. بسته به جایی که مشاهده می کنید، ممکن است مراحل یا فازهای مختلفی را در نظر گرفته شود که بخشی از روند واکنش حادثه است.

برای امتحان CISSP، باید مراحل زیر را به خاطر بسپارید:

- حادثه را تشخیص دهید.

- واکنش به حادثه.
 - گزارش حادثه به پرسنل مناسب.
 - بازیابی حادثه.
 - کلیه مؤلفه‌های تحت تأثیر این حادثه را از بین ببرید تا مطمئن شوید که تمام آثار حادثه برداشته شده است.
 - حادثه را بررسی کرده و تمام یافته‌ها را مستندسازی کنید.
- بررسی واقعی این حادثه در طی مراحل پاسخ، گزارش و بازیابی انجام می‌شود. پس از انجام مراحل تحقیقات جرم شناسی رایانه‌ای و دیجیتالی مناسب، می‌توان از حفظ شواهد اطمینان حاصل کرد.
- روند واکنش حادثه در شکل ۷-۸ نشان داده شده است.



شکل ۷-۸: روند واکنش حوادث

مدیریت واکنش حادثه Incident Response Management

رخدادهای امنیتی ناگزیر اتفاق می‌افتد، و واکنش به این رخدادها در مورد چگونگی آسیب دیدن این رخداد در سازمان بیان می‌شود. سیاست‌های واکنش به حادثه باید بطور رسمی طراحی شده، ارتباط برقرار کرده و دنبال شوند و باید بطور اختصاصی حملات سایبری را علیه سیستم‌های IT سازمانی مورد بررسی قرار دهند.

۱- تشخیص Detect

اولین قدم شناسایی حادثه است. قبل از هرگونه تحقیقات در مورد واکنش به حادثه، متخصصان امنیت ابتدا باید معیارهای مناسب برای دارایی‌های درگیر را انجام دهند، که در ابتدا تشخیص حادثه و تعیین میزان وقوع این حادثه است. در بعضی موارد، در امتداد فاز تریاژ(ارجحیت)، متخصصان امنیت ممکن است تشخیص دهند که یک مثبت کاذب رخ داده است، به این معنی که یک حمله واقعاً رخ نداده است، حتی اگر هشدار نشان داد که این کار انجام شده است. اگر یک حمله تأیید شود، واکنش به حادثه در اقدامات تحقیقاتی پیش می‌رود.

کلیه کنترل های کارآگاهی، مانند ممیزی، در فصل ۱، "امنیت و مدیریت ریسک" مورد بحث قرار گرفته است تا این توانایی را فراهم کند. بدترین نوع حادثه اتفاقی است که بی توجه مانده است.

۲- واکنش Respond

واکنش به حادثه باید از نظر نوع حادثه مناسب باشد. حملات انکار سرویس Denial-of-Service (DoS) علیه وب سرور نیاز به پاسخ سریعتر و متفاوت تری مثلا نسبت به ماوس مفقود شده در اتاق سرور دارد. پاسخ های استاندارد و زمان واکنش در زمان جلوتری تعیین می شود. واکنش شامل مهار این حادثه و قرنطینه دارایی های درگیر برای کاهش تأثیر احتمالی برای جلوگیری از تأثیر بر سایر دارایی ها است. با توجه به نوع حمله و دارایی که تحت تأثیر قرار گرفته و میزان اعتبار داده یا تأثیر ریسک، می توان از روش های مختلفی استفاده کرد. پس از مهار یا ایزوله شدن یک حمله، تحلیلگران باید برای بررسی و تحلیل علت این حادثه تلاش کنند، که شامل تعیین محل وقوع این حادثه است. متخصصان امنیت باید از تجربه و آموزش رسمی استفاده کرده تا نتیجه گیری مناسب را در مورد این حادثه انجام دهند. پس از مشخص شدن علت اصلی، متخصصان امنیت باید سیاست های رسیدگی به حادثه را که در سازمان وجود دارد، دنبال کنند.

۳- کاهش Mitigate

اگرچه کاهش یک بخش استاندارد برای واکنش به حادثه است، ولی به عنوان یک مرحله جداگانه ذکر نشده است. با این حال، متخصصان امنیت باید اهمیت کاهش را به عنوان بخشی از هرگونه واکنش به حادثه درک کنند. کاهش در واقع بخشی از واکنش به یک حادثه است و شامل محدود کردن حوزه که ممکن است حمله به دارایی های سازمان باشد. اگر خسارت وارد شده باشد یا این حادثه ممکن است به سایر دارایی ها گسترش پیدا کرده و تحت تأثیر قرار دهد، تکنیک های کاهش صحیح اطمینان می دهد که این حادثه در محدوده خاصی از دارایی ها قرار دارد. با توجه به نوع حمله ای که رخ داده است گزینه های کاهش متفاوت است. متخصصان امنیت باید پیشاپیش روش هایی را تدوین کنند که در مورد چگونگی کاهش صحیح هرگونه حمله ای که علیه دارایی های سازمانی صورت می گیرد، بطور دقیق توضیح دهند. آماده سازی این روش های کاهش از قبل اطمینان می دهند که کامل هستند و به پرسنل این امکان را می دهند که رویه ها را تست کنند.

۴- گزارش Report

تمام حوادث باید در یک بازه زمانی گزارش شود که منعکس کننده جدی بودن حادثه می باشد. در بسیاری از موارد، ایجاد لیستی از انواع حادثه ها و شخصی که در زمان وقوع آن حادثه تماس می گیرد مفید می باشد. توجه به جزئیات در این مرحله در زمانیکه اطلاعات حساس به زمان هنوز در دسترس است، بسیار مهم است.

۵- بازیابی Recover

بازیابی شامل واکنشی است که برای ایجاد مجدد شبکه یا سیستمی که تحت تأثیر قرار گرفته، طراحی شده است، و شامل تعمیر دارایی های تحت تأثیر و جلوگیری از بروز حوادث مشابه در آینده است. دقیقاً معنی بازیابی بستگی به شرایط و اقدامات بازیابی موجود دارد. به عنوان مثال، اگر اقدامات تحمل خطا انجام شده باشد، بازیابی شامل این مورد نیز می شود که به سادگی اجازه دهند سرورهای موجود در یک خوشه (Cluster) به خوشه دیگری نپردازند. در موارد دیگر، بازیابی به معنای بازیابی سرور از آخرین پشتیبان (Backup) اخیر می باشد. هدف اصلی این مرحله، بازگرداندن همه منابع است. تأخیر در بازگرداندن هر دارایی تا زمانی که، حداقل در برابر حادثه ای که رخ داده است محافظت شود. قبل از بازگرداندن آنها، دارایی ها برای آسیب پذیری و ضعف کاملاً تست شوند.

۶- اصلاح کردن Remediate

این مرحله شامل از بین بردن هرگونه حمله خطرناک Dos یا آسیب زدن به شبکه که هنوز امکان دارد وجود داشته باشد، است. به عنوان مثال، در مورد شیوع ویروس، می تواند به معنای اسکن کلیه سیستم ها برای از بین بردن دستگاه های دارای اثر اضافی باشد. این اقدامات به گونه ای طراحی شده اند که در صورت زمان بیشتر داشتن، جزئیات بیشتری کاهش می یابد.

۷- بررسی و دروس یادگرفته شده Lessons Learned and Review

سرانجام، هر حادثه را بررسی کرده تا آنچه را می توان از آن آموخت، کشف کرد. ممکن است تغییرات رویه ها فراخوانده شود. دروس آموخته شده را با کلیه پرسنلی که ممکن است دوباره با این نوع حادثه روبرو شوند به اشتراک بگذارید. مستندسازی و تحلیل کامل هدف این مرحله است.

اقدامات پیشگیرانه Preventive Measures

طیف گسترده‌ای از تهدیدهای امنیتی که با آن روبرو هستند، کسانی می‌باشند که موظف به حمایت از دارایی‌های یک سازمان هستند. خوشبختانه، ابزارهای متنوعی برای دستیابی به این کار در دسترس است. در این بخش برخی از تهدیدات و رویکردهای کاهش متداول ارائه شده است.

سطح برش Clipping Levels

سطح برش، یک خط مبنا برای خطاهای عادی کاربر تعیین می‌کند، و تخلفاتی که بیش از آن آستانه باشد، به خاطر تجزیه و تحلیل دلیل وقوع تخلفات ثبت خواهد شد. در هنگام استفاده از سطح برش، تعداد مشخصی از وقایع یک فعالیت ممکن است هیچ اطلاعاتی را زمانیکه ضبط فعالیت‌ها با عبور از سطح مشخصی شروع می‌شود، ایجاد نکند. سطح برش در موارد زیر بکار برده می‌شود:

- مقدار داده‌هایی که باید در logهای ممیزی ارزیابی شوند، کاهش یابد.
- خط مبنا برای خطاهای کاربر ارائه شود که تخلفات بالاتر از آن ثبت شود.

انحراف از استاندارد Deviations from Standards

یکی از روش‌هایی که می‌توان برای شناسایی مشکلات کارایی استفاده کرد، تهیه استانداردها یا خط مبنا برای عملکرد سیستمهای خاص می‌باشد. پس از ایجاد این معیارها، انحراف برای استانداردها قابل شناسایی است. این امر به ویژه در شناسایی انواع خاصی از حملات DoS هنگام وقوع مفید است. فراتر از منافع امنیتی، در شناسایی سیستمها قبل از وضعیت تاثیر بهره وری، ممکن است نیاز به بروزرسانی داشته باشند.

رخداد های غیر معمول یا غیر قابل توضیح Unusual or Unexplained Events

در بعضی موارد اتفاقاتی رخ می‌دهد که به نظر نمی‌رسد دلیل منطقی داشته باشند. در صورت بروز مشکلات هرگز نباید به عنوان پاسخ پذیرفته شود. اگرچه تمرکز معمولاً بر روی کارایی سیستم‌ها و استفاده مجدد از سیستم است، اما باید ریشه اصلی مشکلات شناسایی شود. از وسوسه اجرای سریع کار (اغلب با هزینه امنیتی) خودداری شود. هنگامی که زمان اجازه می‌دهد، با

استفاده از یک روش علمی شناختی، دقیقاً بهترین دلیل وقوع رخداد مشخص می‌شود، زیرا به ناچار در صورت عدم رسیدگی به علت اصلی، مشکل مجدداً بوجود می‌آید.

راه اندازی مجدد برنامه ریزی نشده **Unscheduled Reboots**

هنگامی که سیستم‌ها بی اختیار راه اندازی مجدد می‌شوند، به طور معمول نشانه‌ای از مشکلات سخت افزاری است. راه اندازی مجدد باید ثبت و آدرس دهی شود. دمای بالای بیش از حد، علت بسیاری از راه اندازی مجدد است. اغلب راه اندازی مجدد نیز می‌تواند نتیجه حمله DoS باشد. برای ثبت همه راه اندازی‌های مجدد سیستم، یک سیستم نظارت در محل داشته و در مورد مواردی که توسط انسان شروع نشده، تحقیق شود. حالت دیگر در نتیجه بروزرسانی خودکار اتفاق افتاده می‌افتد.

افشای غیر مجاز **Unauthorized Disclosure**

افشای غیرمجاز اطلاعات تهدید بزرگی برای سازمانها است، که شامل تخریب اطلاعات، قطع سرویس، سرقت اطلاعات، فساد اطلاعات و اصلاح نادرست اطلاعات است. برای نظارت بر هرگونه افشای احتمالی اطلاعات، راه حل‌های سازمانی باید بسط داده شوند.

بازیابی مورد اعتماد **Trusted Recovery**

هنگامی که یک برنامه یا سیستم عامل دچار یک خرابی (خرابی، یخ زدگی freeze و غیره) می‌شود، مهم است که سیستم، به گونه‌ای واکنش دهد که سیستم را در یک حالت امن رها کند یا اینکه یک بازیابی مطمئن ایجاد شود. بازیابی مطمئن باعث می‌شود که در هنگام خرابی سیستم یا خرابی سیستم دیگر، امنیت نقض نشود. در کتاب نارنجی Orange Book به یک سیستم نیاز دارد تا بتواند برای کلیه سیستم‌های دارای رتبه B3 یا A1، یک بازیابی مطمئن داشته باشد.

مسیرهای قابل اعتماد **Trusted Paths**

یک مسیر قابل اعتماد یک کانال ارتباطی بین کاربر یا برنامه‌ای است که از طریق آن با پایگاه رایانه قابل اعتماد (TCB) Trusted computer base کار می‌کند. TCB منابعی را برای محافظت از کانال و جلوگیری از به خطر انداختن آن فراهم می‌کند. از سوی دیگر، یک مسیر ارتباطی که از مکانیسم‌های امنیت عادی سیستم محافظت نمی‌شود، یک کانال مخفی Covert Channel

نامیده می شود. با این کار یک قدم بیشتر، اگر واسط ارائه شده به کاربر از این طریق امن شود، به آن یک پوسته قابل اعتماد Trusted shell گفته می شود. امنیت عملیات باید از اعتبارسنجی مسیرها اطمینان داشته باشد. این امر با استفاده از مجموعه log تجزیه و تحلیل log، اسکن آسیب پذیری، مدیریت پچ و بررسی یکپارچگی سیستم رخ می دهد.

کنترل های ورودی / خروجی Input/Output Controls

محور اصلی کنترل ورودی / خروجی انجام کنترلها یا چک کردنها بر روی ورودی است که مجاز به ارسال روی سیستم می شود. انجام اعتبارسنجی ورودی بر روی کلیه اطلاعات پذیرفته شده در سیستم می تواند از مناسب بودن نوع و فرمت داده ها اطمینان داشته که سیستم را در حالت ناامن قرار ندهد.

همینطور، خروجی امن سیستم (چاپگرها، گزارش ها و غیره). تمام اطلاعات خروجی حساس قبل از انتشار باید رسید داشته باشند و کنترل های دسترسی مناسب را بدون در نظر گرفتن فرمتشان انجام دهند.

سخت شدن سیستم System Hardening

یکی دیگر از اهداف حال حاضر امنیت عملیات، اطمینان از سخت شدن کلیه سیستمها در حد امکان است که هنوز هم عملکردی را ارائه می دهد. سخت شدن می تواند هم به صورت فیزیکی و هم به صورت منطقی انجام شود. امنیت فیزیکی سیستمها بعداً در این فصل به تفصیل شرح داده می شود. از منظر منطقی:

- برنامه های غیر ضروری حذف شود.
- سرویس های غیر ضروری غیرفعال شود.
- پورتهای غیرقابل استفاده مسدود شود.
- اگر اتصال دستگاههای ذخیره سازی خارجی و رسانه بهیچ وجه مجاز نیست، شدیداً کنترل شود.

سیستم‌های مدیریت آسیب پذیری Vulnerability Management Systems

در تمام این کتاب بر اهمیت انجام تست آسیب پذیری و نفوذ تأکید شده است. یک سیستم مدیریت آسیب پذیری نرم افزاری است که فرآیند نظارت و تست مداوم شبکه برای آسیب پذیری‌ها را متمرکز کرده و تا حدی خودکار می‌کند. این سیستم‌ها می‌توانند شبکه را برای آسیب پذیری‌ها اسکن کنند، گزارش دهند و در بسیاری موارد بدون مداخله انسان مشکل را برطرف کند. اگرچه یک ابزار با ارزش در جعبه ابزار Toolbox هستند، این سیستم‌ها، علیرغم اینکه ممکن است پیچیده باشند، نمی‌توانند محل آسیب پذیری و آزمایش نفوذ را توسط متخصصان آموزش دیده، دریافت کنند.

IDS / IPS

تنظیم، پیکربندی و نظارت بر هرگونه سیستم شناسایی و جلوگیری از نفوذ IDS / IPS نیز از دیگر وظایف امنیت عملیات هستند. بسیاری از این سیستم‌ها باید بطور منظم با نشانه‌های حمله به روز شوند و آنها را قادر به تشخیص انواع حمله جدید کند. موتورهای آنالیز که از آنها استفاده می‌کنند نیز گاهی اوقات بروزرسانی‌هایی دارند که باید اعمال شوند.

علاوه بر این، فایل‌های log سیستم‌ها قرار است رخدادهای خاصی را ثبت کنند، و اقدامات خاصی را هنگام حادثه انجام دهند، تا آن فایل‌ها به طور مرتب بایگانی و تجزیه و تحلیل شوند. صرف هزینه‌های هنگفت برای نرم افزاری که اطلاعات را جمع آوری کرده و پس از آن عدم توجه به اطلاعات بی معنی می‌کند.

پاسخ نفوذ به همان اندازه مهم است که تشخیص نفوذ و پیشگیری از آن مهم باشد. پاسخ نفوذ درمورد واکنش مناسب به هر اقدام متجاوز می‌باشد. در هنگام تلاش برای نفوذ بیشتر سیستم‌ها از هشدار و سیگنال برای ارتباط با پرسنل یا سیستم‌های مناسب استفاده می‌کنند. یک سازمان باید به موقع به هشدارها و سیگنال‌ها واکنش دهد.

فایروال‌ها (دیوار آتش) Firewalls

فایروال‌ها را می‌توان در چندین سطح پیاده سازی کرد تا ارتباطات مبتنی بر عوامل مختلف امکان پذیر یا جلوگیری شود. اگر کارکنان دریابند که انواع خاصی از ترافیک ناخواسته در حال وقوع است، پیکربندی یک فایروال برای جلوگیری از آن نوع ترافیک، معمولاً بسیار ساده است. فایروال‌ها

می توانند از مرزهای بین شبکه، ترافیک در یک کار فرعی یا یک سیستم واحد محافظت کنند. مطمئن شوید که فایروال ها را به طور کامل با توجه توصیه فروشنده به روز کرده اید.

لیست سفید / لیست سیاه Whitelisting/Blacklisting

لیست سفید هنگامی رخ می دهد که لیستی از آدرس های ایمیل قابل قبول، آدرس های اینترنتی، وب سایت ها، برنامه یا برخی از شناسه های دیگر به عنوان فرستنده مجاز یا در حد مجاز تنظیم شود. لیست سیاه فرستنده های بد را شناسایی می کند. لیست خاکستری جایی در بین این دو فهرست قرار دارد که نمی توان آنها را به عنوان لیست سفید یا لیست سیاه معرفی کرد. در مورد لیست خاکستری، موجودیت جدید باید از یک سری تست ها عبور کند تا مشخص شود لیست سفید یا لیست سیاه خواهد بود یا خیر. لیست سفید، لیست سیاه و لیست خاکستری معمولاً از ابزار فیلتر کردن اسپم استفاده می کنند.

خدمات امنیت شخص ثالث Third-Party Security Services

ممکن است متخصصان امنیت برای یافتن تهدیدات در سازمان، به خدمات امنیت شخص ثالث اعتماد کنند. برخی از سرویس های امنیتی متداول شخص ثالث شامل شناسایی بدافزارها / ویروس ها و Honeypot/Honeynet ها هستند. تکیه کردن بر راه حل ایجاد شده توسط شخص ثالث بسیار ساده تر از تلاش برای توسعه راه حل داخلی سازمان می باشد. همیشه ویژگی های ارائه شده با یک راه حل را تحقیق کنید تا مشخص کنید آیا نیازهای سازمان را برآورده می کند یا خیر. محصولات مختلف موجود را با هم مقایسه کرده تا مطمئن شوید که سازمان بهترین راه حل را برای نیازهای خود خریداری کرده است.

Sandboxing

یک تکنیک مجازی سازی نرم افزاری است که به برنامه ها و پروسه ها اجازه می دهد تا در یک محیط مجازی تفکیک شده اجرا شوند. برنامه ها و فرآیندهای موجود در Sandboxing قادر به ایجاد تغییرات دائمی در سیستم و فایل ها نیست.

برخی از بدافزارها سعی در به تعویق انداختن یا توقف اجرای کد کرده اند و این امکان را برای Sandboxing فراهم می کنند. یک Sandboxing می تواند از قلاب و بررسی های محیطی برای

شناسایی بدافزار استفاده کند. این روشها از بروز بسیاری از بدافزارها جلوگیری نمی کنند، به همین دلیل خدمات امنیتی شخص ثالث دارای اهمیت هستند.

Honeypots / Honeynets

سیستمهایی هستند که با کمبود امنیت برای جلب مهاجمین پیکربندی شده اند تا ادمینها بتوانند در مورد تکنیکهای حمله اطلاعات کسب کنند. در برخی موارد، کل شبکهها به نام Honeynets ها برای این منظور به طور جذاب پیکربندی می شوند. این نوع رویکردها فقط باید توسط شرکت هایی با مهارت استقرار و نظارت صحیح بر روی آنها انجام شود. برخی از خدمات امنیتی شخص ثالث می توانند این عملکرد را برای سازمانها فراهم کنند.

ضد بدافزار / آنتی ویروس Anti-malware/Antivirus

در نهایت، تمام بروزرسانیهای آنتی ویروس و نرم افزار ضد بدافزار مسئول امنیت عملیات است. استقرار یک راه حل جامع ضد بدافزار / آنتی ویروس برای کل شرکت مهم است.

مدیریت پچ Patch Management

اغلب به عنوان زیر مجموعه مدیریت پیکربندی مشاهده می شود. پچهای نرم افزار بروزرسانی هایی است که توسط فروشندگان منتشر می شود و یا مشکلات عملکردی را بابت نقاط ضعف سیستمهای عامل، برنامههای کاربردی و نسخههای سیستم عامل که در دستگاههای شبکه اجرا می شوند، بوسیله کارکردهای امنیتی برطرف می کنند.

برای اطمینان از جدیدترین دستگاههای نصب شده در کلیه دستگاهها، یک سیستم رسمی را مستقر کنید تا مطمئن شوید که همه سیستمها پس از تست کامل در یک محیط غیر عملیاتی آخرین نسخه را دریافت می کند. غیرممکن است که فروشنده بتواند هرگونه تأثیر احتمالی را که بر سیستمهای مهم کسب و کار در شبکه داشته باشد، پیش بینی کند. شرکت مسئولیت اطمینان از اینکه پچها تحت تأثیر عملیات منفی قرار ندهد، می باشد.

چرخه عمر مدیریت پچ شامل مراحل زیر است:

- ✓ اولویت بندی و برنامه ریزی پچ: تعیین اولویت پچها و برنامه ریزی پچهای مستقر.
- ✓ تست پچ: پچهای قبل از استقرار را امتحان کرده تا از عملکرد صحیح آنها مطمئن شده که باعث ایجاد مشکلات سیستم یا امنیت نمی شود.

- ✓ نصب پیچ: پیچ ها در محیط زنده نصب شود.
- ✓ ارزیابی و ممیزی پیچ: پس از استقرار پیچ ها، اطمینان داشته که پیچ ها به درستی کار می کنند.

بسیاری از سازمان ها برای اطمینان از استقرار به موقع پیچ ها، یک سیستم مدیریت متداول پیچ را به کار می گیرند. با استفاده از این سیستم، ادمین ها می توانند قبل از اعزام آنها به سیستمهایی که روی آنها تأثیر می گذارد، تمام پیچ ها را آزمایش و بررسی کنند. ادمین ها می توانند بروزرسانی ها را در ساعات غیر شلوغ زمانبندی کنند.

تغییر فرآیندهای مدیریت Change Management Processes

همه شبکه ها با گذشت زمان تکامل می یابند، رشد و تغییر می کنند. شرکت ها و فرایندهای آنها نیز دچار تحول و تغییر می شوند که این یک مقوله مناسب می باشد. ولی باید تغییرات به روشی ساخت یافته مدیریت شود تا یک حس مشترک در مورد تغییرات حفظ شود. با دنبال کردن مراحل توصیه شده در یک فرایند رسمی، می توان از برعکس شدن کار، جلوگیری کرد. در زیر دستورالعملهایی وجود دارد که بخشی از هر سیاست کنترل تغییر را شامل می شود:

- ✓ کلیه تغییرات باید بصورت رسمی درخواست شود. log های مربوط به تغییر باید حفظ شوند.

- ✓ هر درخواست باید برای اطمینان از پشتیبانی همه اهداف و سیاست ها مورد تجزیه و تحلیل قرار گیرد که شامل پایه گذاری و تحلیل تأثیرات امنیتی است.

- ✓ قبل از تصویب رسمی، کلیه هزینه ها و اثرات روش های اجرایی بررسی شود. با استفاده از داده های جمع آوری شده، تغییرات باید تأیید یا رد شوند.

- ✓ پس از تأیید آنها، مراحل تغییر باید توسعه یابد.

- ✓ در حین اجرا، تست های افزایشی باید انجام شود و در صورت لزوم باید به یک استراتژی از پیش تعیین شده و پیش بینی شده اعتماد کرد. برای ردیابی و کنترل تغییرات در مجموعه ای از اشخاص باید از نسخه سازی (Versioning) استفاده کرد.

- ✓ مستندات کامل باید به صورت یک گزارش رسمی تهیه و به مدیریت ارسال شود.

یکی از مهمترین مزایای پیروی از این روش، امکان استفاده از اسناد و مدارک در برنامه ریزی های آینده است. از درس های آموخته شده می توان استفاده کرد و حتی خود فرآیند نیز می تواند از طریق تجزیه و تحلیل بهبود یابد.

استراتژی‌های بازیابی Recovery Strategies

شناسایی کنترل‌های پیشگیرانه سومین مرحله از مراحل تداوم کسب و کار است که در NIST SP 800-34 R1 بیان شده است. اگر کنترل‌های پیشگیرانه در BIA شناسایی شوند، حوادث فاجعه یا حوادث ناگوار ممکن است کاهش یا از بین بروند. این اقدامات پیشگیرانه، تأثیرات بر روی سیستم را تشخیص داده و یا کاهش می‌دهد. در صورت امکان پذیر بودن و مقرون به صرفه بودن کنترل‌های پیشگیری، روش‌های پیشگیری از اقداماتی که ممکن است برای بازیابی سیستم پس از اختلال لازم باشد، ارجحتر می‌باشد.

بخش‌های بعدی در مورد کنترل‌های پیشگیرانه اولیه که سازمانها می‌توانند به عنوان بخشی از تداوم کسب و کار و بهبود فاجعه از جمله سیستم‌های کارآمد، تاسیسات و قدرت که مورد استفاده قرار گیرد و فن‌آوری‌های تحمل خطا، بیمه، فایل پشتیبانی داده، شناسایی و سرکوب آتش، بحث می‌کند.

سیستم‌های افزونه، تاسیسات و قدرت Redundant Systems, Facilities, and Power

در پیش بینی وقوع مصیبت‌ها و حوادث ناگوار، سازمان‌ها باید افزونگی سیستم‌های مهم، تاسیسات و قدرت را اعمال کرده و هر سیستم شناسایی شده را برای تعیین اینکه آیا اجرای سیستم‌های افزونه مقرون به صرفه هستند، ارزیابی کنند. غالباً اجرای سیستم‌های افزونه در یک مکان جایگزین تضمین می‌کند که خدمات بدون وقفه هستند. سیستم‌های افزونه شامل سرورهای افزونه، روترهای افزونه، سخت افزار داخلی افزونه و حتی ستون فقرات افزونه هستند. افزونگی هنگامی اتفاق می‌افتد که یک سازمان دارای یک مؤلفه ثانویه، سیستم یا دستگاهی باشد که هنگام شکستن واحد اصلی، مسئولیت ادامه کار را بر عهده می‌گیرد.

تاسیسات افزونه تضمین می‌کند که سازمان تاسیسات را در هر سطح مورد نظر خود حفظ می‌کند تا اطمینان دهد که خدمات سازمانی می‌توانند در صورت وقوع یک رخداد مخرب ادامه یابند.

قدرت افزونه با استفاده از منبع برق اضطراری (Uninterruptible power supplies (UPSs و ژنراتور برق انجام می‌شود.

افزونگی روی قطعات منفرد نیز می‌تواند تأمین شود. قطعات یدکی شامل یدکی سرد Cold spares، یدکی گرم Warm spares یا یدکی داغ Hot spares است. یدکی سرد مصرف نمی‌شود اما در صورت نیاز می‌توان آن را وارد سیستم کرد. یدکی گرم در سیستم می‌باشد و منبع تغذیه

ندارد مگر اینکه لازم باشد. یک یدکی داغ که در سیستم وجود دارد و دارای یک منبع تغذیه بوده و آماده بهره برداری در لحظه می باشد.

فن آوری های تحمل خطا Fault-Tolerance Technologies

تحمل خطا یک سیستم را قادر می سازد در صورت خرابی یک یا چند قطعه به کار خود ادامه دهد. تحمل خطا در یک سیستم می تواند شامل کارتهای آداپتور قابل تحمل در برابر خطا و درایوهای ذخیره تحمل پذیر خطا باشد. یکی از شناخته شده ترین سیستم های تحمل در برابر خطا، RAID است.

با پیاده سازی فن آوری های قابل تحمل در برابر خطا، سازمان می تواند مطمئن شود که در صورت عدم موفقیت یک قطعه تحمل خطا، عملکرد عادی رخ می دهد.

بیمه Insurance

اگرچه افزونگی و تحمل خطا در واقع می تواند به عنوان اقدامات پیشگیرانه در برابر شکست عمل کند، اما بیمه در واقع یک اقدام پیشگیرانه نیست. اگر سازمانی در صورت بروز حوادث مخرب، بیمه ای را برای تأمین امنیت خریداری کند، بیمه قدرت محافظت در برابر خود رخداد را ندارد. هدف این بیمه اطمینان از دسترسی سازمان به منابع مالی اضافی برای کمک به بهبود می باشد. به خاطر داشته باشید که تلاش های بهبود بابت یک رخداد مخرب اغلب می تواند هزینه های مالی زیادی را متحمل شود. حتی ممکن است برخی از بهترین تخمین ها زمانی که بهبود واقعی اتفاق می افتد به حد نصاب نرسد. با خرید بیمه، سازمان می تواند مطمئن شود که تراکنش های کلیدی مالی، از جمله حقوق و دستمزد، حساب های پرداخت شده و هرگونه هزینه بازایی تحت پوشش قرار می گیرد.

ارزش گذاری واقعی بیمه Insurance Actual Cost Valuation (ACV) دارایی را بر اساس ارزش موردی در تاریخ ضرر به علاوه ۱۰ درصد جبران می کند. با این حال، باید به خاطر داشت که بیمه درمورد هر نوع چاپی فقط اسناد درج شده، چاپ شده یا مکتوب نسخه های خطی یا سوابق را در بر می گیرد. این بیمه، پول و اوراق بهادار را پوشش نمی دهد. یک نوع خاص از بیمه به نام بیمه اختلال کسب و کار Business Interruption Insurance، محافظت پولی برای هزینه ها و درآمد از دست رفته را فراهم می کند.

سازمانها باید سالانه بیمه نامه ها را بررسی کرده و در صورت لزوم آنها را به روز کنند.

نسخه پشتیبان از داده‌ها Data Backup

تهیه نسخه پشتیبان از داده‌ها در مقابل از بین رفتن داده‌ها جلوگیری کرده اما از وقوع این رخداد جلوگیری نمی‌کند. همه سازمانها باید مطمئن شوند که از کلیه سیستمهایی که فایل‌های مهم را ذخیره می‌کنند، به موقع نسخه پشتیبان گرفته اند. همچنین باید کاربران تشویق شوند تا از فایل‌های شخصی مورد نیاز خود نسخه پشتیبان تهیه کنند. علاوه بر این، تست دوره‌ای فرآیند ترمیم باید انجام شود تا از بازگرداندن فایلها مطمئن شوند.

تشخیص و سرکوب آتش Fire Detection and Suppression

سازمانها باید سیستمهای تشخیص و سرکوب آتش را به عنوان بخشی از هر برنامه تداوم کسب و کار (Business continuity plan (BCP پیاده سازی کنند. شناسایی آتش و سرکوبها براساس روش تشخیص / سرکوب، استفاده متفاوت دارد و در بخش "امنیت محیطی" در فصل ۳ با جزئیات بیشتری مورد بحث قرار گرفت.

در دسترس بودن زیاد High Availability

در دسترس بودن زیاد در بازیابی اطلاعات مفهومی است که تضمین می‌کند داده‌ها همیشه با استفاده از افزونگی و تحمل خطا در دسترس هستند. بیشتر سازمانها راه حل‌های در دسترس بودن زیاد را به عنوان بخشی از هر برنامه بهبود فاجعه (Disaster recovery plan (DRP پیاده سازی می‌کنند.

اصطلاحات و تکنیک‌های در دسترس بودن زیاد که باید درک شود شامل موارد زیر است:

- آرایه‌های اضافی از دیسک‌های مستقل *Redundant Array of Disks*

Independent (RAID) یک فناوری: هارد دیسک است که در آن داده‌ها روی چند

دیسک نوشته شده است به گونه‌ای که دیسک نتواند خراب شود و داده‌ها به سرعت

از دیسک‌های بازسازی شده در آرایه بدون بازیابی از نوار یا سایر رسانه‌های

پشتیبان، نسخه پشتیبان تهیه می‌کند.

- شبکه ذخیره سازی *Storage-area network (SAN)*: دستگاه‌های ذخیره سازی با

ظرفیت بالا که با استفاده از سوئیچ‌های مخصوص ذخیره سازی توسط یک شبکه

خصوصی پر سرعت متصل می‌شوند.

- **ناکامی Failover**: ظرفیت سیستم در صورت بروز خرابی در سیستم اولیه، به سیستم پشتیبان تغییر می کند.
- **تخریب تدریجی Failsoft**: قابلیت یک سیستم برای خاتمه فرآیندهای غیر مهم در هنگام بروز خرابی.
- **خوشه بندی Clustering**: به یک محصول نرم افزاری اطلاق می شود که خدمات متعادل کننده بار را ارائه می دهد. با خوشه بندی، یک نمونه از سرور برنامه کاربردی به عنوان یک کنترل کننده اصلی عمل می کند و با استفاده از الگوریتم های راند رابین، راند رابین وزن مخصوص یا حداقل اتصالات، درخواست ها را در چندین مورد توزیع می کند.
- **تعادل بار Load balancing**: به یک محصول سخت افزاری اشاره دارد که خدمات متعادل کننده بار را ارائه می دهد. کنترلرهای تحویل برنامه کاربردی Application delivery controllers (ADCs) از همان الگوریتم ها پشتیبانی کرده و همچنین از خرد کردن تعداد فرآیندهای پیچیده، مانند CPU هر سرور و استفاده از حافظه، سریعترین زمان پاسخ و غیره استفاده می کنند تا تعادل بار را تنظیم کنند. راه حل های تعادل بار به نام مزارع Farm یا استخرها Pool گفته می شود.

کیفیت خدمات Quality of Service

کیفیت خدمات یا QoS یک فناوری است که منابع شبکه را برای اطمینان از سطح از پیش تعیین شده خدمات مدیریت می کند. QoS اولویت های ترافیکی را به انواع مختلف ترافیک یا پروتکل در یک شبکه اختصاص می دهد. QoS وقتی گلوگاه Bottleneck اتفاق می افتد مستقر می شود و تصمیم می گیرد که کدام ترافیک از بقیه مهمتر است. دقیقاً آنچه که باعث می شود که یک ترافیک مهمتر از ترافیک دیگر باشد مبتنی بر قوانینی است که ادمین تهیه می کند. اهمیت را می توان بر اساس آدرس IP، آدرس MAC و حتی نام سرویس ارائه داد.

با این حال، QoS فقط هنگامی کار می کند که یک گلوگاه در مکان مناسب رخ دهد و تنظیمات اظهارات پهنای باند ما باشند. به عنوان مثال، اگر تنظیمات QoS فراتر از پهنای باند ISP باشد، اگر روتر فرض کند پهنای باند کافی وجود دارد، ترافیک در اولویت قرار نخواهد گرفت. ولی اگر حداکثر ISP برآورده شود، ISP تصمیم می گیرد چه چیزی مهم است یا مهم نیست؟ نکته اصلی برای استقرار QoS، ترافند تنظیمات و مشاهده شبکه به مرور زمان است.

مقاومت سیستم System Resilience

انعطاف پذیری سیستم توانایی یک سیستم، دستگاه یا مرکز داده برای بازیابی سریع و ادامه کار پس از خرابی تجهیزات، قطع برق یا یک اختلال دیگر است. مقاومت سیستم شامل استفاده از مؤلفه‌ها یا تاسیسات اضافی است. هنگامی که یکی از مؤلفه‌ها خراب و یا مختل شود، مؤلفه افزونه یکپارچه وظیفه را بر عهده می‌گیرد و خدمات خود را به کاربران ادامه می‌دهد.

ایجاد استراتژی‌های بازیابی Create Recovery Strategies

سازمانها باید استراتژی‌های بازیابی را برای کلیه دارایی‌هایی که برای عملکرد موفق ضروری هستند ایجاد کنند.

استراتژی‌های بازیابی سطح بالاتر، ترتیب بازگرداندن فرایندها و عملکردها را مشخص می‌کند. استراتژی‌های بازیابی سطح سیستم نحوه بازیابی یک سیستم خاص را تعریف می‌کند. در نظر داشته باشید افرادی که سیستم را به بهترین وجه درک می‌کنند باید استراتژی‌های بازیابی سیستم را تعریف کنند. اگرچه کمیته BCP احتمالاً می‌تواند لیست‌های بهبود اولویت بندی شده و استراتژی‌های بازیابی سطح بالا را ایجاد کند، مدیران سیستم و دیگر پرسنل IT باید در توسعه استراتژی‌های بازیابی برای دارایی‌های فناوری اطلاعات نقش داشته باشند.

وظایف بهبود فاجعه شامل روشهای بازیابی، روشهای ایمنی پرسنل و روشهای ترمیم است. برنامه کلی بازیابی کسب و کار باید کمیته‌ای را برای تصمیم گیری در مورد بهترین مسیر عملیاتی تشکیل دهد. این کمیته طرح (Plan) بازیابی هدایت خود را از کمیته BCP و مدیریت ارشد دریافت می‌کند.

کلیه تصمیمات مربوط به بازیابی باید از قبل گرفته شده و در DRP گنجانیده شود. هر طرح و رویه‌ای که تدوین شده باشد باید به کارکردها یا مراحل مربوط باشد، نه افراد خاص. به عنوان بخشی از برنامه ریزی برای بهبود فاجعه، کمیته طرح بازیابی باید پیش از موعد با فروشندگان مهم تماس بگیرند تا مطمئن شوند که هرگونه تجهیزات یا تدارکات به موقع جایگزین می‌شوند. هنگامی که یک رخداد فاجعه یا ناآرامی رخ داده است، سخنگوی سازمان باید خبرهای بد را در یک کنفرانس مطبوعاتی به طور اضطراری گزارش دهد، قبل از آنکه مطبوعات این خبر را از طریق کانال دیگری بفهمند. DRP باید کلیه دستورالعمل‌های مربوط به اداره مطبوعات را ارائه دهد. سایت کنفرانس مطبوعاتی اضطراری باید قبل از موعد برنامه ریزی شود.

هنگام از سرگیری عملیات عادی پس از یک رخداد مخرب، سازمان باید در صورت عدم اطلاع از علت این رخداد، تحقیقات کاملی انجام دهد. پرسنل باید کلیه هزینه های مربوط به خسارت را که در نتیجه رخداد رخ می دهد، متقبل شوند. علاوه بر این، باید اقدامات لازم برای جلوگیری از صدمه بیشتر به اموال صورت گیرد.

وجه مشترک بین تمام طرح های بازیابی این است که همه طرح ها منسوخ می شوند. به همین دلیل، نیاز به تست و بروزرسانی دارند.

این بخش شامل بحث در مورد طبقه بندی اولویت های بازیابی دارایی، بازیابی فرایندهای کسب و کار، بازیابی تاسیسات، عرضه و بازیابی فناوری، بازیابی محیط کاربر، بازیابی اطلاعات و آموزش پرسنل است.

طبقه بندی اولویت های بازیابی دارایی Categorize Asset Recovery Priorities

هدف زمان بازیابی (RTO) Recovery time objective، زمان بازیابی کار Work Recovery time (WRT) و مقادیر هدف نقطه بازیابی (RPO) Recovery point objective مقادیری هستند که تعیین می کنند چه راه حل بازیابی انتخاب میشود. RTO مقدار زمانی را که یک سازمان برای بازیابی از یک فاجعه نیاز دارد، تعیین می کند و یک RPO مقدار داده ای را که یک سازمان می تواند هنگام وقوع یک فاجعه از دست بدهد، تعیین می کند. مقادیر RTO، WRT، RPO در طی فرایند BIA بدست می آیند.

در تدوین استراتژی بازیابی، کمیته طرح بازیابی RTO، WRT، RPO را در نظر می گیرد و استراتژی های بازیابی را که باید مورد استفاده قرار گیرد برای اطمینان از این که سازمان این اهداف BIA را برآورده می کند، تعیین می کند.

دستگاه ها، سیستم ها و اپلیکیشن های مهم باید زودتر از دستگاه ها، سیستم ها یا اپلیکیشن ها که در این گروه قرار ندارند، بازیابی شوند. در طبقه بندی سیستم ها، مهمترین سیستم هایی که با استفاده از روش های دستی قابل بازیابی نیست، به خاطر داشته باشید. کمیته طرح بازیابی باید راه حل های پشتیبان / بازیابی موجود را درک کرده و سیستم را اجرا کند که باعث بازیابی در مقادیر BIA و محدودیت های هزینه خواهد شد. عامل کلیدی برای بازیابی قابلیت های پردازش داده ها بر اساس اهمیت عملیات تحت تأثیر قرار می گیرد.

بازیابی فرآیند کسب و کار Business Process Recovery

به عنوان بخشی از DRP، کمیته طرح بازیابی باید روابط متقابل بین فرآیندها و سیستم‌ها را درک کند. یک فرایند کسب و کار مجموعه‌ای از فعالیت‌هایی می‌باشد که خدمات یا محصول خاصی را برای مشتری یا مشتریان خاص تولید می‌کند.

به عنوان مثال، اگر سازمان تشخیص دهد که سیستم حسابداری یک اپلیکیشن مهم است و سیستم حسابداری به یک پایگاه داده مزرعه سرور Server farm متکی است، DRP باید پایگاه داده سرور را به عنوان یک دارایی مهم درج کند. اگرچه بازگرداندن کل پایگاه داده مزرعه سرور برای بازیابی سیستم حسابداری مهم ممکن است لازم نباشد، ولی حداقل یکی از سرورهای موجود در مزرعه برای عملکرد مناسب ضروری می‌باشد. اسناد گردش کار برای هر فرایند کسب و کار باید به کمیته طرح بازیابی ارائه شود. به عنوان بخشی از بازیابی فرایندهای کسب و کار، کمیته طرح بازیابی نیز باید نقش و منابع مورد نیاز فرآیند، ابزارهای ورودی و خروجی و واسطه با سایر فرایندهای کسب و کار را درک کند.

ترمیم تأسیسات Facility Recovery

هنگام برخورد با رخدادی که تأسیسات اولیه را بطور جزئی یا کامل از بین ببرد، سازمان به مکانی جایگزین نیاز دارد که در آنجا فعالیت کند تا اینکه تأسیسات اولیه بازسازی ترمیم شود. DRP باید مکان جایگزین و روشهای بازیابی آن را تعریف کرده، که اغلب به آن یک استراتژی بازیابی سایت گفته می‌شود.

DRP باید شامل نه تنها چگونگی به کار بردن مکان جایگزین به کار کامل، بلکه همچنین نحوه بازگشت سازمان از محل جایگزین به تأسیسات اولیه پس از بازسازی و بهبود باشد. همچنین، برای اهداف امنیتی، DRP باید جزئیاتی در مورد کنترل‌های امنیتی که در مرکز اصلی مورد استفاده قرار گرفتند و دستورالعمل‌های مربوط به نحوه اجرای همین کنترل‌های مشابه در محل جایگزین را درج کنند.

مهمترین عامل در پیدا کردن یک مکان جایگزین در طول توسعه DRP، اطمینان از عدم تأثیر توسط همان فاجعه بر روی مکان جایگزین است. این عامل امکان دارد بدان معنی باشد که سازمان باید یک مکان جایگزین را که در یک شهر یا منطقه جغرافیایی دیگری قرار دارد، انتخاب کند. عوامل اصلی تأثیرگذار بر انتخاب مکان جایگزین شامل موارد زیر است:

- موقعیت جغرافیایی
- نیازهای سازمانی
- هزینه مکان
- تلاش برای ترمیم محل

تست یک مکان جایگزین یک بخش اساسی برای هر DRP است. برخی از مکانها نسبت به سایر مکانها آسانتر هستند.

DRP باید دستورالعمل هایی را در مورد زمان و چگونگی تست دوره ای از تاسیسات متناوب برای اطمینان از سازگاری تاسیسات احتمالی با تاسیسات اولیه درج کند. مکان های متفاوتی که متخصصان امنیت باید برای آزمون CISSP درک کنند شامل موارد زیر است:

- سایت داغ Hot site
- سایت سرد Cold site
- سایت گرم Warm site
- سایت سطح سوم Tertiary site
- توافقات متقابل Reciprocal agreements
- سایت های افزونه Redundant sites

✓ سایت داغ Hot Site

سایت داغ یک مرکز اجاره ای است که شامل تمام منابع مورد نیاز برای بهره برداری کامل می باشد. این محیط شامل رایانه ها، کفپوش ها، تاسیسات کامل، سیم کشی برق و ارتباطات، تجهیزات شبکه و UPS است. اغلب تنها منبعی که باید در یک سایت داغ بازیابی شود، اطلاعات سازمان است. تنها کافی است چند ساعت طول بکشد تا یک سایت داغ به بهره برداری کامل برسد. اگرچه یک سایت داغ سریعترین بازیابی را ارائه می دهد، اما پرهزینه ترین نگهداری را شامل می شود. علاوه بر این، اگر سازمان نیاز به سخت افزار اختصاصی یا نرم افزار اختصاصی داشته باشد، می توان آن را به سختی مدیریت کرد. یک سایت داغ نیاز به کنترل های امنیتی مشابه با تاسیسات اولیه و افزونگی کامل، از جمله سخت افزار، نرم افزار و سیم کشی ارتباطات دارد.

✓ سایت سرد Cold Site

تاسیسات استیجاری که فقط شامل سیم کشی برق و ارتباطات، تهویه هوا، لوله کشی و کفپوش‌ها است. هیچ تجهیزات ارتباطی، سخت افزاری شبکه یا رایانه‌ای در سایت سرد نصب نمی‌شود تا زمانی که لازم باشد سایت به بهره برداری کامل برسد. به همین دلیل، یک سایت سرد برای بازیابی نسبت به یک سایت گرم یا داغ به زمان بسیار بیشتری نیاز دارد. اگرچه یک سایت سرد کمترین حالت بازیابی را دارد، اما نگهداری آن کمترین هزینه را دارد. همچنین دارای سخت ترین تست می‌باشد.

✓ سایت گرم Warm Site

یک سایت گرم یک مرکز اجاره‌ای است که شامل سیم کشی برق و ارتباطات، خدمات کامل و تجهیزات شبکه می‌باشد. در بیشتر موارد، تنها دستگاه‌هایی که در یک سایت گرم قرار نمی‌گیرند، رایانه‌ها هستند. زمان بازسازی سایت گرم از بازسازی سایت داغ طولانی تر اما کوتاهتر از سایت سرد است.

زمان بازسازی و هزینه یک سایت گرم جایی بین یک سایت داغ و سایت سرد است. این مکان بطور گسترده جایگزین مکان اجاره‌ای پیاده سازی می‌شود. اگرچه تست یک سایت گرم از تست یک سایت سرد آسان تر است، اما یک سایت گرم برای تست نسبت به یک سایت داغ نیاز به تلاش بیشتری دارد.

شکل ۷-۹ نموداری است که مولفه‌های مستقر در این سه سایت را مقایسه می‌کند.

	Hot Site	Warm Site	Cold Site
Electrical Connection	Yes	Yes	Yes
Peripherals	Yes	Some	None
Networking	Yes	None	None
Servers and Other Hardware	Yes	None	None
Applications	Yes	None	None

شکل ۷-۹: مقایسه سایت داغ، سایت گرم و سایت سرد

✓ سایت سطح سوم Tertiary Site

یک سایت پشتیبان ثانویه می باشد که در صورت عدم وجود سایت داغ، سایت گرم یا سایت سرد یک جایگزین فراهم می کند. بسیاری از شرکت های بزرگ برای محافظت در برابر فاجعه هایی که مناطق بزرگ جغرافیایی را تحت تأثیر قرار می دهند، سایت های سطح سوم را پیاده سازی می کنند. به عنوان مثال، اگر یک سازمان نیاز به یک مرکز داده دارد که در ساحل واقع شده باشد، این سازمان ممکن است مکان اصلی خود را در نیواورلئان، لوئیزیانا و سایت داغ خود به صورت سیار در آلاباما داشته باشد. این سازمان ممکن است محلی را برای تعیین سایت سطح سوم در میامی، فلوریدا در نظر بگیرد، زیرا طوفان می تواند هر دو ساحل خلیج لوئیزیانا و خلیج آلاباما را تحت تأثیر قرار دهد.

✓ توافقات متقابل Reciprocal Agreements

توافق متقابل توافق بین دو سازمان است که نیازهای تکنولوژیکی و زیرساخت های مشابهی دارند. در این توافق، هر دو سازمان موافقت می کنند که در صورت عدم استفاده از هر یک از تاسیسات اولیه سازمان، به عنوان یک مکان جایگزین برای دیگری عمل کنند. متأسفانه در بیشتر موارد، این توافقات قابل پیاده سازی نیستند. یک نقطه ضعف این سایت این است که ممکن است نتواند بار کاری و عملکرد مورد نیاز سازمان دیگر را تحمل کند.

توجه داشته باشید

توافق کمک های متقابل یک توافق (Mutual aid agreement) از پیش تنظیم شده بین دو سازمان است که در آن هر سازمان موافقت می کند در صورت بروز فاجعه به دیگری کمک کند.

سایت های افزونه Redundant sites

سایت افزونه یا سایت منعکس کننده Mirrored site سایتی است که به صورت یکسان مثل سایت اصلی پیگیری شده است. یک سایت افزونه یا منعکس کننده یک سایت اجاره ای نیست بلکه معمولاً متعلق به همان سایت اصلی سازمان است. سازمان وظیفه حفظ سایت افزونه را بر عهده دارد. سایت های پردازش چندگانه نیز می توانند پیگیری شوند تا به عنوان سایت های افزونه فعالیت کنند.

اگرچه سایت‌های افزونه برای نگهداری بسیار پرهزینه هستند، اما بسیاری از سازمان‌ها امروزه اینگونه سایت‌ها را به عنوان یک هزینه لازم برای اطمینان از ارائه خدمات بی وقفه می‌دانند.

تهیه و بازیابی فناوری Supply and Technology Recovery

اگرچه بازیابی تأسیسات اغلب دغدغه‌ای برای فاجعه‌های کوچک یا رخداد‌های مخرب ندارد، اما تقریباً تمام تلاش‌های بازیابی معمولاً مستلزم بازیابی منابع و فناوری است. سازمان‌ها باید مطمئن شوند که هر DRP شامل دستورالعمل‌ها و روش‌های بازیابی منابع و فناوری است. به عنوان بخشی از تأمین و بازیابی فناوری، DRP باید در صورت خرید لوازم جدید و دارایی‌های فناوری، کلیه اطلاعات تماس با فروشنده را در بر بگیرد. DRP باید شامل اطلاعات بازیابی در مورد دارایی‌های زیر باشد که باید ترمیم شوند:

- تهیه نسخه پشتیبان از سخت افزار
- تهیه نسخه پشتیبان از نرم افزار
- منابع انسانی
- گرمایش، تهویه و تهویه هوا (HVAC)
- تدارکات
- مستندات

۱- پشتیبان از سخت افزار Hardware Backup

سخت افزاری که باید به عنوان بخشی از DRP گنجانده شود، شامل رایانه‌های مشتری، رایانه‌های سرور، روترها، سوئیچ‌ها، فایروال‌ها و هر سخت افزار دیگری است که در شبکه سازمان در حال اجرا است. DRP نه تنها باید دستورالعمل‌ها و روش‌های بازیابی تمام داده‌های موجود در هر یک از این دستگاه‌ها را داشته باشد بلکه اطلاعاتی را در مورد بازیابی این سیستم‌ها به صورت دستی در صورت آسیب دیدن یا به طور کامل تخریب شدن سیستم‌ها، نیز درج کند. دستگاه‌های میراثی که دیگر در بازار خرده فروشی موجود نیستند نیز باید شناسایی شوند.

به عنوان بخشی از تهیه DRP، تیم برنامه بازیابی باید مقدار زمانی را که فروشندگان سخت افزار در اختیار آنها قرار می‌دهد جایگزینی برای هر سخت افزار آسیب دیده یا از بین رفته تعیین کنند. بدون داشتن این اطلاعات مستند، هرگونه برنامه بازیابی به دلیل کمبود منابع ممکن است بی تاثیر باشد. اگر فروشندگان قادر به تهیه سخت افزار جایگزینی به موقع نباشند، ممکن است

سازمان‌ها نیاز به گزینه‌های دیگر، از جمله خرید سیستم‌های افزونه و ذخیره آنها در یک مکان جایگزین، داشته باشند. در صورت امکان جایگزینی دستگاه‌های قدیمی، سازمان‌ها باید قبل از وقوع فاجعه اقدامات لازم را برای جایگزینی آنها انجام دهند.

۲- نسخه پشتیبان از نرم افزار Software Backup

حتی اگر یک سازمان از هر دستگاهی برای بازگرداندن زیرساخت‌های خود لازم داشته باشد، در صورت عدم دسترسی به اپلیکیشن‌ها و نرم افزارهایی که در دستگاه‌ها اجرا می‌شوند، این دستگاه‌ها بی فایده هستند، اپلیکیشن‌ها و نرم افزارها شامل هر سیستم عامل، پایگاه‌های داده و اپلیکیشن‌های لازم برای اجرا روی دستگاه هستند.

بسیاری از سازمان‌ها ممکن است فکر کنند که در صورت داشتن نسخه پشتیبان در هر نوار، دی وی دی، فلش درایو، هارد دیسک و یا رسانه‌های دیگر از نرم افزارهای خود، این شرط برآورده می‌شود. اما کلیه نرم افزاری که از آن نسخه پشتیبان تهیه شده است، حداقل به یک سیستم عامل نیاز دارند که روی دستگاهی که در آن بازایی شده است، پیاده سازی شوند. این نسخه‌های پشتیبان از داده‌ها اغلب نیاز دارند که نرم افزار مدیریت پشتیبان در دستگاه پشتیبان گیری کار کند، خواه سرور باشد یا دستگاه اختصاصی.

کلیه رسانه‌های نصب نرم افزار، بسته‌های سرویس و سایر بروزرسانی‌های لازم باید در یک مکان جایگزین ذخیره شوند. علاوه بر این، تمام اطلاعات مجوز لیسانس باید به عنوان بخشی از DRP ثبت شود. سرانجام، باید از پشتیبان‌های مکرر اپلیکیشن‌ها استفاده شود، خواه از طریق سیستم پشتیبان داخلی اپلیکیشن یا از طریق پشتیبان سازمانی دیگر. تهیه نسخه پشتیبان فقط در صورت بازگرداندن مفید است بنابراین DRP باید تمام مراحل مربوط به آن را کاملاً مستند کند. در بسیاری موارد، اپلیکیشن‌ها از یک فروشنده نرم افزار خریداری می‌شوند و فقط فروشنده نرم افزار کد نویسی را که در اپلیکیشن‌ها رخ می‌دهد درک می‌کند. از آنجا که هیچ تضمینی در بازار امروز وجود ندارد، برخی از سازمان‌ها ممکن است که برای اطمینان از محافظت در برابر نابودی یک فروشنده نرم افزار، باید تصمیمی اتخاذ کنند. Escrow نرم افزار توافقی است که به موجب آن به شخص ثالث کد منبع نرم افزار داده می‌شود تا مطمئن شود که در صورت بروز شرایط خاص برای فروشنده نرم افزار، از جمله ورشکستگی و فاجعه، مشتری به کد منبع دسترسی دارد.

۳- منابع انسانی Human Resources

هیچ سازمانی قادر به فعالیت بدون پرسنل نیست. برنامه اضطراری سرنشینان به طور خاص روشهایی را برای به حداقل رساندن تلفات یا آسیب دیدگی هنگام وقوع تهدید، مورد بررسی قرار می‌دهد. تیم منابع انسانی مسئولیت تماس با کلیه پرسنل در صورت بروز فاجعه را برعهده دارد. اطلاعات تماس کلیه کارکنان باید در محل و خارج از سایت نگهداری شود. اعضای متعدد تیم HR باید به اطلاعات تماس پرسنل دسترسی داشته باشند. به خاطر داشته باشید که ایمنی پرسنل همیشه دغدغه اصلی است. کلیه منابع دیگر فقط پس از ایمن بودن پرسنل باید محافظت شوند.

پس از اتمام رخداد اولیه، تیم HR باید روحیه پرسنل و محافظت در مقابل استرس و فرسودگی کارکنان را در طی دوره بهبودی نظارت کند. اگر آموزش متقاطع مناسبی روی داده باشد، می‌توان چندین پرسنل را در طی مراحل بهبودی چرخاند. هر DRP باید نیاز به فراهم کردن دوره‌های استراحت کافی را برای هرگونه پرسنل درگیر در فرآیند بازیابی حوادث در نظر بگیرد. همچنین باید دستورالعمل‌های مربوط به چگونگی جایگزینی هر پرسنلی که قربانی فاجعه هستند را شامل شود.

سازمان باید مطمئن شود که حقوق و سایر بودجه برای پرسنل در حین و بعد از فاجعه تداوم دارد. از آنجا که بودجه می‌تواند هم برای پرسنل و هم برای خرید منابع بسیار مهم باشد، بررسی‌های مجاز و امضا شده باید به صورت ایمن در محلی ذخیره شود. در صورت عدم دسترسی به مدیریت ارشد، مدیریت سطح پایین با کنترل دسترسی مناسب باید توانایی پراکندگی وجوه را با استفاده از چک‌ها داشته باشد.

همچنین باید یک برنامه جانشینی اجرایی ایجاد شود تا مطمئن شود که سازمان اقدامات لازم را برای حمایت از خود و ادامه فعالیت انجام می‌دهد.

۴- تدارکات Supplies

غالباً فاجعه در تأمین منابع مورد نیاز سازمان از جمله کاغذ، کابل کشی و حتی آب تأثیر می‌گذارد. سازمان باید منابعی را که برای فعالیتهای روزمره خود حیاتی است و فروشندگانی که از این منابع می‌توان بدست آورد، مستند سازد. از آنجا که فروشندگان تدارکات نیز می‌توانند از این فاجعه متاثر شوند، باید تأمین کنندگان جایگزین نیز شناسایی شوند.

۵- مستندات Documentation

برای اینکه موفقیت در برابر بحران موفقیت آمیز باشد، پرسنل درگیر باید قادر به انجام مراحل بازیابی مناسب باشند. اگرچه مستندات کلیه این رویه ها ممکن است خسته کننده باشد، اما لازم است مطمئن شود که بازیابی اتفاق می افتد. علاوه بر این، از هر بخش در سازمان خواسته می شود تصمیم بگیرند که مستندات دپارتمان برای انجام کارهای روزانه مورد نیاز است. این اسناد باید در یک مکان مرکزی در محلی ذخیره شود و یک نسخه نیز در خارج از مکان سازمان نگهداری شود. پرسنل خاص باید وظیفه داشته باشند که تهیه این اسناد، در صورت مناسب، ذخیره و به روز شوند.

بهبود محیط کاربر User Environment Recovery

کلیه جنبه های بهبود محیط کاربر نهایی باید به عنوان بخشی از DRP گنجانده شود تا مطمئن شود که کاربران نهایی می توانند در اسرع وقت به کار خود باز گردند. به عنوان بخشی از این بهبود محیط کاربر، اعلان کاربر نهایی باید رخ دهد. پس از وقوع یک فاجعه باید به کاربران اطلاع داده شود که پس از بروز فاجعه از کجا و از چه زمانی گزارش کنند. بهبود واقعی محیط کاربر باید به صورت مرحله ای انجام شود، که مهمترین عملکردها در ابتدا ترمیم می شوند. الزامات کاربر باید مستند سازی شود تا تضمین شود که تمام جنبه های محیط کاربر بهبود می یابد. به عنوان مثال، کاربران در یک بخش مهم ممکن است همه به رایانه مشتری خود نیاز داشته باشند. همین کاربران ممکن است به یک اپلیکیشن که در یک سرور قرار دارد نیز نیاز داشته باشند. اگر سرور بازیابی نشود، کاربران حتی در صورت موجود بودن رایانه های مشتری خود قادر به انجام وظایف شغلی خود نخواهند بود.

در نهایت، مراحل دستی که می تواند برای هر عملکردی مورد استفاده قرار گیرد، باید مستند شود. از آنجا که ما امروزه به فناوری وابسته هستیم، اغلب از روش های دستی برای انجام کارهای شغلی خود غافل می شویم. مستندسازی این روشهای دستی ممکن است تضمین کند که عملیات رخ می دهد حتی اگر با نرخ کاهش یافته اتفاق بیفتد.

بازیابی داده Data Recovery

در بیشتر سازمان ها، داده‌ها یکی از مهمترین دارایی‌ها هنگام بازیابی از یک فاجعه است. BCP ها و DRP ها باید دستورالعمل‌ها و روش‌های بازیابی داده را در بر گیرند. با این حال، تیم‌های عملیاتی باید مشخص کنند که از کدام داده‌ها نسخه پشتیبان تهیه شده، چند بار از داده‌ها نسخه پشتیبان تهیه شده و روش تهیه نسخه پشتیبان چیست. بنابراین زمانیکه که این بخش در مورد پشتیبان گیری از داده‌ها بحث می‌کند، به خاطر داشته باشید که تیم‌های BCP در واقع هیچ تصمیمی برای تهیه نسخه پشتیبان از داده‌ها ندارند. تیم‌های BCP در درجه اول دغدغه این موضوع را دارند که داده‌های پشتیبان گرفته شده را به موقع بازیابی کنند.

در این بخش درمورد انواع و برنامه‌های تهیه نسخه پشتیبان از داده‌ها و همچنین روش‌های پشتیبان گیری الکترونیکی که سازمانها می‌توانند پیاده سازی کنند، بحث می‌شود.

طرح‌های کلی و انواع نسخه پشتیبان از داده‌ها Data Backup Types and Schemes

برای طراحی یک راه حل مناسب برای بازیابی داده، متخصصان امنیت باید انواع مختلفی از تهیه نسخه پشتیبان از داده‌ها را که می‌تواند رخ دهد و نحوه استفاده از این پشتیبان‌ها در کنار هم را برای بازگرداندن محیط‌های زنده درک کنند. برای آزمون CISSP، متخصصان امنیت باید طرح‌های کلی و انواع نسخه پشتیبان از داده‌های زیر را درک کنند:

- پشتیبان گیری کامل
- پشتیبان گیری دیفرانسیل (پشتیبان گیری متغیر)
- پشتیبان گیری افزایشی
- کپی نسخه پشتیبان
- تهیه نسخه پشتیبان روزانه
- پشتیبان گیری تراکنش log
- در مرحله اول، ابتدا استفاده از برنامه چرخش
- طرح چرخش پدر بزرگ / پدر / پسر

سه نسخه پشتیبان داده اصلی عبارتند از پشتیبان گیری کامل، پشتیبان گیری‌های دیفرانسیل و پشتیبان گیری‌های افزایشی. برای درک این سه نوع پشتیبان داده، باید مفهوم بیت بایگانی

Archive Bit درک شود. وقتی یک فایل ایجاد یا به روز می شود، بیت بایگانی فایل فعال می شود. اگر بیت بایگانی پاک شود، فایل در طی تهیه نسخه پشتیبان بعدی بایگانی نمی شود. اگر بیت بایگانی فعال باشد، فایل در طی تهیه نسخه پشتیبان بعدی بایگانی می شود.

با داشتن پشتیبان گیری کامل، از کلیه داده ها پشتیبان تهیه می شود. در طی مراحل پشتیبان گیری کامل، بیت بایگانی برای هر فایل پاک می شود. تهیه نسخه پشتیبان کامل طولانی ترین زمان و بیشترین مکان برای تکمیل شدن دارد. با این حال، اگر یک سازمان فقط از پشتیبان گیری کامل استفاده می کند، فقط آخرین نسخه پشتیبان کامل باید بازیابی شود. هر نسخه پشتیبانی که از پشتیبان گیری دیفرانسیل و افزایشی استفاده کند، ابتدا با یک نسخه پشتیبان کامل به عنوان پایه اصلی (خط مبنا) آن شروع می شود. تهیه نسخه پشتیبان کامل مناسب ترین نسخه برای ساخت بایگانی خارج از سایت (مکان سازمان) است.

در یک نسخه پشتیبان دیفرانسیل، از کلیه فایل هایی که در آخرین نسخه پشتیبان کامل تغییر یافته است، نسخه پشتیبان تهیه می شود. در طی فرآیند تهیه نسخه پشتیبان دیفرانسیل، مقدار بایگانی برای هر فایل پاک نمی شود. تهیه نسخه پشتیبان دیفرانسیل تهیه شده ممکن است از زمان کوتاه و فضای کمی تا افزایش در زمان تهیه نسخه پشتیبان و مقدار فضای مورد نیاز خود متفاوت باشد. اگر پشتیبان گیری کامل از ابتدای آن زمان رخ نداده باشد، هر نسخه پشتیبان دیفرانسیل از کلیه فایل های موجود در نسخه پشتیبان تهیه شده قبلی استفاده می کند. در سازمانی که از یک طرح کامل / دیفرانسیل استفاده می شود، باید فقط پشتیبان گیری کامل و آخرین نسخه پشتیبان دیفرانسیل بازیابی شود، یعنی فقط به دو نسخه پشتیبان نیاز می باشد.

یک نسخه پشتیبان افزایشی تهیه شده از کلیه فایل هایی که از آخرین پشتیبان گیری کامل یا افزایشی تغییر یافته، تهیه می شود. در طی مراحل پشتیبان گیری افزایشی، مقدار بایگانی برای هر فایل پاک می شود. یک نسخه پشتیبان تهیه افزایشی معمولاً کمترین زمان و مکان را برای تکمیل نیاز دارد. در سازمانی که از یک طرح کامل / افزایشی استفاده می کند، پشتیبان گیری کامل و هر نسخه پشتیبان افزایشی بعدی باید بازیابی شود. پشتیبان گیری های افزایشی باید به ترتیب ترمیم شوند. اگر سازمان شما یک پشتیبان گیری کامل از روز یکشنبه و یک نسخه پشتیبان افزایشی روزانه را از دوشنبه تا شنبه انجام دهد، برای ترمیم داده ها به حداکثر هفت نسخه پشتیبان نیاز است. شکل ۷-۱۰ انواع پشتیبان تهیه می کند.

Backup Type	Data Backed Up	Backup Time	Restore Time	Storage Space
Full Backup	All Data	Slowest	Fast	High
Incremental Backup	Only New/Modified Files/Folders	Fast	Moderate	Lowest
Differential Backup	All Data Since Last Full	Moderate	Fast	Moderate

شکل ۷-۱۰: مقایسه انواع پشتیبان

نسخه پشتیبان کپی و نسخه پشتیبان روزانه، دو نوع نسخه پشتیبان ویژه هستند که جزء برنامه‌های تهیه پشتیبان مکرر برنامه ریزی شده محسوب نمی‌شوند، زیرا برای ترمیم به هیچ نوع پشتیبان دیگری احتیاج ندارند. تهیه نسخه پشتیبان از کپی شبیه به نسخه‌های پشتیبان معمولی است اما مقدار بایگانی فایل را دوباره تنظیم نمی‌کند. نسخه پشتیبان تهیه روزانه از زمانسج یک فایل برای تعیین نیاز به بایگانی کردن استفاده می‌کند. تهیه نسخه پشتیبان روزانه در محیط‌های بحرانی که در آن چندین نسخه پشتیبان روزانه مورد نیاز است، رایج است زیرا فایل‌ها به طور مداوم به روز می‌شوند.

تهیه نسخه پشتیبان تراکنش (log (Transaction)، فقط در محیط‌هایی استفاده می‌شود که گرفتن همه تراکنش‌هایی که از آخرین نسخه پشتیبان تهیه شده است مهم است. پشتیبان‌گیری تراکنش log به سازمان‌ها کمک می‌کند به بازیابی در یک نقطه خاص و در زمان خاص دست یافته و بیشتر در محیط‌های پایگاه داده استفاده می‌شوند.

اگرچه درایوهای نوار مغناطیسی هنوز هم برای تهیه نسخه پشتیبان از داده‌ها استفاده می‌شوند، امروزه بسیاری از سازمان‌ها داده‌های خود را در دیسک‌های نوری از جمله CD-ROM، DVD و دیسک‌های Blu-ray، درایوهای مغناطیسی با ظرفیت بالا و پر سرعت، رسانه مبتنی بر فلش، یا رسانه‌های دیگر قرار می‌دهند. مهم نیست که رسانه‌ها استفاده شده اند، حفظ پشتیبان از هر سایت و خارج از سایت مهم می‌باشد. نسخه‌های پشتیبان در محل در یک ضد آب یا مقاوم در برابر حرارت، مقاوم در برابر آتش، ذخیره شود.

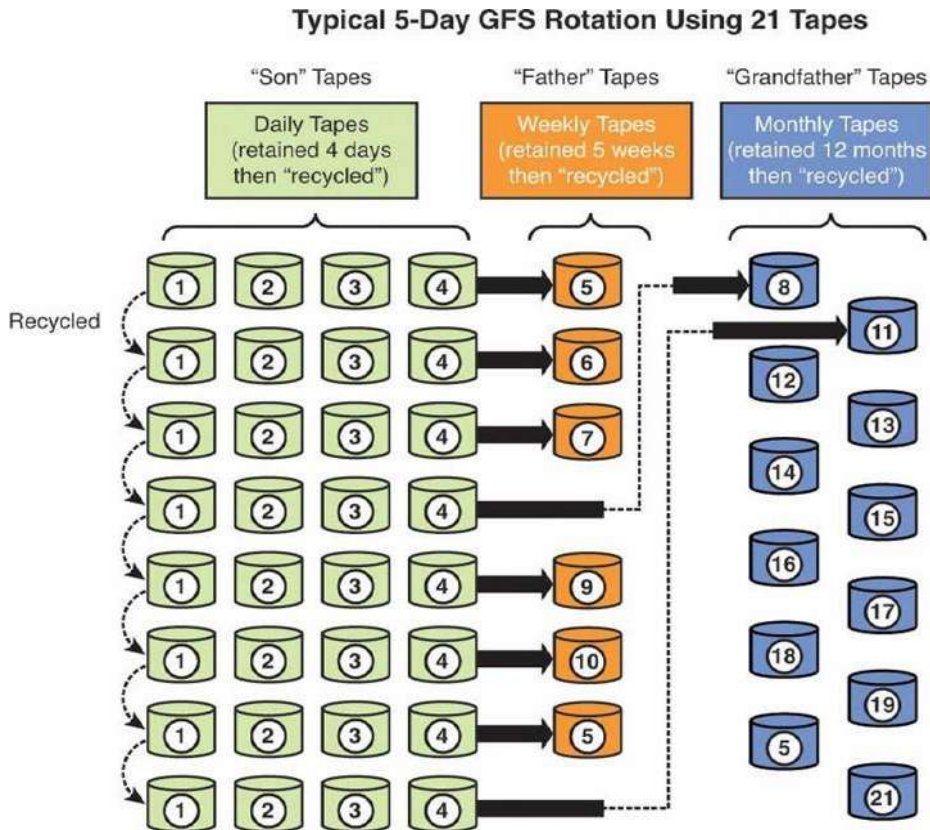
به عنوان بخشی از هر برنامه پشتیبان‌گیری، یک سازمان همچنین باید از برنامه چرخش پشتیبان استفاده کند. ملاحظات مربوط به هزینه و ذخیره سازی اغلب بیانگر این است که پس از مدتی

استفاده مجدد، از رسانه های پشتیبان استفاده شود. اگر این استفاده مجدد از قبل برنامه ریزی نشده باشد، استفاده بیش از حد رسانه ها می تواند غیرقابل اعتماد باشند. دو مورد از رایج ترین طرح چرخش پشتیبان، اول ورود اول خروج، و پدربزرگ / پدر / پسر هستند.

در طرح اول ورود، اول خروج (First in, First out (FIFO جدیدترین نسخه پشتیبان در قدیمی ترین رسانه ها ذخیره می شود. اگرچه این ساده ترین طرح چرخش است، اما از خطاهای داده محافظت نمی کند. اگر خطایی در داده ها وجود داشته باشد، ممکن است سازمان نسخه ای از داده های دارای خطا را نداشته باشد.

در طرح پدربزرگ / پدر / پسر (Grandfather/Father/Son (GFS سه مجموعه پشتیبان تعریف شده است. ۳ مجموعه اغلب روزانه، هفتگی و ماهانه است. تهیه نسخه پشتیبان روزانه پسران هستند، پشتیبان های هفتگی پدران هستند و تهیه پشتیبان ماهانه پدربزرگ ها است. هر هفته، یک پسر در مجموعه پدر پیشرفت می کند و هر ماه، یک پدر در مجموعه پدربزرگ پیشرفت می کند.

شکل ۷-۱۱ چرخش معمولی ۵ روزه GFS را با استفاده از ۲۱ نوار نشان می دهد. نوارهای (Tape) روزانه معمولاً از پشتیبان گیریه های دیفرانسیل یا افزایشی هستند. نوارهای هفتگی و ماهانه باید یک نسخه پشتیبان گیری کامل باشند.



شکل ۷-۱۱: طرح چرخش پشتیبان پدر بزرگ / پدر / پسر

پشتیبان گیری الکترونیکی Electronic Backup

راه حل های پشتیبان گیری الکترونیکی از داده ها سریعتر و دقیق تر از نسخه پشتیبان گیری های عادی، پشتیبان تهیه می کنند و در هنگام تغییر اطلاعات اغلب به بهترین وجه پیاده سازی می شوند.

برای آزمون CISSP، باید با شرایط و راه حل های پشتیبان الکترونیکی زیر آشنا باشید:

✓ Vaulting Electronic: کپی ها در هنگام وقوع تغییرات، این روش در زمان واقعی (Real Time) اتفاق می افتد.

✓ Remote journaling: روزنامه یا تراکنش ورود خارج از سایت را در یک زمان بندی منظم کپی می کند. این روش در دسته ها اتفاق می افتد.

- ✓ Tape vaulting: ایجاد پشتیبان از طریق یک خط ارتباط مستقیم به سیستم پشتیبان در یک مرکز خارج از سایت.
 - ✓ مدیریت ذخیره سازی سلسله مراتبی (HSM): Hierarchical Storage Management: فروشگاهها اغلب به داده های رسانه ای تندتر، سریعتر دسترسی دارند و کمتر به داده های رسانه کندتر دسترسی دارند.
 - ✓ جعبه نوری Optical jukebox: داده ها را روی دیسک های نوری ذخیره می شوند و از روباتیک برای بارگذاری load و تخلیه دیسک های نوری در صورت نیاز استفاده می شود. این روش در صورت نیاز ۲۴/۷ در دسترس می باشد که ایده آل است.
 - ✓ همانندسازی Replication: داده ها را از یک مکان ذخیره به مکان دیگر کپی می کند. سنکرون های (همزمان) همانندسازی با استفاده از داده های ثابت بروزرسانی را تضمین می کنند که در یک مکان نزدیک در همان زمان هستند، در حالی که همانند سازی آسنکرون (غیرهمزمان) بروزرسانی ها را با توجه به زمان بندی از پیش تعیین شده به تأخیر می اندازد.
- بسیاری از شرکت ها از راه حل های تهیه نسخه پشتیبان ابری یا همانند سازی استفاده می کنند. هر سازمانی که راه حل ابری را در نظر بگیرد، باید درباره پیامدهای امنیت کامل در این نوع استقرار تحقیق کند.

آموزش پرسنل Training Personnel

حتی اگر یک سازمان برای توسعه دقیق ترین BCP و DRP اقدامات لازم را انجام دهد، در صورتی که کارکنان سازمان در هنگام بروز فاجعه مهارت لازم برای بازیابی کامل دارایی های سازمان را نداشته باشند، این برنامه ها بی فایده است. برای اطمینان از وقوع آموزش کافی باید به پرسنل زمان و منابع مالی مناسب داده شود، که شامل اجازه دادن به پرسنل برای تست DRP می شود. آموزش باید از منابع داخلی و خارجی انجام شود. هنگامی که وظایف شغلی تغییر می کند یا پرسنل جدید استخدام می شوند، باید سیاست هایی اتخاذ شود تا انتقال مناسب دانش تضمین شود.

بهبود فاجعه Disaster Recovery

بهبود فاجعه شامل بازیابی خدمات و سیستم‌ها از وضعیت اضطراری یا وضعیت موقت است که ممکن است عملیات در جایی باشد که در حال اجرا هستند اما در مرکز اصلی یا منابع بهینه قرار ندارند. برنامه بهبود فاجعه (Disaster recovery plan (DRP به تفصیل در فصل ۱ مورد بحث قرار گرفته است. در این فصل، ما در مورد فرآیند بهبود فاجعه بیشتر، از نظر واکنش، پرسنل، ارتباطات، ارزیابی، ترمیم آموزش و آگاهی بحث می‌کنیم.

۱- واکنش Response

پس از وقوع یک رخداد، باید پرسنل مربوطه برای شروع ارتباطاتی که به تیم بازیابی مناسب و پرسنل آسیب دیده رخداد هشدار داده و تماس بگیرند. سپس تمام تیم‌های ذکر شده در بخش پرسنل باید وظایف خود را انجام دهند. یک فرآیند سلسله مراتبی باید به گونه‌ای تدوین شود که هر تیم وظایف خود را به عنوان بخشی از فرآیند بهبود فاجعه به ترتیب صحیح انجام دهد.

۲- پرسنل Personnel

اگرچه اولویت‌های شماره یک و شماره دو هنگام وقوع یک فاجعه، ایمنی و سلامتی پرسنل و کاهش خسارت است، به همین ترتیب، پس از رسیدگی به این دو، بهبودی از یک فاجعه به سرعت تبدیل به اولویت سازمان می‌شود. با این حال، در صورت عدم آموزش صحیح پرسنل و آماده سازی، هیچ سازمانی نمی‌تواند از یک فاجعه بهبود یابد. برای اطمینان از اینکه پرسنل می‌توانند وظایف خود را در هنگام بهبودی در برابر سوانح انجام دهند، باید وظایف شغلی خود را بدانند و درک کنند.

در طی هر گونه بهبود فاجعه، مدیریت مالی بسیار مهم است. مدیریت مالی معمولاً شامل رئیس ارشد مالی و سایر پرسنل اصلی حسابداری می‌باشد. این گروه باید هزینه‌های بهبود را ردیابی کرده و پیش بینی‌های گردش پول را ارزیابی کنند. آنها بطور رسمی هرگونه بیمه گر Insurer را از مطالبات مطرح شده مطلع می‌کنند. سرانجام، این گروه وظیفه تعیین دستورالعمل‌های ادامه کارمزد، تهیه رویه‌ها و مراحل پیگیری هزینه‌های اضطراری را برعهده دارند.

سازمان‌ها باید تصمیم بگیرند که تیم‌ها در هنگام بهبود فاجعه نیاز هستند و از قرار گرفتن پرسنل مناسب در هر یک از این تیم‌ها مطمئن شوند. مدیر بهبود فاجعه اقدامات بهبود کوتاه مدت را بلافاصله پس از یک فاجعه هدایت می‌کند.

سازمانها ممکن است برای ارائه پشتیبانی مناسب از DRP، تیم های زیر را پیاده سازی کنند:

- تیم ارزیابی خسارت Damage Assessment Team
- تیم حقوقی Legal Team
- تیم روابط رسانه ای Media Relations Team
- تیم بازیابی Recovery Team
- تیم جابجایی Relocation Team
- تیم ترمیم Restoration Team
- تیم نجات Salvage Team
- تیم امنیت Security Team

✓ تیم ارزیابی خسارت Damage Assessment Team

وظیفه تعیین علت بروز فاجعه و میزان خسارت وارده به دارایی های سازمان را بر عهده دارد. این تیم کلیه دارایی های درگیر و عملکرد دارایی های مهم پس از فاجعه را شناسایی می کند. تیم ارزیابی خسارت تعیین می کند که کدام دارایی ها به ترمیم و جایگزینی نیاز دارند و با تیم های مناسب که باید فعال شوند، تماس گرفته می شود.

✓ تیم حقوقی Legal Team

این تیم حقوقی بلافاصله پس از فاجعه و در هنگام بهبود فاجعه به کلیه موضوعات حقوقی رسیدگی می کند. اگرچه تیم روابط رسانه ای پیام را ارسال می کند، تیم حقوقی بر وقایع روابط عمومی که برای رفع این فاجعه برگزار می شود، نظارت می کند. برای اطمینان از عدم رعایت کلیه عملیات بهبود قوانین و مقررات فدرال و ایالتی باید با تیم حقوقی مشورت کرد.

✓ تیم روابط رسانه ای Media Relations Team

تیم روابط رسانه ای هر زمان که شرایط اضطراری فراتر از تاسیسات سازمان براساس دستورالعمل مندرج در DRP ارائه شود، به اطلاع عموم و رسانه می رساند. سایت کنفرانس مطبوعاتی اضطراری باید از قبل برنامه ریزی شود. هنگام انتشار بیانیه های عمومی، تیم روابط رسانه ای باید درباره آنچه که درباره این رخداد و تأثیرات آن شناخته شده است، صادقانه و دقیق باشند. پاسخ سازمان به رسانه ها در حین و بعد از این رخداد باید متحد و یکسان باشد.

یک سخنگوی معتبر و آگاه باید واکنش سازمان را ارائه دهد. سخنگو هنگام برخورد با رسانه‌ها پس از فاجعه، باید خبرهای بد را قبل از کشف رسانه از طریق کانال‌های دیگر گزارش دهد. هرکسی که خبرهای فاجعه را به مردم اعلام می‌کند، باید درک کند که مخاطب چنین خبرهایی شامل رسانه‌ها، اتحادیه‌ها، ذینفعان، همسایگان، کارمندان، پیمانکاران و حتی رقبا می‌باشند.

✓ تیم بازیابی Recovery Team

وظیفه اصلی تیم بازیابی عملکردهای کسب و کار مهم در تأسیسات جایگزین است. این تیم بیشتر شامل اطمینان از وجود دارایی‌های فیزیکی، از جمله رایانه‌ها و سایر دستگاه‌ها، سیم کشی و غیره است. تیم بازیابی معمولاً بر تیم‌های جابجایی و ترمیم نظارت می‌کند.

✓ تیم جابجایی Relocation Team

تیم جابجایی بر انتقال واقعی دارایی‌ها بین مکان نظارت می‌کند که شامل انتقال دارایی از سایت اصلی به سایت جایگزین و سپس برگشت آن دارایی‌ها در هنگام آماده شدن سایت اولیه برای فعالیت است.

✓ تیم ترمیم Restoration Team

تیم ترمیم در واقع تضمین می‌کند که دارایی‌ها و داده‌ها به عملیات بازگردانده می‌شوند. تیم ترمیم نیاز به دسترسی به رسانه پشتیبان دارد.

✓ تیم نجات Salvage Team

تیم نجات تمام دارایی‌های موجود در محل فاجعه را بازیابی می‌کند و اطمینان می‌دهد که سایت اولیه به حالت عادی باز می‌گردد. تیم نجات، تمیز کردن تجهیزات، بازسازی تأسیسات اصلی را مدیریت می‌کند و هرگونه متخصصی را برای کار در فرایند بازیابی مشخص می‌کند. در بیشتر موارد، تیم نجات وقتی عملیات می‌تواند در محل فاجعه مجدد ادامه یابد، اعلام می‌کند.

✓ تیم امنیت Security Team

تیم امنیت مسئولیت مدیریت امنیت را در هر دو سایت فاجعه و هر مکان جایگزین که سازمان در طی بازیابی از آن استفاده می‌کند، بر عهده دارد. از آنجا که منطقه جغرافیایی که تیم امنیت

پس از فاجعه باید مدیریت کند اغلب بسیار بزرگتر است، ممکن است تیم امنیت برای کمک به این روند نیاز به استخدام پیمانکاران خارجی داشته باشد. استفاده از این پیمانکاران خارجی برای محافظت از دسترسی فیزیکی به سایت ها و استفاده از منابع داخلی برای تأمین امنیت در داخل تاسیسات همیشه بهتر است زیرا کاهش این وضعیت ممکن است صدور اعتبار دسترسی مناسب را برای پیمانکاران را دشوار کند.

۱- ارتباطات Communications

ارتباط در حین بهبود فاجعه برای اطمینان از اینکه سازمان به موقع بهبود می یابد مهم است. همچنین مهم است که تضمین شود که هیچ پستی حذف نشده و مراحل به صورت صحیح اتفاق می افتد. ارتباط با پرسنل بستگی به این دارد که چه کسی در مورد فاجعه با شما تماس می گیرد. پرسنل متضرر از یک فاجعه باید ارتباطاتی دریافت کنند که در آن سیستم های آسیب دیده، زمان خاموشی پیش بینی شده و هرگونه احتمالی را که باید در این میان دنبال کرد، دریافت کنند. تیم های مختلف برای بهبود فاجعه باید ارتباطاتی را دریافت کنند که مربوط به وظایف خود در هنگام بهبودی فاجعه باشد.

در حین بهبود، متخصصان امنیت باید با تیم های مختلف همکاری نزدیکی داشته باشند تا از حفظ تمام دارایی ها مطمئن شوند. همه تیم های درگیر در این فرایند همچنین اغلب باید با یکدیگر ارتباط برقرار کنند تا پیشرفت در مورد یکدیگر به روز شود.

۲- ارزیابی Assessment

هنگامی که یک رخداد اتفاق می دهد، پرسنل باید شدت و تأثیر آن را ارزیابی کنند. با انجام این کار تضمین شود که واکنش مناسب انجام شده است.

بیشتر سازمان ها دسته بندی رخدادها را تشکیل می دهند، از جمله غیر رخداد، رخداد و رخداد شدید (Non-incident, Incident, Severe incident). هر سازمان باید فرایند ارزیابی فاجعه را در پیش بگیرد تا تضمین شود که پرسنل هر رخداد را به درستی ارزیابی می کنند.

۳- ترمیم Restoration

روند ترمیم شامل بازگرداندن سیستم ها و تاسیسات اولیه به عملکرد عادی است. پرسنل درگیر در این فرایند به دارایی هایی که در این رخداد تحت تأثیر قرار گرفته اند، بستگی دارد. هر تیمی

که در بازیابی دارایی‌ها نقش دارد باید تلاش‌های خود را برای بازیابی دقیق انجام دهد. بدون هماهنگی دقیق، بازیابی می‌تواند تأثیر منفی بگذارد. به عنوان مثال، اگر بازیابی کامل یک برنامه وب مستلزم عملکرد سرورهای پایگاه داده باشد، ادمین پایگاه داده باید با ادمین برنامه وب همکاری نزدیک داشته باشد تا اطمینان حاصل شود که هر دو (برنامه وب و پایگاه داده) به عملکرد عادی بازگردانده شده است.

۴- آموزش و آگاهی Training and Awareness

به پرسنل در تمام سطوح نیاز است که آموزش صحیحی در مورد فرآیند بهبود فاجعه ارائه شود. به کاربران عادی فقط باید آموزش و آگاهی داده شود تا روند پیچیدگی را درک کنند. رهبری نیاز به آموزش در مورد چگونگی رهبری سازمان در هنگام بحران دارد. تیم‌های فنی به روش‌های بازیابی و تدارکات احتیاج دارند. متخصصان امنیت به آموزش نحوه محافظت از دارایی‌ها در دوران بازیابی نیاز دارند.

در اکثر سازمانها آموزش مداوم در کسب و کار و آگاهی از بهبود فاجعه به عنوان بخشی از آموزش‌های اولیه در هنگام استخدام به پرسنل داده می‌شود. سازمانها همچنین باید بطور دوره‌ای پرسنل را به روز کنند تا مطمئن شوند که بهبود فاجعه را فراموش نکرده اند.

طرح‌های تست بازیابی Testing Recovery Plans

پس از مستند سازی کامل BCP، یک سازمان باید اقدامات لازم را برای اطمینان از حفظ و به روز ماندن این طرح انجام دهد. حداقل یک سازمان باید سالانه BCP و DRP را ارزیابی و اصلاح کند. این ارزیابی معمولاً شامل نوعی تست است تا از صحت و دقت طرح‌ها اطمینان حاصل شود. تست مهم است زیرا هر طرحی قابل اجرا نیست مگر اینکه تست آن انجام شده باشد. از طریق تست، نادرست‌ها، نواقص و حذفیات تشخیص داده می‌شود.

تست BCP و DRP پرسنل را برای انجام وظایف خود آماده می‌کند. همچنین تضمین می‌کند که نسخه پشتیبان جایگزین سایت می‌تواند در صورت نیاز فعالیت کند. وقتی تست انجام شد، در صورت عدم یافتن مشکل در مورد این طرح، احتمالاً تست دارای نقص می‌باشد.

انواع تست‌هایی که معمولاً برای ارزیابی BCP و DRP استفاده می‌شود شامل موارد زیر است:

✓ تست خواندن Read-through test

✓ تست چک لیست Checklist test

- ✓ اجرای جدول بالا Table-top exercise
- ✓ تست پیاده روی ساختاری Structured walk-through test
- ✓ تست شبیه سازی Simulation test
- ✓ تست موازی Parallel test
- ✓ تست وقفه کامل Full-interruption test
- ✓ مانور عملکرد Functional drill
- ✓ مانور تخلیه Evacuation drill

تست خواندن Read-Through Test

تست خواندن از طریق تیم‌هایی که درگیر بخشی از هر طرح بازیابی هستند، انجام می‌شود. این تیم‌ها طرحی را که تدوین شده است، می‌خوانند و تلاش می‌کنند هرگونه عدم صحت و نارضایتی در طرح را شناسایی کنند.

تست چک لیست Checklist Test

تست چک لیست زمانی اتفاق می‌افتد که مدیران هر بخش یا منطقه فعالیت، BCP را بررسی کنند. این مدیران هرگونه تغییر در طرح را یادداشت می‌کنند. سپس کمیته BCP از تمام یادداشتهای مدیریتی برای ایجاد تغییر در BCP استفاده می‌کنند.

اجرای جدول سطح بالا Table-Top Exercise

یک اجرای جدول سطح بالا مقرون به صرفه ترین و کارآمدترین روش برای شناسایی مناطق همپوشانی در طرح قبل از انجام تست سطح بالاتر است. یک اجرای جدول سطح بالا یک جلسه طوفان مغزی غیررسمی است که مشارکت رهبران مشاغل و سایر کارمندان کلیدی را ترغیب می‌کند. در یک اجرای سطح بالا، شرکت کنندگان با سناریوی فاجعه خاصی که بر آنها تمرکز می‌کنند موافقت می‌کنند.

تست بررسی ساخت یافته Structured Walk-Through Test

تست بررسی ساخت یافته شامل نمایندگان هر بخش یا منطقه عملیاتی است که دقت صحت و سقم BCP را بررسی می‌کنند. این نوع تست مهمترین آزمایشی می‌باشد که انجام می‌شود قبل از اینکه فاجعه زنده رخ دهد.

تست شبیه سازی Simulation Test

در یک تست شبیه سازی، عملیات و پرسنل پشتیبانی، DRP را در یک سناریوی نقش آفرینی اجرا می‌کنند. این تست مراحل و تهدیدهای حذف شده را مشخص می‌کند.

تست موازی Parallel Test

تست موازی شامل آوردن سایت بهبود به وضعیت آمادگی عملیات اما حفظ عملیات در سایت اصلی می‌باشد.

تست وقفه کامل Full-Interruption Test

تست وقفه کامل شامل خاموش کردن تأسیسات اولیه و رساندن تأسیسات جایگزین تا بهره‌برداری کامل است. این یک سوئیچ سخت است که تمام پردازش‌ها در تأسیسات اولیه انجام می‌شود تا زمانی که "سوئیچ" زده شود. این نوع تست به هماهنگی کامل بین طرفین احتیاج دارد و شامل اطلاع رسانی کاربران قبل از تست برنامه ریزی شده است. یک سازمان باید فقط در صورتی که تمام آزمونهای دیگر اجرا شده و موفق باشند، این نوع تست را انجام دهد.

مانور عملکرد Functional Drill

یک عملکرد واحد یا دپارتمانی را تست می‌کند تا مشاهده کند که DRP عملکرد کامل دارد یا خیر. این نوع مانور نیاز به مشارکت پرسنلی دارد که عملکرد را انجام می‌دهند.

مانور تخلیه Evacuation drill

در یک مانور تخلیه، پرسنل دستورالعمل تخلیه یا پناهگاه در محل را برای یک نوع فاجعه خاص دنبال می کنند. در این نوع مانور، پرسنل باید منطقه را برای گزارش در هنگام وقوع تخلیه درک کرده و در آن زمان کلیه پرسنل باید حساب شوند.

اجرا و برنامه ریزی ادامه کسب و کار Business Continuity Planning and Exercises

بعد از اتمام تست، تمام نتایج تست باید مستند سازی شوند و طرح ها باید اصلاح شوند تا نتایج را منعکس کنند. لیست فعالیت های موفق و ناموفق از تست ها برای حفظ مدیریت هنگام استفاده از BCP مفید ترین خواهد بود. کلیه اطلاعات منسوخ در طرح ها باید حذف شوند و هرگونه اطلاعات جدیدی باید اضافه شود. علاوه بر این، اصلاح اطلاعات فعلی بر اساس آیین نامه ها، قوانین یا پروتکل های جدید ممکن است ضروری باشد.

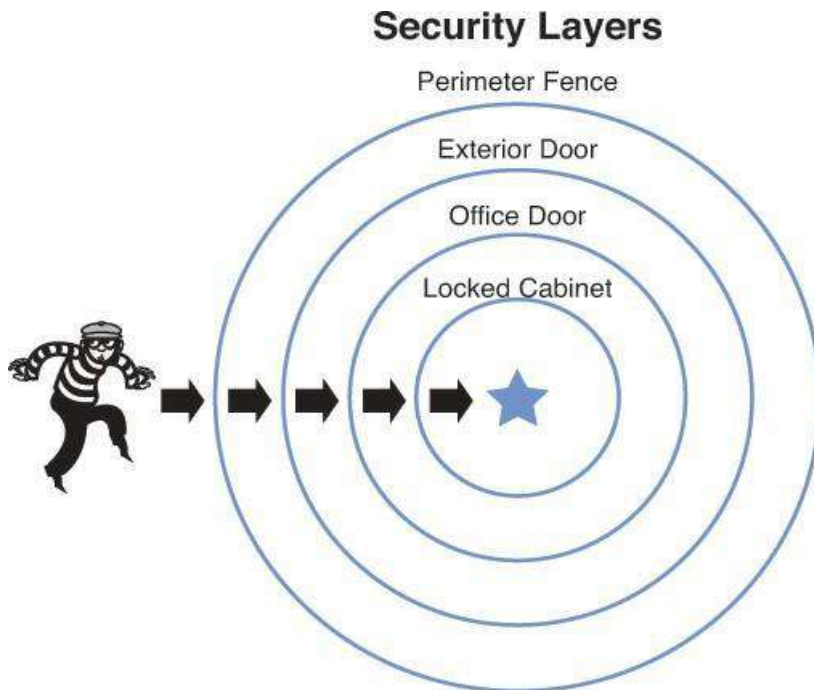
کنترل نسخه از طرح ها باید تضمین شود که سازمان همیشه از جدیدترین نسخه استفاده می کند. علاوه بر این، BCP باید در چندین مکان ذخیره شود تا در صورت نابودی مکانی در اثر فاجعه، در دسترس باشد. چند پرسنل باید آخرین نسخه از طرح ها را داشته باشند تا اطمینان حاصل شود که در صورت عدم دسترسی پرسنل اصلی اگر نیاز داشته باشند، می توانند برنامه ها را بازیابی کنند.

امنیت فیزیکی Physical Security

امنیت فیزیکی شامل استفاده از کنترل های امنیتی مناسب برای محافظت از تمام دارایی ها در برابر دسترسی فیزیکی است. امنیت محیط شامل اجرای کنترل های امنیتی محیطی مناسب، از جمله دروازه ها Gate و نرده ها Fence، تشخیص نفوذ محیطی، روشنایی، نیروی گشت زنی و کنترل دسترسی برای جلوگیری از دسترسی به محیط پیرامون یک مرکز است. امنیت و امنیت داخلی شامل پیاده سازی ساختمان های مناسب و کنترل های امنیتی داخلی است.

امنیت محیط Perimeter Security

هنگام در نظر گرفتن امنیت محیطی یک تأسیسات، استفاده از یک رویکرد جامع، که گاهی با عنوان رویکرد دایره متحدالمرکز Concentric circle شناخته می‌شود، مفید است (شکل ۷-۱۲ را مشاهده شود). این رویکرد به ایجاد لایه‌هایی از موانع فیزیکی در اطلاعات وابسته است.



شکل ۷-۱۲: رویکرد دایره متحدالمرکز

در این بخش، به طور مفصل به اجرای این مفهوم خواهیم پرداخت.

دروازه و نرده Gates and Fences

بیرونی‌ترین حلقه در رویکرد دایره متحدالمرکز دروازه‌ها و نرده‌هایی است که تأسیسات را احاطه کرده‌اند. در درون آن حلقه‌های داخلی از موانع فیزیکی وجود دارد که هرکدام از آنها دغدغه‌های خاص خود را دارند. در این بخش ملاحظات مربوط به موانع (بولارد)، نرده‌ها، دروازه‌ها و دیوارها مورد بررسی قرار می‌گیرد.

موانع (بولاردها) Barriers (Bollards)

موانع موسوم به بولاردها در اطراف حاشیه ساختمانهای جدید اداری و دولتی کاملاً رایج شده است. این پستهای عمودی کوتاه که در راه ورودی ساختمان و پیاده روهای خط کشی شده وجود دارد که به محافظت از وسایل نقلیه که احتمال دارد عمداً یا ناخواسته با ساختمان تصادف کند یا وارد ساختمان شوند یا به پیاده رو آسیب وارد کند، کمک می‌کند. بولاردها را می‌توان از انواع مختلفی از مواد ساخت. مواردی که در شکل ۷-۱۳ نشان داده شده است از استیل ضدزنگ می‌باشد.



شکل ۷-۱۳

نرده‌ها (حصارها) Fences

نرده اولین خط دفاعی در الگوی دایره متحدالمرکز هستند. هنگام انتخاب نوع نرده برای نصب، قصد فردی را که می‌خواهید دلسرد کنید، در نظر بگیرید. با توجه به ارتفاع نرده‌ها از دستورالعمل‌های زیر استفاده کنید:

- نرده‌های ۳ تا ۴ فوت تنها مانع مهاجمان سطحی می‌شود.
- نرده‌های ۶ تا ۷ فوت بسیار بلند هستند و به راحتی نمی‌توان بالا رفت.
- نرده‌ها ۸ فوت و بلندتر، مانع مزاحمان مصمم تر به ویژه هنگامی که همراه با سیم خاردار هستند می‌شود.

حصار جغرافیای منطقه جغرافیایی است که در آن دستگاه‌ها با استفاده از نوعی ارتباط فرکانس رادیویی مدیریت می‌شوند. به عنوان مثال، یک حصار جغرافیایی می‌تواند در شعاع اطراف یک فروشگاه یا نقطه محل یا در یک مجموعه از مرزهای از پیش تعریف شده، مانند اطراف یک منطقه مدرسه قرار گیرد. از آن برای ردیابی کاربران یا دستگاه‌های ورودی یا خروج از منطقه جغرافیایی استفاده می‌شود. هشدارها می‌توانند پیکربندی شوند تا به کاربر دستگاه و اپراتور حصار جغرافیایی، مکان دستگاه را پیام دهند.

دروازه Gates

در صورت عدم استفاده صحیح از دروازه می‌تواند نقاط ضعفی در یک حصار باشد. دروازه به روش زیر رتبه بندی می‌شود. هر مرحله در کلاس نیاز به سطح حفاظت بیشتری دارد:

- ✓ کلاس ۱: کاربرد مسکونی Residential use
- ✓ کلاس ۲: کاربرد تجاری Commercial usage
- ✓ کلاس ۳: کاربرد صنعتی Industrial usage
- ✓ کلاس ۴: منطقه محدود Restricted area

دیوارها Walls

در بعضی موارد ممکن است دیوارها را در اطراف یک تاسیسات ایجاد کنند. در این صورت، و هنگامی که امنیت محیط بسیار مهم است، سیستم‌های تشخیص نفوذ می‌توانند مستقر شوند تا به هرگونه تخریب دیوارها هشدار دهند. این نوع سیستم‌ها در بخش بعدی با جزئیات بیشتری پوشش داده شده‌اند.

تشخیص نفوذ محیطی Perimeter Intrusion Detection

علیرغم اینکه از نرده‌ها یا دیوارها استفاده می‌کنید یا حتی اگر تصمیم به استقرار هیچ یک از این موانع ندارید، می‌توانید با استفاده از یکی از زیر سیستم‌های تشخیص نفوذ محیطی میزان قرار

گرفتن در معرض نفوذ را به میزان قابل توجهی کاهش دهید. تمام سیستمهای شرح داده شده بعدی روشهای تشخیص نفوذ فیزیکی در نظر گرفته می شوند.

سنسورهای مادون قرمز Infrared Sensors

سیستمهای مادون قرمز منفعل Passive infrared systems با شناسایی تغییرات در امواج گرما در یک منطقه کار می کنند. از آنجا که وجود یک متجاوز باعث افزایش دمای ذرات هوای اطراف می شود، این سیستم در صورت بروز هشدار یا صداها، هشدار می دهد.

سیستمهای الکترومکانیکی Electromechanical Systems

سیستمهای الکترومکانیکی با تشخیص وقفه در یک مدار الکتریکی کار می کنند. به عنوان مثال، مدار ممکن است از یک پنجره یا درب عبور کند و هنگامی که پنجره یا درب باز می شود، مدار شکسته می شود، زنگ خطر را بر طبق آن تنظیم شده است. نمونه دیگر ممکن است یک پد فشاری باشد که در زیر فرش برای شناسایی حضور افراد قرار گرفته است.

سیستمهای فوتوالکتریک Photoelectric Systems

سیستمهای فوتومتریک یا فوتوالکتریک با تشخیص تغییرات در نور عمل می کنند و در مناطق بدون پنجره استفاده می شوند. آنها پرتوی از نور را به سراسر منطقه می فرستند و در صورت قطع شدن پرتو (به عنوان مثال توسط شخص)، زنگ خطر به صدا در می آید.

سیستمهای تشخیص صوتی Acoustical Detection Systems

سیستمهای صوتی از میکروفنهای استراتژیک برای تشخیص هر صدای ایجاد شده در هنگام ورود اجباری استفاده می کنند. این سیستمها فقط در مناطقی کار می کنند که صدای زیادی در اطراف آن وجود ندارد. آنها به طور معمول بسیار حساس هستند و این امر باعث می شود بسیاری از هشدارهای دروغین در یک منطقه با صدای بلند مانند درب کنار خیابان شلوغ ایجاد شوند.

ردیاب حرکت موج Wave Motion Detector

این دستگاهها الگوی موجی را در منطقه ایجاد می کنند و هر حرکتی را که باعث اختلال در الگوی موج شود، تشخیص می دهند. وقتی الگو مختل می شود، زنگ هشدار به صدا در می آید.

ظرفیت توان آشکارساز Capacitance Detector

این دستگاهها یک میدان مغناطیسی را منتشر می کنند و میدان را نظارت می کنند. در صورت خراب شدن منطقه، که هنگام ورود شخص به آن منطقه رخ می دهد، زنگ خطر به صدا در می آید.

دوربین مدار بسته CCTV

سیستم دوربین مدار بسته Closed-Circuit Television (CCTV) از مجموعه دوربینهایی استفاده می کند که می توانند در زمان واقعی کنترل شوند یا می توانند روزهایی از فعالیت را ثبت کنند که در زمان های بعدی مورد نیاز، مشاهده شوند. در تاسیسات امنیتی سطح بالا، معمولاً مورد بررسی قرار می گیرند. یکی از مهمترین مزایای استفاده از دوربین مدار بسته این است که باعث افزایش قابلیت های دید نگهبان می شود. نگهبانان می توانند مناطق بزرگتر را به طور هم زمان از یک مکان مرکزی کنترل کنند. دوربین مدار بسته دسته ای از نظارت فیزیکی می باشد، نه نظارت بر رایانه / شبکه.

انواع دوربین ها شامل دوربین های در فضای باز، دوربین های مادون قرمز، دوربین های موقعیت ثابت، دوربین های Pan/Tilt، دوربین های گنبدی Dome Cameras و دوربین های پروتکل اینترنت یا IP است. هنگام اجرای دوربین ها، سازمان ها باید لنز مناسب، وضوح تصویر، فریم در ثانیه Frames per second (FPS) و فشردگی سازی را انتخاب کنند. علاوه بر این، تجزیه و تحلیل الزامات روشنایی دوربین های مختلف باید مد نظر قرار گیرد. یک سیستم دوربین مدار بسته باید با توجه به میزان نوری که در مکان قرار دارد، کار کند. بعلاوه، یک سازمان باید انواع مختلف نمایشگرهای مانیتور، از جمله نمایشگرهای تک تصویر، انشعاب صفحه نمایش و نمایشگرهای بزرگ را درک کند.

روشنایی Lighting

یکی از بهترین راهها برای جلوگیری از جرم، تابش نور در مناطق مهم است. در این بخش برخی از انواع روشنایی و برخی از سیستم های روشنایی که اثبات شده اثربخش هستند را بررسی می کنیم. نورپردازی یک کنترل فیزیکی برای امنیت فیزیکی محسوب می شود.

انواع سیستم ها Types of Systems

متخصص امنیت باید با چندین نوع سیستم روشنایی آشنا باشد:

- روشنایی مداوم Continuous lighting: مجموعه ای از چراغ ها که نور کافی را در یک منطقه ایجاد می کنند.
- روشنایی آماده به کار Standby lighting: نوعی سیستمی است که فقط در زمان های مشخص یا با برنامه زمانبندی شده روشن می شود.
- روشنایی متحرک Movable lighting: نورپردازی که در صورت لزوم قابل جابجایی مجدد است.
- روشنایی اضطراری Emergency lighting: سیستم های روشنایی با منبع تغذیه خود که در هنگام قطع انرژی، از آنها استفاده می کنند.

انواع روشنایی Types of Lighting

هنگام انتخاب منبع روشنایی یا نوع چراغ، تعدادی گزینه وجود دارد. موارد زیر رایج ترین گزینه ها است:

- فلورسنت Fluorescent: لامپ تخلیه گاز بخار جیوه با فشار بسیار کم که از فلورسانس برای تولید نور مرئی استفاده می کند.
- بخار جیوه Mercury vapor: لامپ تخلیه گاز که قوس الکتریکی از طریق جیوه تبخیر شده و برای تولید نور استفاده می شود.
- بخار سدیم Sodium vapor : لامپ تخلیه گاز که از سدیم در حالت برانگیخته برای تولید نور استفاده می کند.
- لامپهای کوارتز Quartz lamps: لامپ متشکل از یک منبع نور ماوراء بنفش، مانند بخار جیوه، در یک لامپ سیلیس ذوب شده که نور ماوراء بنفش را با جذب کم منتقل می کند.

علیرغم منبع نور، روشنایی را با درخشش نور درجه بندی می کند. هنگام قرارگیری چراغ ها، باید این امتیاز را در نظر بگیرید. به عنوان مثال، اگر یک لامپ نوری کنترل شده نصب شده بر روی قطب ۵ متری بتواند مساحتی به قطر ۳۰ متر را روشن کند، برای اهداف روشنایی امنیتی، فاصله

بین وسایل جانبی باید ۳۰ فوت باشد. علاوه بر این، باید نور محیط بیرونی گسترده‌ای از ورودی‌ها یا مناطق پارکینگ وجود داشته باشد تا متجاوزین سطحی را دلسرد کند.

نیروی گشت Patrol Force

حضور یک نگهبان در حال گشت زنی در مرکز باعث تقویت عالی برای سایر سیستم‌های تشخیص می‌شود. این گزینه بیشترین انعطاف پذیری را در واکنش به هر اتفاق می‌دهد. یکی از مهمترین موفقیت‌ها، آموزش کافی نگهبانان است، به همین دلیل آنها برای هرگونه وقایع آماده هستند. برای هر اتفاق احتمالی باید پاسخی آماده ارائه شود. یکی از مهمترین مزایای این رویکرد این است که نگهبانان می‌توانند براساس شرایطی که سیستم‌های خودکار قادر به انجام آن نیستند از قضاوت تبعیض آمیز استفاده کنند.

نیروی گشت می‌تواند در سازمان استخدام شود، آموزش دیده و کنترل شود و یا سازمان می‌تواند با یک شرکت امنیتی قرارداد ببندد. یک سازمان می‌تواند آموزش و عملکرد یک نیروی گشت داخلی را کنترل کند. با این حال، برخی از سازمان‌ها برای اطمینان از بی طرفی، نیروی گشت زنی را از بیرون تأمین می‌کنند.

کنترل دسترسی Access Control

در هنگام دسترسی فیزیکی به مرکز، تعدادی از دستورالعمل‌ها در رابطه با نگهداری سوابق باید رعایت شود. هر تلاش موفق و ناموفق برای ورود به تأسیسات، از جمله مواردی که پذیرش داده شد، باید به شرح زیر ثبت شود:

- تاریخ و زمان
- نقطه ورود خاص
- شناسه کاربری که در حین تلاش به کار رفته است

ساختمان و امنیت داخلی Building and Internal Security

ساختمان و امنیت داخلی شامل قفل‌ها، کلیدها و الزامات اسکورت / کنترل بازدید کننده است که سازمان‌ها باید در نظر بگیرند.

حریم شخصی و ایمنی پرسنل Personnel Privacy and Safety

منابع انسانی مهمترین دارایی است که سازمان در اختیار دارد. شاید به خاطر داشته باشید که در صورت بروز آتش سوزی، اولین عملی که همیشه انجام می شود تخلیه کلیه پرسنل است. ایمنی آنها قبل از همه ملاحظات دیگر لازم است. اگرچه تجهیزات و در بیشتر موارد داده ها قابل بازیابی هستند، اما از منابع انسانی نه پشتیبانی تهیه می شود و نه جایگزینی تهیه می شود. یک طرح اضطراری اضطراب (Occupant Emergency Plan (OEP) روشهای هماهنگی را برای به حداقل رساندن تلفات یا آسیب دیدگی و محافظت از خسارتهای دارایی در پاسخ به یک تهدید فیزیکی فراهم می کند. در هر نوع فاجعه، ایمنی پرسنل اولین دغدغه می باشد. سازمان وظیفه حفاظت از حریم خصوصی اطلاعات هر فرد را دارد، به خصوص که مربوط به پرسنل و سوابق پزشکی باشد. اگرچه این انتظار از حریم خصوصی الزامی نیست و معمولاً به فعالیتهای آنها در شبکه گسترش نمی یابد، هر دو قوانین فدرال و ایالتی سازمانها مسئول انتشار این نوع اطلاعات و تخلفات هستند، اگر شرکت مسئولیت پذیر باشد محکوم به جریمه های سنگین و دعاوی احتمالی می شوند. سازمانها باید سیاست هایی را برای مقابله با فشار کار، مسافرت و نظارت بر کارمندان تدوین کنند.

فشار Duress

فشار کارکنان هنگامی اتفاق می افتد که یک کارمند مجبور به انجام عملی توسط شخصی دیگر شود. این یک دغدغه خاص برای مدیریت سطح بالا یا کارمندان دارای مجوزهای امنیتی بالا است زیرا آنها به دارایی های اضافی دسترسی دارند. سازمانها باید به کارمندان آموزش دهند که در شرایط اضطراب چه باید انجام بدهند. برای هر کد امنیتی، پین یا گذرواژه ای که استفاده می شود، اجرای یک کد فشار ثانویه یک سیاست مناسب است. سپس اگر پرسنل تحت فشار هستند، برای دسترسی به سیستم ها، تاسیسات یا دارایی های دیگر از کد فشار استفاده کنند. به پرسنل امنیتی هشدار داده می شود که از کد فشار استفاده شده است. سازمانها باید به پرسنل تأکید کنند که حمایت از زندگی نسبت به ملاحظات دیگر ارجحیت دارد.

مسافرت Travel

کارمندان غالباً برای مقاصد کسب و کار مسافرت می‌کنند و هنگام مسافرت دارایی‌های سازمان را دریافت می‌کنند. برای کارکنان باید تضمین شود که دارایی‌های ثبت شده توسط سازمان را در طی دوره سفر ایمن نگه دارند و در ملاء عام، باید از دارایی‌های سازمان بسیار مراقب کنند. همچنین باید دستورالعمل گزارش صحیح در مورد دارایی‌های از دست رفته یا دزدیده شده را دریافت کنند.

نظارت Monitoring

خصوصاً برای کارکنان دارای سطح مجوز بالا، اقدامات کارمندان در دارایی‌های سازمانی ممکن است لازم باشد، کنترل شود. با این حال، مهم است که پرسنل درک کنند که تحت نظارت هستند. سازمان‌هایی که بر کارکنان نظارت می‌کنند، باید عدم انتظار از اظهارنامه حریم خصوصی صادر کنند. به کارمندان باید در هنگام استخدام یک نسخه از این بیانیه داده شود و باید رسید این بیانیه را امضا کنند. علاوه بر این، یادآوری‌های دوره‌ای از این خط مشی باید در مکان‌های برجسته، از جمله در تابلوهای اعلانات، صفحه‌های ورود به سیستم و وب سایت‌ها قرار گیرد. برای اینکه هر نظارت مؤثر باشد، سازمانها باید رفتارهای اولیه را برای کاربران ثبت کنند.

فصل ۸

امنیت توسعه نرم افزار
(Software Development Security)

این فصل موضوعات زیر را در بر می گیرد:

❖ **مفاهیم توسعه نرم افزار Software Development Concepts:** در مورد معماری

نرم افزار و زبانهایی که برای اجرای آنها استفاده می شود، بحث می کند.

❖ **امنیت در چرخه عمر توسعه سیستم و نرم افزار Security in the System and**

Software Development Life Cycle: مفاهیم مورد بحث شامل مراحل چرخه عمر

توسعه سیستم، چرخه عمر توسعه نرم افزار، روش های توسعه نرم افزار و مدل های بلوغ و تیم محصول یکپارچه می باشد.

❖ **کنترل امنیتی در توسعه Security Controls in Development:** مفاهیم مورد

بحث شامل بهترین شیوه های توسعه نرم افزار، امنیت محیط نرم افزار، مسائل مربوط به کد منبع، ابزار تجزیه و تحلیل کد منبع، امنیت مخزن کد، امنیت واسط برنامه نویسی اپلیکیشن، تهدیدات نرم افزاری و مکانیسم های محافظت از نرم افزار است.

❖ **ارزیابی اثربخشی امنیت نرم افزار Assess Software Security Effectiveness:**

مفاهیم مورد بحث شامل ممیزی و ورود به سیستم، تحلیل ریسک و کاهش، و رگرسیون و آزمون پذیرش است.

❖ **تأثیر امنیتی نرم افزارهای اکتسابی Security Impact of Acquired Software:**

در مورد چرخه عمر نرم افزار اکتسابی و تأثیر امنیتی نرم افزار خریداری شده بحث می کند.

امنیت توسعه نرم افزار تمام مسائل مربوط به امنیت را تحت پوشش قرار می دهد و کنترل هایی را که متخصصان امنیت هنگام برخورد با نرم افزارهای تجاری یا داخلی تولید می کنند، باید در بر داشته باشند و شامل درک چرخه عمر توسعه نرم افزار و امکان ارزیابی اثربخشی امنیت نرم افزار و تأثیر نرم افزار است.

این نرم افزار در میان تمام عملکردهای سیستم های رایانه ای قرار دارد. انواع مختلف نرم افزار، از جمله سیستم عامل ها، برنامه ها و اپلیکیشن ها، با هم کار می کنند تا دستورالعمل ها را از یک انسان به سخت افزار ارائه دهند. تمام این دستورالعمل ها با هدف عملی کردن برخی فعالیت ها ایجاد می شوند.

هنگام نگارش و توسعه نرم افزار، می توان بر کارایی و سهولت استفاده یا امنیت آن تمرکز داشت. در بسیاری موارد، این دو هدف ممکن است درمیان قصد و نیت ها صورت گیرد. توجه ناکافی به

امنیت یک قطعه از نرم افزار منجر به ایجاد نرم افزار می شود که می تواند مسائل امنیتی را هم به برنامه و هم برای سیستمهایی که در آن اجرا شده است، ایجاد کند. علاوه بر این، برخی از انواع نرم افزارها به طور عمد برای ایجاد منفذهای امنیتی در یک شبکه یا سیستم ایجاد شده اند. در این فصل به بحث در مورد روش توسعه نرم افزار، بهترین روشها برای توسعه امن و انواع بدافزارها و روشهای کاهش اثرات مخرب می پردازد.

مفاهیم توسعه نرم افزار Software Development Concepts

نرم افزار شامل دستورالعمل های کتبی است که به انسان امکان برقراری ارتباط با سخت افزار رایانه را می دهد. این دستورالعمل ها به زبان های مختلف برنامه نویسی نوشته شده اند. از آنجا که برنامه نویسی در طول سال ها تکامل یافته است، هر زبان پی در پی عملکرد بیشتری را به برنامه نویسان ارائه داده است. زبان های برنامه نویسی را می توان با توجه به نوع دستورالعمل هایی که ایجاد می کنند و همچنین با کدام قسمت از سیستم صحبت می کنند، در دسته هایی طبقه بندی کرد. این بخش دسته اصلی را در بر می گیرد.

زبانهای ماشینی Machine Languages

زبانهای ماشینی دستورالعمل ها را مستقیماً به پردازنده ارائه می دهند. این زبان تنها نوع برنامه نویسی بود که در دهه ۱۹۵۰ انجام شد و از دستورالعمل های اصلی دودویی و بدون کامپایلر یا مفسر استفاده می کرد (برنامه هایی که انواع زبانهای سطح بالا را به شکلی تبدیل می کنند که توسط پردازنده قابل اجرا باشد). این نوع برنامه نویسی هم وقت گیر بود و هم در معرض خطا، بیشتر این برنامه ها به دلیل نیاز به نگه داشتن استحکام طولانی در مدت آنها، بسیار ابتدایی بودند.

زبان اسمبلی و اسمبلرها Assembly Languages and Assemblers

زبانهای اسمبلی یک قدم بالاتر در نظر گرفته می شوند، زبانهای اسمبلی از نمادها یا یادآورها (ممونیک) Mnemonics برای نشان دادن بخش هایی از کد باینری (دودویی) پیچیده استفاده می کنند.

در نتیجه، این زبانها برای تبدیل کد به سطح دستگاه از اسمبلر استفاده می کنند. اگرچه این کد را تا حد زیادی ساده و کوتاه می کند، اما هنوز نیاز به دانش گسترده ای در مورد معماری رایانه دارد. این بدان معنی است که هر کدی که به این زبانها نوشته شده باشد از نظر سخت افزاری

خاص خواهد بود. اگرچه نوشتن زبان اسمبلی نوشتن ساده تر از زبان ماشین است، اما ایجاد به طور کامل زبان های سطح بالا، آسان نیست.

زبان های سطح بالا، کامپایلرها و مفسرها High-Level Languages, Compilers, and Interpreters

در دهه ۱۹۶۰، سطح سوم زبان به نام زبانهای سطح بالا پدید آمد. این دستورالعملها از جملات انتزاعی و خلاصه استفاده می کنند برای مثال IF-THEN-ELSE و مستقل از پردازنده هستند. کار با آنها راحت تر است، و ترکیب (Syntax) آنها بیشتر به زبان انسان شباهت دارد. در این کد از اسمبلرها یا کامپایلرها استفاده شده است تا دستورالعملها را به کد دستگاه تبدیل کند. نتیجه نهایی، کاهش کدنویسان مورد نیاز برای یک پروژه خاص است.

نسل چهارم از زبانها به نام زبان های سطح بسیار بالا روی الگوریتم های انتزاعی متمرکز شده اند که برخی از پیچیدگی ها را از برنامه نویس پنهان می کنند، و این برنامه نویس را آزاد می کند تا به جای جزئیاتی که در پشت پرده هست، روی مشکلات دنیای واقعی که سعی در حل آنها دارند، متمرکز شوند.

سرانجام، در دهه ۱۹۹۰، نسل پنجم از زبانها شروع به ظهور کردند که به آنها زبان های طبیعی گفته می شود. هدف استفاده از این زبانها، ایجاد نرم افزاری است که می تواند به تنهایی مشکلات را برطرف کرده و نیازی به یک برنامه نویس برای ایجاد کد برای مقابله با مشکل ندارد. اگرچه این هدف کاملاً تحقق نیافته است، استفاده از پردازش دانش بنیان و هوش مصنوعی ارزش دنبال کردن را دارد.

در رابطه با امنیت بین کد کامپایل شده و کد تفسیر شده، تفاوت قابل توجهی وجود دارد. از آنجا که کد کامپایل شده قبلاً به زبان دودویی ترجمه شده است، تشخیص کدهای مخرب در داخل یک برنامه بسیار دشوار است. از طرف دیگر کد تفسیر شده از یک مفسر زبان استفاده می کند که یک قطعه نرم افزاری است که به کاربر نهایی اجازه می دهد تا یک برنامه را به زبانی قابل خواندن توسط انسان بنویسد و این برنامه را مستقیماً توسط مفسر اجرا کند. در این حالت، کشف کد مخرب تا حدودی راحت تر است زیرا کد توسط انسان قابل خواندن است.

برنامه نویسی شی گرا Object-Oriented Programming

در توسعه نرم افزار کلاسیک، داده‌ها به یک برنامه وارد می‌شوند، برنامه از ابتدا تا انتها داده‌ها را مدیریت می‌کند، و یک نتیجه بازگردانده می‌شود. برنامه نویسی شی گرا یا OOP عملکرد مشابهی را ارائه می‌دهد اما از طریق تکنیک‌های مختلف، کارآیی بیشتری دارد. در OOP، اشیاء در یک سلسله مراتب از کلاسها با خصوصیات به نام صفاتی Attributes که به هریک ضمیمه هستند، سازماندهی می‌شوند. OOP بر استفاده از اشیاء و روشها به جای انواع یا تغییر شکلها مانند سایر رویکردهای نرم افزاری تأکید دارد.

برنامه نویس کلاس اشیاء را ایجاد می‌کند اما نه همه اشیاء. نرم افزار در این برنامه امکان ایجاد اشیاء را در صورت نیاز از طریق درخواست ایجاد می‌کند. هنگامی که یک درخواست وارد می‌شود، معمولاً از یک شی موجود برای انجام یک شی جدید، تابعی ایجاد می‌شود و کد لازم ساخته می‌شود. فرقی نمی‌کند اشیاء با یک زبان برنامه نویسی متفاوت نوشته شوند زمانی که اشیاء توانایی برقراری ارتباط با یکدیگر را داشته باشند، فرایندی که معمولاً از طریق واسط برنامه نویسی برنامه یا API امکان پذیر است.

علاوه بر این، به دلیل اینکه اشیاء در کلاسهای سلسله مراتبی سازماندهی می‌شوند، روشهای شی object (عملکردها یا رویه‌ها) از طریق فرایندی به نام وراثت می‌توانند از کلاس به زیر کلاس منتقل شوند. اشیاء حاوی مقادیر کپسوله شده هستند. اشیاء با پیامهای ارسال شده، با API یک شیء دیگر ارتباط برقرار می‌کنند. ممکن است اشیاء مختلف به همان پیام واکنش نشان دهند، که رفتار شی Object's behavior نامیده می‌شود. کدی که تعریف می‌کند چگونه یک شیء با توجه به یک پیام رفتار خواهد کرد، روش Method آن نامیده می‌شود.

برخی از قسمت‌های یک شی ممکن است خصوصی باشد، به این معنی که داده‌های داخلی و عملکرد آن توسط اشیاء دیگر قابل مشاهده نیست. این حریم خصوصی از طریق فرایند کپسوله سازی Encapsulation فراهم می‌شود و گاهی به آن مخفی سازی داده Data Hiding نیز می‌گویند. انتزاع Abstraction، توانایی تضعیف این جزئیات داخلی غیر ضروری می‌باشد. سایر اشیاء، موضوعها و برنامه‌ها می‌توانند از ویژگی‌های اشیاء از طریق واسطهای استاندارد و بدون دغدغه در مورد جزئیات عملکرد استفاده کنند.

OOP از انواع داده با دامنه تعریف شده استفاده می‌کند. برنامه نویسان باید کلیه اشیاء داده و روابط آنها را از طریق فرایندی به نام مدل سازی داده شناسایی کنند. سپس شی به یک کلاس

شی تعمیم داده شده و به عنوان بخشی از یک دنباله منطقی تعریف می شود، همچنین به آن روشی گفته می شود که برای دستکاری شی استفاده می شود. می توان از یک شیء در برنامه های مختلف استفاده کرد.

نمونه هایی از زبان های OOP عبارتند از ++C، Simula 67، Smalltalk است. تعدادی از مزایای OOP عبارتند از:

- ماژولار بودن (بر اساس بخش های مجزا) در طراحی از طریق اشیاء خودمختار.
- تعریف اجزای داخلی بدون اینکه روی سایر قسمت های سیستم تأثیر بگذارد.
- قابلیت استفاده مجدد از مولفه ها.
- نقشه های بیشتری را برای نیازهای کسب و کار تهیه می کند.

چند ریختی Polymorphism

در یک سیستم شی گرا، چند ریختی اشیاء بسیاری از کلاسهای مختلف را نشان می دهد که توسط برخی از ابرکلاسهای رایج مرتبط هستند. بنابراین، هر شیئی که با این نام مشخص شده باشد می تواند به روشهای متفاوتی به مجموعه عملکردهای مختلف پاسخ دهد. در چند ریختی توانایی اشیاء مختلف با نام مشترک برای واکنش به همان پیام یا ورودی، خروجی متفاوت است. به عنوان مثال، ممکن است سه شیء ورودی Toyota Corolla را دریافت کند. خروجی یک شیء ممکن است "کم فشار" باشد، ممکن است دیگری "استفاده از سوخت معمولی" باشد، و دیگری ممکن است "۱۸۰۰۰ هزینه" داشته باشد. در بعضی موارد این اختلافات ناشی از این واقعیت است، که اشیاء از کلاسهای والدین خود ویژگیهای مختلفی به ارث برده اند.

چند منظوره Polyinstantiation

چند منظوره مانع از دستیابی به اشیاء سطح پایین از سطح امنیتی بالاتر می شود. اشیاء بسته به داده هایی که در آن قرار دارند ممکن است متفاوت عمل کنند. به همین دلیل، تعیین اینکه آیا ویژگیهای امنیتی ارثی معتبر هستند، دشوار است. چند منظوره از حملات استنتاج پایگاه داده Inference database جلوگیری می کند.

کپسوله سازی Encapsulation

کپسوله سازی با جلوگیری از دسترسی مستقیم به داده‌های موجود در شی، از اشیاء محافظت می‌کند و تضمین می‌کند که از داده‌های خصوصی محافظت می‌شود. با این حال، کپسوله سازی استفاده از سیاستهای امنیتی مناسب در مورد یک شی را دشوار می‌کند زیرا تعیین اینکه چه چیزی در آن موجود است، دشوار است.

انسجام Cohesion

انسجام، اصطلاحی است که برای توصیف چند وظیفه مختلف یک ماژول می‌تواند انجام شود. اگر به تعداد کمی عملکرد یا یک عملکرد واحد محدود شود، گفته می‌شود که از انسجام بالایی برخوردار است. انسجام بالا در این امر از این جهت مناسب است که می‌توان بدون تأثیرگذاری بر ماژول‌های دیگر، مدل را تغییر داد. همچنین استفاده مجدد از ماژول را آسان تر می‌کند. بالاترین انسجام با محدود کردن دامنه عملکرد یک ماژول ارائه می‌شود.

اتصال Coupling

اتصال بیان می‌کند که چقدر تعامل یک ماژول با ماژول دیگر برای انجام کار خود نیاز دارد. اتصال پایین یا سست نشان می‌دهد که یک ماژول به ماژول‌های دیگر احتیاج ندارد، در حالی که اتصال بالا برعکس آن می‌باشد. اگر ماژول A قبل از شروع کار، باید از نتیجه پیامهای ارسالی به سه ماژول دیگر منتظر بماند، گفته می‌شود که اتصال بالایی دارد. از جمع بندی این دو بخش آخر، بهترین برنامه نویسی، انسجام بالا و اتصال کم را فراهم می‌کند.

ساختارهای داده Data Structures

ساختار داده به رابطه منطقی بین عناصر داده اشاره دارد. این میزان ارتباط عناصر، روشهای دسترسی و جایگزینهای پردازش و سازماندهی عناصر داده را نشان می‌دهد. این روابط می‌توانند ساده یا پیچیده باشند. از دیگه امنیتی، باید روابط یا روشی که ارتباط مؤلفه‌های مختلف نرم افزاری و فرمت‌های داده‌ای که از آنها استفاده می‌شود، به خوبی درک شده تا آسیب پذیری هایی که توسط این ساختار داده‌ها در معرض افشا قرار دارند درک شود.

توزیع سیستم های شی گرا Distributed Object-Oriented Systems

همانطور که بسیاری از اپلیکیشن ها، در یک چارچوب مشتری / سرور عمل می کنند، راه حل انجام محاسبات (رایانش) توزیع شده Distributed Computing است. این بدان معنی است که مولفه های موجود در سیستم های مختلف باید بتوانند یکدیگر را پیدا کرده و در یک شبکه ارتباط برقرار کنند. به طور معمول، بخش عمده ای از راه حل روی سرور قرار دارد و یک قطعه کوچکتر نیز روی مشتری قرار دارد. این امر نیاز به برخی از معماری ها برای پشتیبانی از این ارتباط فرایند به فرایند دارد. چندین مورد وجود دارد که می توان به اختصار مورد بحث قرار گیرد.

CORBA

معماری کارگزار درخواست مشترک شی Common Object Request Broker Architecture (CORBA) یک استاندارد شی گرا باز است که توسط گروه مدیریت شی Object Management Group (OMG) ساخته شده است. این استاندارد از مؤلفه ای به نام Object Request Broker (ORB) برای پیاده سازی مبادلات بین اشیاء، در یک محیط ناهمگن و توزیع شده استفاده می کند.

ORB تمام ارتباطات بین مؤلفه ها را مدیریت می کند. این درخواست ها را برای خدمات دهی از اپلیکیشن مشتری دریافت می کند، درخواست را به سرور هدایت می کند و سپس پاسخ را به اپلیکیشن مشتری ارجاع می دهد. ORB ارتباطات را بصورت محلی یا از راه دور امکان پذیر می کند. حتی ممکن است بین مؤلفه هایی که به زبان های مختلف نوشته شده اند امکان پذیر باشد زیرا آنها از یک واسط استاندارد برای برقراری ارتباط با ORB استفاده می کنند.

ORB مسئول اجرای سیاست های امنیتی است، که توصیف می کند کاربران و سیستم مجاز به انجام چه کارهایی هستند و چه محدودیتی را انجام می دهد، و این چهار نوع سیاست را ارائه می دهد: کنترل دسترسی، محافظت از داده ها، عدم تحقیق و ممیزی.

DCOM و COM

الگوی مولفه تشکیل دهنده شیء (COM) Component Object Model الگویی برای برقراری ارتباط بین پردازش ها در همان رایانه است، در حالی که همانطور که از نام آن پیداست، الگوی شیء مولفه توزیع شده (DCOM) Distributed Component Object Model الگویی برای

ارتباط بین پردازش‌ها در بخش‌های مختلف شبکه است. DCOM به عنوان واسطه بین فرآیندهای از راه دور کار می‌کند (به نام ارتباطات بین پردازشی [Interprocess communication [IPC]). DCOM همان خدمات ارائه شده توسط ORB را در چارچوب CORBA ارائه می‌دهد. یعنی اتصال داده، خدمات پیام و خدمات تراکنش توزیع شده. همه این عملکردها در یک فن آوری که از همان واسطه کاربری COM استفاده می‌شود یکپارچه شده اند.

OLE

تعبیه و پیوند شی (Object Linking and Embedding (OLE روشی برای به اشتراک گذاری اشیاء بر روی یک رایانه محلی است که از COM به عنوان پایه آن استفاده می‌کند. در حقیقت، OLE گاهی به عنوان جد COM توصیف می‌شود، و اجازه می‌دهد تا اشیاء در اسناد (صفحات گسترده، گرافیک و غیره) تعبیه شوند. اصطلاح پیوند دادن Linking به ارتباط بین یک برنامه با برنامه دیگر اشاره دارد و اصطلاح تعبیه Embedding عبارت است از قرار دادن داده‌ها در یک برنامه خارجی یا سند.

جاوا Java

Enterprise Edition (Java EE), بستر Java یکی دیگر از مدل‌های مؤلفه توزیع شده است که به زبان برنامه نویسی جاوا تکیه دارد و چارچوبی است که برای توسعه نرم افزاری مورد استفاده قرار می‌گیرد که APIها را برای خدمات شبکه فراهم می‌کند و از یک فرایند ارتباطی پردازش مبتنی بر CORBA استفاده می‌کند. هدف آن تهیه روشی استاندارد برای تهیه کد Back-End است که منطق کسب و کار را برای اپلیکیشن‌های سازمانی انجام می‌دهد.

SOA

یک روش جدیدتر برای ارائه یک مدل محاسباتی توزیع شده، معماری خدمات محور Service-Oriented Architecture (SOA) است. این تئوری در مورد ارائه قابلیت‌های ارتباطی مبتنی بر وب عمل می‌کند بدون اینکه هر اپلیکیشن نیاز به کدنویسی اضافی در هر برنامه داشته باشد. این نرم افزار از واسطه‌های استاندارد و مؤلفه‌هایی به نام کارگزاران خدمات Service Brokers برای تسهیل ارتباط بین اپلیکیشن‌های مبتنی بر وب استفاده می‌کند.

کد سیار Mobile Code

کد سیار نوعی کدی است که می تواند از طریق شبکه منتقل شود و سپس بر روی یک سیستم یا دستگاه از راه دور اجرا شود. دغدغه های امنیتی با کد سیار حول محور جلوگیری از اجرای کدهای مخرب و بدون اطلاع کاربر می گردد. در این بخش دو نوع اصلی کد سیار، اپلت های جاوا و برنامه های ActiveX و نحوه کارکرد آنها ارائه شده است.

• برنامه های جاوا

برنامه های (اپلتها) جاوا یک مولفه کوچک است که با استفاده از جاوا ساخته شده و در یک مرورگر وب ایجاد شده است. همچنین پلتفرم مستقلی می باشد و کد میانی به نام کد بایت ایجاد کرده که مخصوص پردازنده نیست. وقتی اپلت از رایانه دانلود downloads می کند، ماشین مجازی جاوا Java virtual machine (JVM) که باید در رایانه مقصد موجود باشد، کد بایت را به کد دستگاه تبدیل می کند.

JVM برنامه را در یک محیط حفاظت شده به نام Sandbox اجرا می کند. این ویژگی امنیتی مهم، با نام Java Security Model (JSM)، به کاهش میزان خسارت های ناشی از کد مخرب کمک می کند. با این وجود، مشکل اپلت های خصمانه را (که به آن ماژول های محتوای فعال نیز می گویند) از بین نمی برد، بنابراین اپلت های جاوا هنوز هم باید مورد سوءظن قرار گیرند زیرا ممکن است بعد از دانلود از اینترنت، یک حمله عمدی آغاز شود.

• ActiveX

یک فناوری مایکروسافت است که از OOP استفاده می کند و مبتنی بر COM و DCOM است. این برنامه های خودکفا، کنترل نامیده می شوند و پس از دانلود به بخشی از سیستم عامل تبدیل می شوند. مشکل این است که این کنترل ها در چارچوب امنیتی کاربر فعلی اجرا می شوند، که در بسیاری از موارد دارای حقوق ادمین می باشد و بدان معنی است که یک کنترل مخرب ActiveX می تواند صدمات جدی وارد کند.

ActiveX از فناوری شناسه معتبر Authenticode برای امضای کنترل دیجیتالی استفاده می کند. مشاهده شده که این سیستم دارای نقص قابل توجهی است، و کنترل های ActiveX به طور کلی مورد سوءظن بیشتری نسبت به اپلت های جاوا قرار می گیرند.

امنیت در چرخه عمر توسعه نرم افزار و سیستم Security in the System and Software Development Life Cycle

هنگام نوشتن کد برای نرم افزار جدید، توسعه دهندگان باید مطمئن شوند که کنترل‌های امنیتی مناسب انجام شده و کد امن می‌باشد این بخش شامل چرخه عمر توسعه سیستم، چرخه عمر توسعه نرم افزار، روش‌های توسعه نرم افزار و مدل‌های بلوغ و تیم محصول یکپارچه است.

چرخه عمر توسعه سیستم System Development Life Cycle

وقتی سازمان عملکردهای جدیدی را تعریف می‌کند که باید به مشتریان خود در داخل ارائه دهد، باید سیستم‌هایی را برای ارائه آن عملکرد ایجاد کند. بسیاری از تصمیمات باید اتخاذ شوند و یک فرایند منطقی باید در تصمیم‌گیری‌ها دنبال شود. به این فرایند چرخه عمر توسعه سیستم SDLC (System Development Life Cycle) گفته می‌شود. به جای اینکه یک رویکرد تصادفی باشد، مراحل واضح و منطقی را دنبال می‌کند تا مطمئن شوند که سیستمی که در پایان مراحل توسعه ظهور می‌کند، عملکرد مورد نظر را با سطح قابل قبولی از امنیت فراهم می‌کند. SDLC مراحل زیر را شامل می‌شود:

- ۱- شروع Initiate
- ۲- کسب / توسعه Acquire/Develop
- ۳- پیاده سازی Implement
- ۴- عملیات / حفظ و نگهداری Operate/Maintain
- ۵- مرتب کردن Dispose

در این بخش پنج مرحله از چرخه عمر توسعه سیستم توضیح داده شده است.

۱- شروع Initiate

در این مرحله، این فهم ایجاد می‌شود که یک ویژگی یا عملکرد جدید در یک نرم افزار موجود، درخواست شده یا مورد نیاز است. این ویژگی جدید ممکن است ارتقاء یک محصول موجود یا توسعه یک نرم افزار کاملاً جدید باشد. در هر دو صورت، مرحله شروع شامل تصمیم‌گیری در مورد خرید یا توسعه محصول داخلی است.

در این مرحله، یک سازمان باید به راه حل الزامات امنیتی فکر کند. ایجاد ارزیابی اولیه ریسک می‌تواند مورد استفاده قرار گیرد تا جزئیات و محرمانه بودن، یکپارچگی و در دسترس بودن

(CIA) را مورد تفسیر قرار دهد. شناسایی این موضوعات در ابتدا بسیار مهم است بنابراین این ملاحظات می توانند راهنمای خرید یا توسعه راه حل باشند. هرچه زودتر در چرخه عمر توسعه سیستم الزامات امنیتی مشخص شود، احتمال بیشتری دارد که در محصول نهایی با موفقیت به این موضوعات پرداخته شود.

۲- اکتساب / توسعه Acquire / Development

در مرحله اکتساب / توسعه، چرخه عمر توسعه سیستم، مجموعه ای از فعالیت ها انجام می شود که زمینه را برای تسهیل تصمیم گیری در مورد دستیابی یا توسعه راه حل فراهم می کند. سپس سازمان در مورد راه حل تصمیم گیری می کند. این فعالیت ها برای دریافت پاسخ به سؤالات زیر طراحی شده اند:

- چه عملکردهایی برای اجرای سیستم نیاز دارد؟
 - ریسک های احتمالی CIA که باعث افشا راه حل می شود چیست؟
 - برای برآورده کردن الزامات قانونی و نظارتی باید چه سطوح حفاظتی ارائه شود؟
 - برای اطمینان از کاهش دغدغه های امنیتی، چه تست هایی لازم است؟
 - چگونه راه حل های مختلف شخص ثالث این دغدغه ها را برطرف می کند؟
 - کنترل های امنیتی مورد نیاز راه حل چگونه سایر بخش های سیاست امنیتی شرکت را تحت تأثیر قرار می دهد؟
 - برای ارزیابی موفقیت کنترل های امنیتی از چه معیارهایی استفاده خواهد شد؟
- پاسخ به این سؤالات باید راهنمای اکتساب / توسعه تصمیم گیری و همچنین مراحل باشد که در این مرحله از چرخه عمر توسعه سیستم را دنبال می کند.

۳- پیاده سازی Implement

در مرحله پیاده سازی، راه حل Solution به محیط زنده بدون تکمیل گواهینامه و اعتبارنامه آن معرفی می شود. صدور گواهینامه فرآیند تأیید فنی اثربخشی و امنیت راه حل Solution است. فرآیند اعتبارسنجی شامل مجوز رسمی برای معرفی راه حل در محیط محصول توسط مدیریت است.

۴- عملیات / حفظ و نگهداری Operate/Maintain

پس از عملیاتی شدن سیستم در محیط، این روند پایان نمی‌یابد. انجام یک خط مبنای عملکرد بسیار مهم است به طوری که امکان نظارت مداوم وجود داشته باشد. خط مبنا تضمین می‌کند که مسائل عملکرد به سرعت تعیین می‌شود. هرگونه تغییر در طول زمان (افزودن ویژگی‌های جدید، پیچ‌های راه حل و غیره) باید با توجه به تأثیرات روی پایه، از نزدیک مورد بررسی قرار گیرد.

ایجاد یک فرآیند رسمی مدیریت تغییر، تضمین می‌کند که همه تغییرات تأیید شده و مستند هستند. از آنجا که هرگونه تغییر می‌تواند بر امنیت و عملکرد تأثیر بگذارد، باید توجه ویژه‌ای به نظارت بر راه حل پس از هرگونه تغییر شود.

سرانجام، ارزیابی آسیب پذیری و تست نفوذ پس از اجرای راه حل می‌تواند به کشف هرگونه مشکل امنیتی یا عملکردی که ممکن است با تغییر ایجاد شده یا در نتیجه یک تهدید جدید بوجود آمده باشد، کمک کند.

۵- مرتب کردن Dispose

مرحله Dispose شامل حذف راه حل از محیط هنگام رسیدن به سودمندی آن است. وقتی این اتفاق بیفتد، یک سازمان باید موضوعات خاصی را در نظر بگیرد. که شامل موارد زیر هستند:

- ۱- آیا حذف یا جایگزینی راه حل ایجاد حفره امنیتی در شبکه است؟
- ۲- چگونه می‌توان سیستم را به شکلی منظم خاتمه داد تا باعث قطع ارتباط بین کسب و کار نگردد؟
- ۳- چگونه می‌توان داده‌های باقی مانده بر روی هر سیستم را حذف کرد؟
- ۴- چگونه باید هر سیستم فیزیکی که بخشی از راه حل بود با خیال راحت از بین برود؟
- ۵- آیا موارد قانونی یا نظارتی وجود دارد که منجر به تخریب داده‌ها شود؟

چرخه عمر توسعه نرم افزار Software Development Life Cycle

چرخه عمر توسعه نرم افزار می‌تواند به عنوان زیر مجموعه چرخه عمر توسعه سیستم در نظر گرفته شود که هر سیستم تحت توسعه می‌تواند (اما نه لزوماً) شامل توسعه نرم افزار برای پشتیبانی از راه حل نباشد. هدف چرخه عمر توسعه نرم افزار ارائه چارچوب قابل پیش بینی از رویه‌های طراحی شده برای شناسایی کلیه الزامات با توجه به عملکرد، هزینه، قابلیت اطمینان و

برنامه تحویل و اطمینان از برآورده شدن هر یک از آنها در راه حل نهایی است. در این بخش مراحل چرخه عمر توسعه نرم افزار به تفکیک می پردازد و نحوه کمک به هر مرحله در این هدف نهایی تشریح می شود. به خاطر داشته باشید که مراحل موجود در چرخه عمر توسعه نرم افزار می تواند براساس ارائه دهنده متفاوت باشد و این تنها یک نمونه رایج می باشد. بخش های زیر مراحل چرخه عمر توسعه نرم افزار را با جزئیات شرح می دهد:

- ۱- طرح / شروع پروژه Plan/Initiate Project
- ۲- جمع آوری الزامات Gather Requirements
- ۳- طراحی Design
- ۴- توسعه Develop
- ۵- آزمون / اعتبار سنجی Test/Validate
- ۶- انتشار / حفظ و نگهداری Release/Maintain
- ۷- صدور گواهینامه / اعتبار. Certify/Accredit
- ۸- مدیریت تغییر و مدیریت پیکربندی / جایگزینی. Change Management and Configuration Management/Replacement

۱- طرح / شروع پروژه Plan / Initiate Project

در مرحله طرح / شروع پروژه از چرخه عمر توسعه نرم افزار، سازمان تصمیم می گیرد پروژه جدید توسعه نرم افزار را آغاز کند و به طور رسمی پروژه را برنامه ریزی کند. متخصصان امنیت باید در این مرحله درگیر شوند تا مشخص کنند که آیا اطلاعات درگیر در پروژه نیاز به محافظت دارد یا خیر، و آیا باید از برنامه به صورت جدا از داده های پردازش شده محافظت شود. متخصصان امنیت باید نتایج مورد انتظار برنامه جدید را تجزیه و تحلیل کنند تا مشخص شود که داده های حاصل از سازمان دارای ارزش بالاتری هستند و اگر اینچنین است به حفاظت بیشتری نیاز دارند. هر گونه اطلاعاتی که توسط برنامه بدست می آید، به یک مقدار اختصاص داده شده توسط صاحب آن نیاز دارد و هرگونه الزامات ویژه نظارتی یا انطباقی نیاز به مستند سازی دارد. به عنوان مثال، اطلاعات مراقبت های بهداشتی توسط چندین قانون فدرال تنظیم می شود و باید از آن محافظت شود. طبقه بندی کلیه داده های ورودی و خروجی برنامه نیاز به مستند سازی دارد و کنترل های برنامه مناسب باید مستند شود تا از داده های ورودی و خروجی محافظت شود.

انتقال داده‌ها نیز باید تعیین شود تا انواع شبکه‌های مورد استفاده مشخص شود. همه منابع داده نیز باید مورد تجزیه و تحلیل قرار گیرند. سرانجام، تأثیر برنامه در عملیات سازمانی و فرهنگ نیاز به تجزیه و تحلیل دارد.

۲- جمع آوری الزامات Gather Requirements

در مرحله جمع آوری الزامات چرخه عمر توسعه نرم افزار، هم عملکرد و هم الزامات امنیتی راه حل مشخص شده‌ای است. این الزامات می‌تواند از منابع مختلفی مانند ارزیابی محصولات رقیب برای یک محصول تجاری گرفته شود تا نیاز کاربران برای یک راه حل داخلی بررسی شود. در بعضی موارد، این الزامات می‌تواند از درخواست مستقیم مشتری فعلی ناشی شود.

از دیدگاه امنیتی، یک سازمان باید آسیب پذیری‌ها و تهدیدات احتمالی را شناسایی کند. هنگامی که این ارزیابی انجام شد، باید هدف نرم افزار و محیط مورد انتظار در نظر گرفته شود. علاوه بر این، داده‌هایی که توسط راه حل ایجاد و یا استفاده خواهد شد باید حساسیت آن ارزیابی شود. تعیین امتیاز تأثیر حریم خصوصی به داده‌ها برای کمک به راهنمایی اقدامات در نظر گرفته شده برای محافظت از داده‌ها در ارائه ممکن است مفید باشد.

۳- طراحی Design

در مرحله طراحی چرخه عمر توسعه نرم افزار، یک سازمان توضیحات مفصلي درباره چگونگی برآوردن نرم افزار از کلیه اهداف عملکردی و امنیتی ارائه می‌دهد. در این مرحله تلاش می‌شود تا رفتار داخلی و عملکردهای نرم افزار را با الزامات خاص ترسیم کرده تا بتواند الزاماتی را که قبل از اجرا و تست برآورده نشده اند، شناسایی کند.

در طی این فرآیند، وضعیت اپلیکیشن در هر مرحله از فعالیتهای آن مشخص می‌شود. وضعیت اپلیکیشن به وضعیت عملکردی و امنیتی آن در طی هر عملیاتی که انجام می‌دهد اشاره دارد. بنابراین باید کلیه عملیات ممکن شناسایی شود. این کار برای اطمینان از اینکه نرم افزارها به هیچ وجه وارد حالت ناامن نشوند یا در یک روش غیرقابل پیش بینی عمل نکنند، انجام می‌شود. شناسایی سطح حمله نیز بخشی از این تحلیل است. سطح حمله اهرم‌هایی را که می‌تواند یک مهاجم استفاده کند، توصیف می‌کند. مقدار سطح حمله ممکن است در حالت‌های مختلف اپلیکیشن تغییر کند، اما به هیچ وجه نباید سطح حمله ارائه شده نیازهای امنیتی مشخص شده در مرحله جمع آوری را نقض کند.

۴- توسعه Develop

مرحله توسعه شامل نوشتن کد یا دستورالعمل هایی است که باعث می شود نرم افزار کار کند. تأکید این مرحله پایبندی جدی به روشهای رمزگذاری امن است. بعضی از مدل هایی که می توانند به ارتقاء رمزگذاری امن کمک کنند، در بخش بعدی در بخش "بهترین روش های توسعه امنیت نرم افزار" ارائه شده است.

بسیاری از مسائل امنیتی با نرم افزار از طریق شیوه های رمزگذاری ناامن از قبیل عدم اعتبار سنجی ورودی یا بررسی نوع داده ایجاد می شوند. شناسایی این موارد در یک بررسی کد، سعی در پیش فرض همه سناریوهای حمله احتمالی و تأثیر آنها بر روی کد دارد. عدم شناسایی این موارد می تواند به حمله هایی مانند سرریز بافر و نفوذ و سایر شرایط خطایی منجر شود که بعداً در این فصل به آن می پردازیم.

۵- تست / اعتبار سنجی Test / Validate

در مرحله تست / اعتبار سنجی، چندین نوع تست باید انجام شود، از جمله روش هایی برای شناسایی خطاهای عملکردی و همچنین مسائل امنیتی. روش متمایزی که میزان تست سیستم را ارزیابی می کند و منطق برنامه خاصی را که آزمایش نشده است شناسایی می کند، روش تست داده Test data method نامیده می شود. این روش نه تنها ورودی مورد انتظار یا معتبر را تست می کند، بلکه مقادیر نامعتبر و غیرمنتظره را نیز برای ارزیابی رفتار نرم افزار در هر دو حالت تست می کند. باید یک حمله فعال برای حمله به نرم افزار انجام شود، مثل تلاش برای سرریز بافر و حملات انکار سرویس DoS.

برخی از اهداف تست انجام شده:

- تست تأیید صحت Verification testing: تعیین می کند که آیا مشخصات طراحی اصلی رعایت شده است یا خیر.
- تست اعتبار سنجی Validation testing: نمای سطح بالاتری را نشان می دهد و تعیین می کند که آیا هدف اصلی این نرم افزار حاصل شده است یا خیر.

نرم افزار به طور معمول در قطعات یا ماژول هایی از کد ساخته شده است که بعداً برای تولید محصول نهایی جمع می شوند. هر ماژول باید به روشی جداگانه تست شود، به روشی بنام تست واحد Unit testing. داشتن کارمندان توسعه در انجام این تست بسیار مهم است، اما با کمک

گروه دیگری از مهندسين نسبت به افرادی که کد را نوشتند، می‌توان مطمئن شد که یک فرآیند بی‌طرفانه اتفاق می‌افتد. این نمونه خوبی از مفهوم تفکیک وظایف است.

موارد زیر باید مشخصات تست واحد باشد:

- داده‌های تست بخشی از مشخصات است.
 - تست باید مقادیر خارج از محدوده و شرایط خارج از محدوده را بررسی کند.
 - نتایج خروجی تست صحیح باید از قبل تهیه و شناخته شود.
 - داده‌های درست یا واقعی برای استفاده در مراحل تست واحد توصیه نمی‌شوند.
- تست‌های اضافی که توصیه می‌شود شامل موارد زیر است:
- تست یکپارچه سازی Integration testing: نحوه کار ماژول‌ها را با یکدیگر ارزیابی می‌کند و تعیین می‌کند که مشخصات عملکردی و امنیتی برآورده شده‌اند یا خیر.
 - تست پذیرش Acceptance testing: اطمینان می‌دهد که مشتری (چه داخلی و چه خارجی) از عملکرد نرم افزار راضی است.
 - تست رگرسیون Regression testing: بعد از ایجاد تغییر در کد، محل اطمینان ایجاد می‌شود تا تضمین شود که این تغییرات نه عملکرد و نه امنیت را کاهش داده‌اند.

۶- انتشار / حفظ نگهداری Release/Maintain

مرحله انتشار / نگهداری شامل اجرای نرم افزار در محیط زنده و نظارت مداوم بر عملکرد آن است. یافتن مشکلات امنیتی و عملکرد اضافی در این مرحله، به عنوان نرم افزار شروع واسط با سایر عناصر شبکه، امری غیر عادی نیست.

در بسیاری از موارد، آسیب پذیری‌ها در محیط‌های زنده کشف می‌شوند که هیچ گونه اصلاح یا پچی در آن وجود ندارد، که به آنها آسیب پذیری صفر روز Zero-day Vulnerability گفته می‌شود. البته بهتر است سازمان از کارمندان پشتیبانی برخوردار باشد و این مسائل را کشف کند تا اینکه افرادی که به دنبال بهره برداری از آسیب پذیری هستند آنها را کشف کنند.

۷- گواهی / اعتبار Certify/Accredit

صدور گواهی فرایند ارزیابی نرم افزار برای اثربخشی امنیتی با توجه به نیاز مشتری است. امتیازات مطمئناً می‌تواند ورودی این امر باشد، اما تنها مورد قابل توجه نیست. اعتبارسنجی پذیرش رسمی کفایت امنیت کلی یک سیستم توسط مدیریت است. اعتبارسنجی موقت برای مدت مشخصی

اختصاص داده می شود و لیست های مورد نیاز در اپلیکیشن ها، سیستم ها یا اسناد معتبر را فهرست می کند. اعطای اعتبارنامه کامل به اعتبارسنجی بدون هیچ گونه تغییر و تحول لازم را تصدیق می کند. اعتبارنامه موقت پس از تکمیل، تجزیه و تحلیل و تأیید توسط نهاد صدور مجوز را، اعتبارنامه کامل می گویند. در حالیکه صدور گواهینامه و اعتبارنامه مرتبط هستند، ولی آنها به عنوان دو مرحله در یک فرآیند در نظر گرفته نمی شوند.

۸- مدیریت تغییر / مدیریت پیکربندی / جایگزینی Change Management and Configuration Management/Replacement

پس از استقرار یک راه حل در یک محیط زنده، به ناچار تغییرات اضافی رخ می دهد که باید به دلیل مشکلات امنیتی در نرم افزار ایجاد شده باشند. در بعضی موارد ممکن است این نرم افزار برای افزایش یا افزایش کارایی آن تغییر یابد. در هر دو صورت، تغییرات باید از طریق یک فرایند رسمی تغییر و مدیریت پیکربندی صورت گیرد.

هدف از این فرآیند اطمینان از این است که کلیه تغییرات در پیکربندی و در منبع توسط پرسنل مناسب تأیید شده و به صورت امن و منطقی انجام شود. این فرایند باید همیشه از ادامه عملکرد در محیط زنده مطمئن شود و تغییرات باید کاملاً مستند شده، از جمله کلیه تغییرات در سخت افزار و نرم افزار.

در برخی موارد، ممکن است لازم باشد اپلیکیشن ها یا سیستم ها را به طور کامل جایگزین کرد. ممکن است برخی از شکستها با پیشرفت یا تغییرات برطرف شوند و ممکن است خرابی رخ دهد که احتمال دارد تنها با جایگزینی کامل اپلیکیشن برطرف شود.

روش های توسعه نرم افزار و مدل های بلوغ Software Development Methods and Maturity Models

در جریان ایجاد نرم افزار طی دهه های گذشته، توسعه دهندگان موردهای زیادی در مورد روند توسعه آموخته اند. از آنجا که پروژه های توسعه از یک توسعه دهنده منفرد به تیم های کوچک تبدیل شده اند و تیم های بزرگ در حال توسعه روی پروژه های عظیم با ماژول های زیادی کار می کنند که باید به طور ایمن در تعامل باشند، مدل های توسعه ای برای افزایش کارایی و موفقیت این پروژه ها ایجاد شده اند. در این بخش برخی از مدل های رایج به همراه مفاهیم و شیوه هایی که برای اجرای آنها باید درک شوند را در بر می گیرد.

در این بخش روشهای زیر توسعه نرم افزار مورد بحث قرار گرفته است:

۱. ساخت و تعمیر
۲. آبشار
۳. ۷ شکل
۴. نمونه سازی
۵. مدل نمونه اولیه اصلاح شده
۶. افزایشی
۷. مارپیچ
۸. چابک
۹. توسعه سریع اپلیکیشن
۱۰. توسعه تجزیه و تحلیل مشترک (JAD)
۱۱. اتاق تمیز
۱۲. توسعه برنامه نویسی ساخت یافته
۱۳. مدل اکتشافی
۱۴. مهندسی نرم افزار به کمک رایانه (CASE)
۱۵. توسعه مبتنی بر مؤلفه
۱۶. مدل قابلیت بلوغ یکپارچه (CMMI) Capability Maturity Model Integration
۱۷. مدل ISO 9001: 2015/90003: 2014

✓ ساخت و تعمیر Build و Fix

اگرچه این یک الگوی رسمی نیست، رویکرد Build و Fix روشی را توصیف می کند که در گذشته به طور قطع مورد استفاده قرار می گرفت، ولی تا حد زیادی بی اعتبار بوده و اکنون به عنوان الگویی برای نحوه مدیریت یک پروژه توسعه استفاده نمی شود. به عبارت ساده تر، در این روش، نرم افزار در اسرع وقت توسعه یافته و منتشر می شود.

هیچ مکانیزم کنترل رسمی برای ارائه بازخورد در طی فرآیند استفاده نمی شود. این محصول به بازار عرضه می شود و مشکلات به صورت کشف شده با پیچ و بسته های سرویس برطرف می شود. اگرچه این رویکرد باعث می شود محصول سریعتر و ارزان تر به بازار عرضه شود، اما در بلند مدت

هزینه‌های مربوط به رفع مشکلات و خسارت موازی به محصول موجود در بازار از هرگونه هزینه صرفه جویی اولیه بالاتر است.

با وجود این، به نظر می‌رسد این مدل هنوز در حال استفاده است، اکثر توسعه دهندگان موفق به این نتیجه رسیده اند که یکی از مدل‌های دیگری که در این بخش مورد بحث قرار گرفته است را پیاده سازی کنند تا محصول اولیه اگرچه لزوماً کامل نبوده، اما بسیار نزدیکتر به همه عملکردها و الزامات امنیتی طرح باشد. علاوه بر این، استفاده از این مدل‌ها به شناسایی و از بین بردن هرچه بیشتر حفره‌ها (bugها) کمک می‌کند بدون استفاده مشتری به عنوان "کنترل کیفیت".

در این مدل ساده از فرایند توسعه نرم افزار، فرضیات غیرواقعی خاصی ساخته شده است، از جمله:

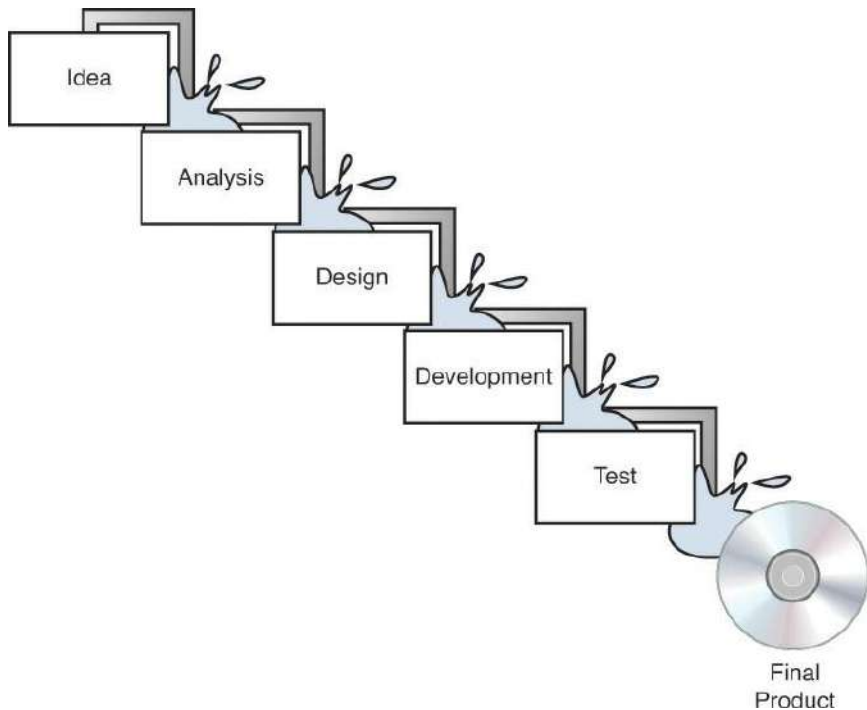
- هر مرحله می‌تواند بدون تأثیر مراحل بعدی تکمیل و نهایی شود، که ممکن است نیاز به دوبارکاری داشته باشد.

- تکرار (دوبارکاری و تکرار) از جمله مراحل فرایندی که معمولاً در مدل‌های دیگر فراخوانی می‌شود، در این مدل تأکید نمی‌شود.

- مراحل مانند برخی از مدل‌های دیگر که در اینجا مورد بحث قرار گرفته است، به عنوان نقاط عطف فردی مشاهده نمی‌شوند.

✓ آبشار Waterfall

مدل آبشار اصلی فرایند توسعه را به مراحل مشخصی تقسیم می‌کند. اگرچه این مدل تا حدودی یک رویکرد سخت است، اما روند اصلی به عنوان یک سری مراحل متوالی است که بدون بازگشت به مراحل قبلی دنبال می‌شود. این رویکرد توسعه افزایشی Incremental development نامیده می‌شود. شکل ۸-۱ نمایانگر روند آبشار است.

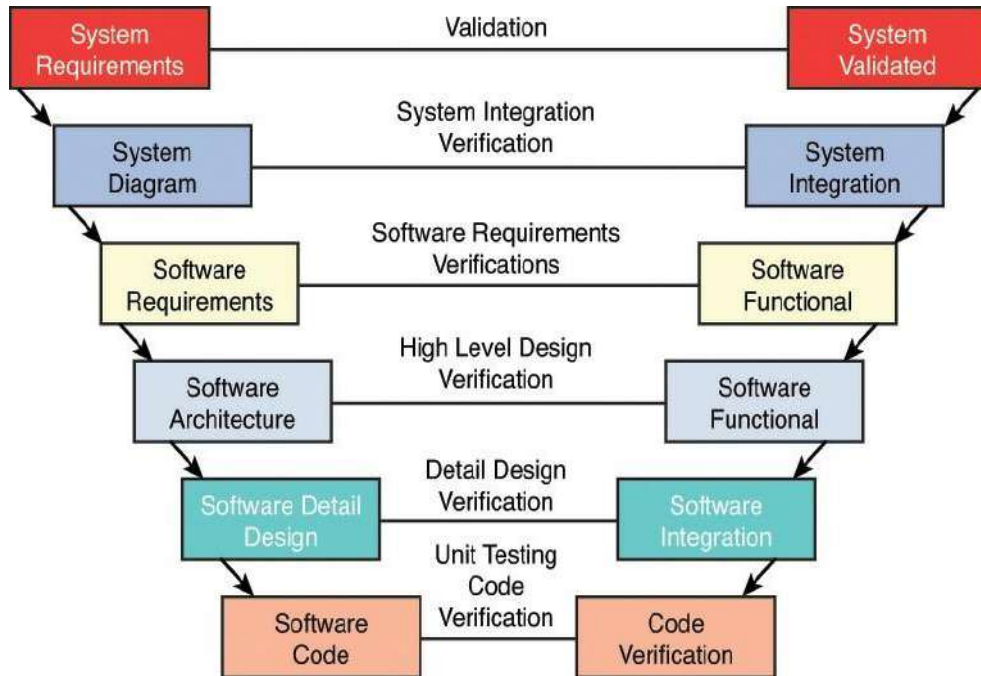


شکل ۸-۱: مدل آبشار

در مدل اصلاح شده Waterfall، هر مرحله از فرآیند توسعه نقطه عطف خاص خود را در فرآیند مدیریت پروژه در نظر می‌گیرد. تکرار نامحدود به عقب (بازگشت به مراحل اولیه برای رفع مشکلات) در این مدل مجاز نیست. اما، تأیید و اعتبار سنجی محصول در این مدل انجام می‌شود. مشکلاتی که در طول پروژه کشف می‌شوند، بازگشت به مراحل اولیه را آغاز نمی‌کنند، بلکه پس از اتمام پروژه با آنها برخورد می‌شود.

مدل V شکل

مدل V شکل نیز تا حدودی سخت است اما در درجه اول با روش آبشار متفاوت است زیرا در هر مرحله تایید و اعتبارسنجی انجام می‌شود. اگرچه این مدل می‌تواند زمانی کار کند که کلیه الزامات به صورت مقدماتی به خوبی درک شود (اغلب این طور نیست) و تغییرات دامنه بالقوه اندک باشد، اما این کار را برای اجرای همزمان رخدادها فراهم نمی‌کند زیرا این یک فرآیند متوالی مانند آبشار است. در این مدل احتمال موفقیت بیشتر وجود دارد زیرا در هر مرحله تست را انجام می‌دهد. شکل ۸-۲ نمایانگر این فرآیند است.



شکل ۸-۲: مدل V شکل

✓ نمونه سازی Prototyping

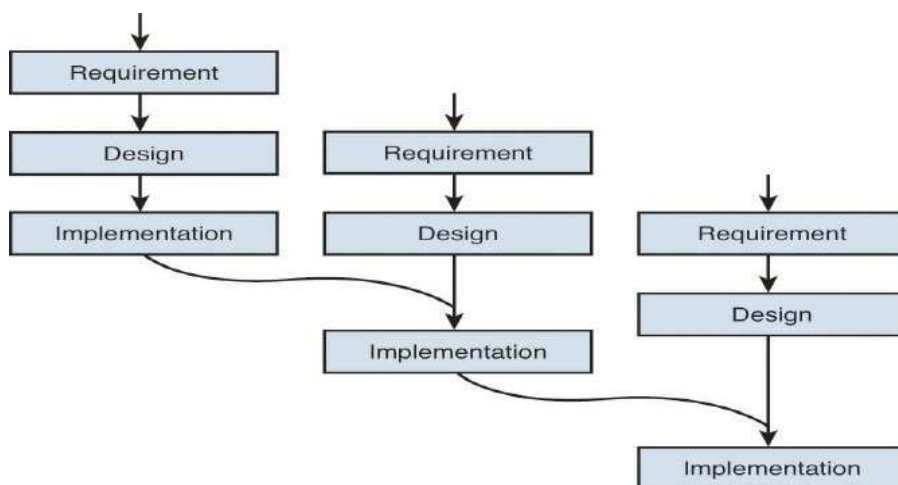
اگرچه این یک مدل رسمی برای خود نمی باشد، ولی نمونه سازی استفاده از نمونه کد برای کشف یک رویکرد خاص برای حل یک مشکل است قبل از اینکه زمان و هزینه های گسترده در رویکرد سرمایه گذاری شود. این مدل به تیم اجازه می دهد تا ابزار کد نمونه را شناسایی کرده و همچنین مشکلات طراحی را با رویکرد مشخص کنند. سیستم های نمونه سازی می توانند در زمان و هزینه قابل توجهی صرفه جویی کنند زیرا لازم نیست کل محصول نهایی را برای شروع تست کنند.

✓ مدل نمونه اصلاح شده (MPM) Modified Prototype Model

MPM یک روش نمونه سازی است که بیشتر برای توسعه برنامه های وب استفاده می شود. با استفاده از این مدل، عملکردهای اساسی بصورت رسمی به سرعت مستقر می شوند. مرحله نگهداری پس از استقرار آغاز می شود. برنامه با گذشت زمان تکامل می یابد. روند این مدل قابل انعطاف است.

افزایشی Incremental

به پالایش مدل اصلی آبشار که بیان می کند نرم افزار باید با افزایش قابلیت های کاربردی توسعه یابد، مدل افزایشی نامیده می شود. در این مدل، یک نسخه کاری یا تکرار راه حل تا زمان تکمیل محصول نهایی تولید، تست و دوباره تولید می شود. می توان از آن به عنوان یک سری از مدل آبشار عنوان کرد. پس از اتمام هر تکرار یا نسخه از نرم افزار، تست برای شناسایی شکاف ها در عملکرد و امنیت طراحی اصلی انجام می شود. سپس مراحل مشابه تجزیه و تحلیل، طراحی، کد و مراحل تست با همان شکافها برطرف می شود. زمانی که محصول با توجه به طرح اصلی قابل قبول تلقی می شود، انتشار می یابد. شکل ۸-۳ نمایانگر این فرآیند است.

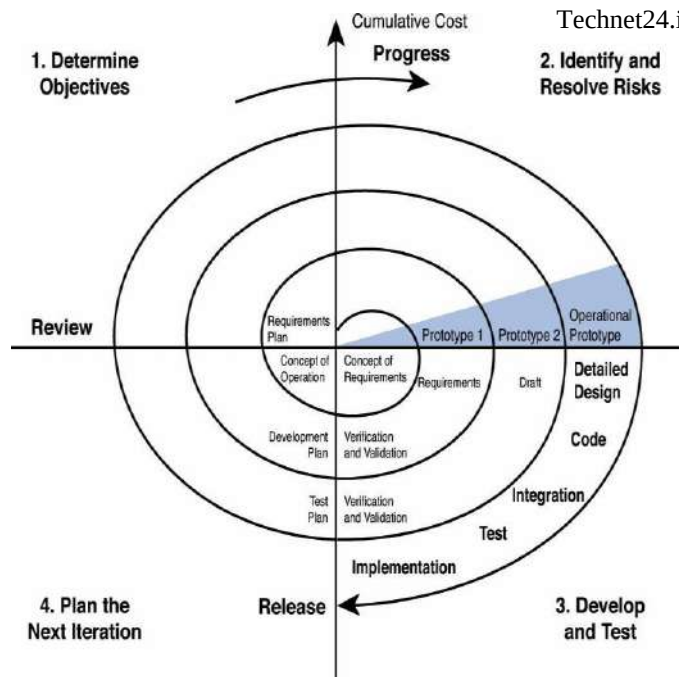


شکل ۸-۳: مدل افزایشی

✓ مارپیچ (حلزونی) Spiral

مدل مارپیچ (حلزونی) در واقع یک ابرمدل Meta-model می باشد که تعدادی از مدل های توسعه نرم افزار را شامل می شود. همچنین این مدل یک رویکرد تکراری است اما در هر مرحله تأکید بیشتر بر تحلیل ریسک دارد. نمونه های اولیه در هر مرحله تولید می شوند و این فرآیند را می توان حلقه ای دانست که باعث می شود گردش به عقب داشته تا نگاهی انتقادی به ریسک های مورد بررسی داشته باشد، در حالی که هنوز هم به ریسک های جدیدی که ممکن است در آخرین تکرار ایجاد شده باشد، امکان مشاهده را می دهد.

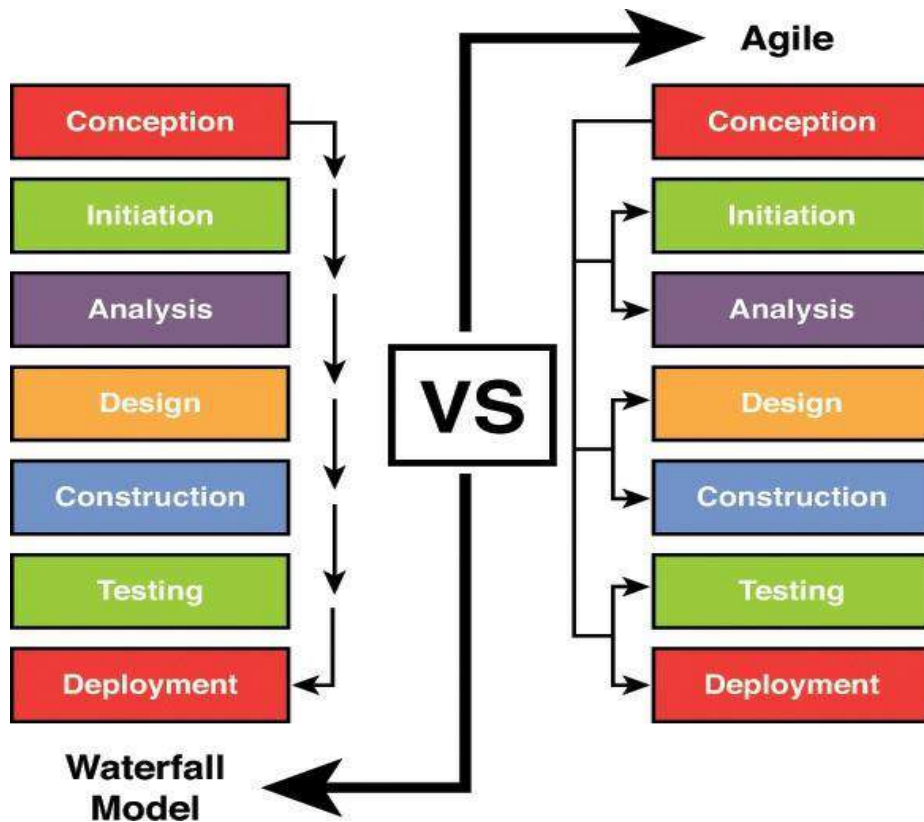
این مدل فرض می کند که دانش در هر تکرار بدست می آید و باید همانطور که تکامل می یابد، در طرح گنجانیده شود. برخی موارد حتی در هر تکرار نیز اظهار نظر و مشاهداتی را انجام می دهد. شکل ۴-۸ نمایانگر این فرآیند است. بعد شعاعی نمودار نمایانگر هزینه تجمعی است و بعد زاویه ای بیانگر پیشرفت های انجام شده در تکمیل هر چرخه است.



شکل ۴-۸: مدل مارپیچ

✓ چابک Agile

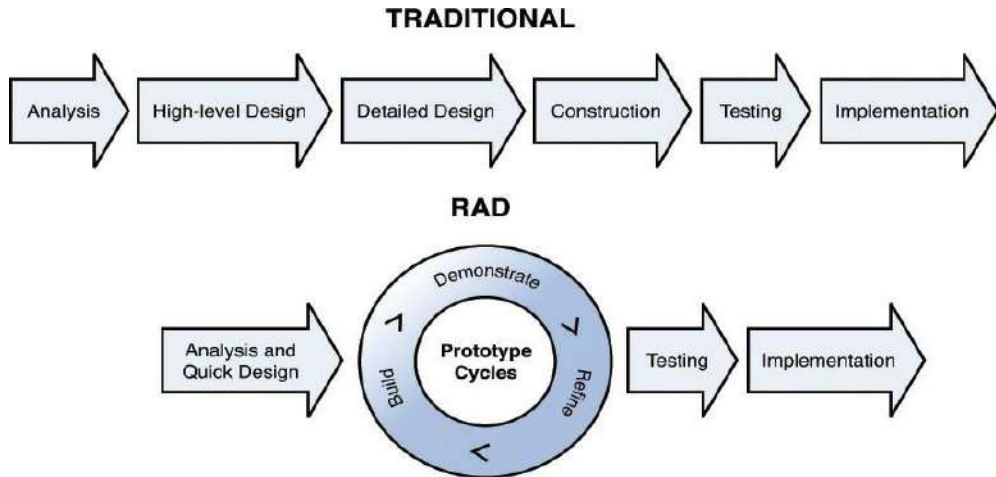
بسیاری از فرآیندهای مورد بحث تاکنون متکی و پایبند سخت به مدل های فرآیند محور هستند. در بسیاری از موارد، تمرکز بیشتر روی دنبال کردن مراحل رویه ای است تا واکنش سریع به تغییرات و افزایش کارایی. مدل چابک تأکید بیشتری بر بازخورد مداوم و کار تیمی متقابل دارد. سعی می شود به اندازه کافی قدرتمند باشد تا در برابر موقعیت هایی که در طول توسعه بوجود می آیند واکنش نشان دهند. زمان کمتری برای تجزیه و تحلیل مقدماتی صرف می شود و تأکید بیشتری بر یادگیری روند کار و درج دروس آموخته شده در زمان واقعی می شود. همچنین در طول فرایند تعامل بیشتری با مشتری وجود دارد.



شکل ۸-۵: مقایسه مدل چابک و آبشار

توسعه سریع برنامه‌های کاربردی (RAD) Rapid Application Development

در مدل توسعه سریع برنامه کاربردی یا RAD، زمان کمتری برای طراحی صرف می‌شود و تأکید بر تولید سریع نمونه‌های اولیه با این فرض است که دانش حیاتی را فقط با آزمایش و خطا می‌توان بدست آورد. این مدل به ویژه هنگامی مفید است که الزامات در ابتدا به خوبی درک نشده باشند و با بوجود آمدن مشکلات و چالش‌ها در حین ساخت نمونه‌های اولیه، ساخته می‌شوند. شکل ۸-۶ مقایسه مدل RAD با مدل‌های سنتی است، جایی که پروژه به طور کامل تکمیل شده و سپس تأیید و معتبر می‌شود.



شکل ۸-۶: مدل های سنتی و RAD

✓ توسعه تجزیه و تحلیل مشترک (JAD) Joint Analysis Development

مدل JAD از رویکرد تیمی استفاده می کند. این مدل از کارگاه های آموزشی استفاده می کند تا هر دو در مورد الزامات به توافق برسند و اختلافات را برطرف سازد. تئوری این مدل اینگونه است که جمع کردن همه طرفین باهم در همه مراحل باعث می شود در پایان فرآیند محصول رضایت بخش تری ظاهر شود.

✓ اتاق تمیز Cleanroom

در مقایسه با مدل JAD، مدل Cleanroom به مراحل رسمی و کاملاً به یک روش ساخت یافته تر پایبند است. تلاش می شود از طریق آزمایشات گسترده از خطاها و اشتباهات جلوگیری شود. این روش در شرایطی کار می کند که کیفیت بالا حیاتی باشد، اپلیکیشن بسیار مهم باشد، یا راه حل باید در یک فرآیند صدور گواهینامه سختگیرانه انجام شود.

✓ توسعه برنامه نویسی ساخت یافته Structured Programming Development

در مدل توسعه برنامه نویسی ساخت یافته، برنامه نویسان برنامه هایی را می نویسند در حالی که تأثیر بر کیفیت محصولات نهایی می گذارند. این یکی از شناخته شده ترین مدل های توسعه است و نیاز به فرآیندهای تعریف شده دارد. محصول در پایان هر مرحله برای تأیید بررسی می شود. امنیت به شکلی رسمی و ساختار یافته اضافه می شود.

✓ مدل اکتشافی Exploratory Model

در مدل اکتشافی، الزامات بر اساس آنچه در حال حاضر موجود است، صورت می‌گیرد. فرضیات در مورد چگونگی عملکرد سیستم مستند شده است. برای ایجاد یک سیستم قابل استفاده، بینشها و پیشنهادات دیگر در هنگام کشف ترکیب می‌شوند. در این مدل، امنیت احتمالاً بر پیشرفت‌ها اولویت نخواهد داشت. در نتیجه، کنترل‌های امنیتی اغلب به صورت موقت انجام می‌شود.

✓ مهندسی نرم افزار به کمک رایانه (CASE) Computer-Aided Software Engineering

روش CASE از رایانه‌ها و ابزارهای رایانه‌ای برای کمک به تجزیه و تحلیل، طراحی، توسعه، پیاده سازی و نگهداری نرم افزار استفاده می‌کند و مستلزم ایجاد ابزارهای نرم افزاری و آموزش برای توسعه دهندگان است. ابزارهای CASE به دسته‌های زیر تقسیم می‌شوند:

۱. مدل سازی تجزیه و تحلیل و کسب و کار Business and analysis modeling
۲. توسعه Development
۳. تأیید و اعتبار سنجی Verification and validation
۴. مدیریت پیکربندی Configuration management
۵. معیار و اندازه گیری Metrics and measurement
۶. مدیریت پروژه Project management

✓ توسعه مبتنی بر مؤلفه Component-Based Development

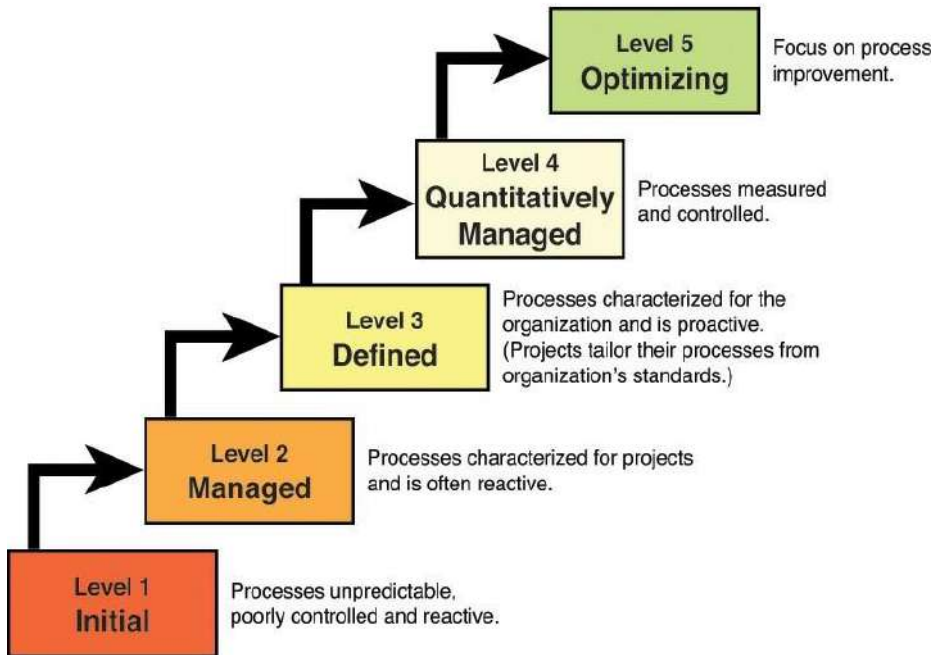
روش توسعه مبتنی بر مؤلفه از ساختن بلوکها استفاده می‌کند تا یک برنامه را بجای ساخت، اسمبل کند. مزیت این روش از نظر امنیت این است که مؤلفه‌ها قبل از استفاده در برنامه، از نظر امنیتی تست می‌شوند.

✓ مدل قابلیت بلوغ یکپارچه

Capability Maturity Model Integration (CMMI) مجموعه‌ای کامل از دستورالعمل‌ها است که به کلیه مراحل چرخه عمر توسعه نرم افزار می‌پردازد. این مدل مجموعه‌ای از مراحل یا سطح بلوغ را توصیف می‌کند که می‌تواند یک فرایند توسعه را طی کند، از آنجا که از مدل

hoc)ساخت و تعمیر) به مرحله دیگری می‌رود که شامل یک برنامه بودجه‌ای برای بهبود مستمر است. شکل ۷-۸ سطح بلوغ آن را نشان داده و هریک را توضیح می‌دهد.

Characteristics of Maturity Levels



شکل ۷-۸: سطوح بلوغ CMMI

ISO 9001:2015/90003:2014

ISO 9001: 2015 یک استاندارد سیستم مدیریت کیفیت است که به تازگی منتشر شده است. این استاندارد نیازها برای سیستم مدیریت کیفیت را مشخص می‌کند وقتی که یک سازمان (۱) باید توانایی خود را برای ارائه به طور مداوم محصولات و خدماتی مطابق با مشتری و الزامات قانونی و مقرر قابل اجرا نشان دهد و (۲) هدف از این کار افزایش رضایت مشتری از طریق استفاده مؤثر از سیستم، از جمله فرایندهای بهبود سیستم و اطمینان از انطباق با مشتری و الزامات قانونی و مقررات قابل اجرا است.

کلیه الزامات ISO 9001:2015 عمومی است و علیرغم نوع یا اندازه آن و همینطور علیرغم محصولات و خدمات ارائه شده، برای هر سازمان قابل اجرا می‌باشد.

ISO 9003: 2014 سازمانها را در استفاده از ISO 9001: 2015 از نظر اکتساب، تهیه، توسعه، بهره برداری و نگهداری نرم افزارهای رایانه‌ای و خدمات پشتیبانی مرتبط راهنمایی می‌کند. این الزامات را ISO 9001: 2015 اضافه نمی‌کند مگر اینکه تغییر کند.

کاربرد ISO / IEC 90003: 2014 مناسب با نرم افزارهایی است که قسمتی از یک قرارداد تجاری با یک سازمان دیگر است، ممکن است محصولی که برای یک بخش بازار در دسترس است، برای پشتیبانی از فرآیندهای یک سازمان، تعبیه شده در یک محصول سخت افزاری یا مربوط به خدمات نرم افزاری برخی از سازمانها که در همه این فعالیتها شرکت داشته باشد. افراد دیگر ممکن است در یک ناحیه تخصص داشته باشند. هر شرایطی که باشد، سیستم مدیریت کیفیت سازمان باید کلیه جوانب (نرم افزاری و غیر نرم افزاری) مشاغل را پوشش دهد.

ISO / IEC 90003: 2014 موضوعاتی که باید مورد توجه قرار گیرد را مشخص می‌کند و مستقل از فناوری، مدل‌های چرخه عمر، فرآیندهای توسعه، دنباله فعالیتها و ساختار سازمانی است که توسط یک سازمان استفاده می‌شود. راهنمایی و دستورالعمل‌های اضافی و مراجعه مکرر به استانداردهای مهندسی نرم افزار ISO / IEC JTC 1 / SC 7 برای کمک به کاربرد ISO 9001: 2015، به ویژه ISO / IEC 12207: 2008 ارائه شده است. ISO 9001: 2015 مربوط به سیستم‌های مدیریت کیفیت است و ISO / IEC 12207: 2008 مربوط به سیستم‌ها و مهندسی نرم افزار و فرآیندهای چرخه عمر نرم افزار است. کل دامنه این دو استاندارد برای متخصص امنیت مهم نیست. با این حال، متخصص امنیت باید مطمئن شود که تیم توسعه نرم افزار این استانداردها را درک کرده و از آنها پیروی می‌کند.

تیم محصول یکپارچه Integrated Product Team

توسعه محصولات و فرایندهای یکپارچه Integrated Product and Process Development (IPPD) کلیه فعالیتهای ضروری اکتساب را از طریق استفاده از تیم‌های چند تخصصی برای بهینه سازی مراحل طراحی، ساخت و پشتیبانی انجام می‌دهند. IPPD هزینه‌های تعیین شده و اهداف عملکرد را از مفهوم محصول از طریق تولید، از جمله پشتیبانی میدانی، تسهیل می‌کند. یکی از اصول مهم IPPD کار تیمی چند تخصصی از طریق تیم‌های محصولات یکپارچه Integrated Product Teams (IPTs) است.

فرآیند دستیابی به طور معمول به پنج فاز تقسیم می‌شود که چهار فاز رسمی اول توسط نقاط عطف تصمیم‌گیری تفکیک می‌شوند. این پنج فاز شامل:

- ۱- فاز صفر: مفهوم اکتشاف (CE) Concept Exploration
 - ۲- فاز اول: تعریف برنامه و کاهش ریسک (PDRR) Program Definition and Risk Reduction
 - ۳- فاز دوم: توسعه ساخت و مهندسی (EMD) Engineering and Manufacturing Development
 - ۴- فاز سوم: تولید، زمینه سازی / استقرار و پشتیبانی عملیاتی
 - ۵- Production, Fielding/Deployment, and Operational Support (PFDOS)
 - ۶- دفع و تخریب زدایی (DD) Demilitarization and Disposal
- در کتاب DoD آمده است که IPT باید کارآمد و مؤثر باشد. نکته مهمی که باید به خاطر داشته باشید این است که هر IPT در IPPD مأموریتی برای تهیه و عرضه یک محصول و فرآیندهای مرتبط با آن دارد. در سطح برنامه، مشخصات IPT شامل موارد زیر است:
- مسئولیت یک محصول یا فرآیند تعریف شده
 - اقتدار بر منابع و پرسنل
 - یک برنامه توافق شده برای تحویل محصول تعریف شده
 - یک سطح ریسک توافق شده برای عرضه محصول تعریف شده
 - مجموعه‌ای از معیارهای اندازه گیری قابل توافق
- IPTها بخشی تفکیک ناپذیر از فرایند نظارت و دستیابی به فرایند بررسی هستند. به طور کلی دو سطح IPT وجود دارد: تیم محصول یکپارچه در سطح کار Working-Level Integrated Product Team (WIPT) و تیم محصول یکپارچه فراگیر Overarching Integrated Product Team (OIPT). هر برنامه باید دارای یک WIPT و حداقل یک WIPT باشد. WIPT باید روی یک موضوع خاص، از جمله هزینه / عملکرد، خط مبنا برنامه، استراتژی اکتساب، تست و ارزیابی یا پیمانکاری تمرکز کند. یک تیم محصول یکپارچه کامل یا Integrating integrated Product Team (IIPT)، که نوعی WIPT است، باید تلاش‌های WIPT را هماهنگ کند و کلیه مباحث برنامه، از جمله مواردی را که در IPT دیگر به آنها اختصاص نیافته است، پوشش دهد. مشارکت IPT راه اصلی برای هر سازمانی است که بخشی از برنامه اکتساب باشد. IIPT به دلیل اینکه بینش برنامه در سطح کارکنان نسبت به برنامه‌ها در سطح برنامه را تسهیل می‌کند و ورودی لازم را به OIPT ارائه می‌دهد، ضروری است.
- DevOps که ترکیبی از توسعه و عملیات (Operations, Development) است، ضمن اتوماسیون فرایند تحویل نرم افزار و تغییرات زیرساختی، بر همکاری و ارتباط توسعه دهندگان نرم افزار و

سایر متخصصان فناوری اطلاعات تأکید دارد. هدف این است که مطمئن شود که ساخت، تست و انتشار نرم افزار می تواند سریعتر، بیشتر و با اطمینان بیشتری اتفاق بیفتد.

کنترل های امنیتی در توسعه Security Controls in Development

کنترل های امنیتی در توسعه نرم افزار باید بدرستی اجرا شوند تا اطمینان حاصل شود که مسائل امنیتی با نرم افزار برای سازمان مشکل ساز نمی شوند. برای ارائه کنترل های امنیتی، توسعه دهندگان باید:

- ✓ بهترین راهکارهای امنیت توسعه نرم افزار و امنیت محیط نرم افزار را درک کنند.
- ✓ مشکلات کد منبع را شناسایی کرده و بدانند که ابزارهای تحلیل کد منبع در دسترس هستند و چه کاری انجام می دهند.
- ✓ امنیت مخازن کد را تأمین کنند.
- ✓ اجرای واسط امنیتی در برنامه نویسی نرم افزار.
- ✓ تهدیدات نرم افزار و مکانیسم های محافظت از نرم افزار درک شود.

بهترین راهکارهای توسعه نرم افزار Software Development Security Best Practices

تعدادی از سازمانها برای حمایت از هدف اطمینان از دستیابی کامل نرم افزار با توجه به عملکرد و امنیت، سعی در جمع آوری مجموعه ای از بهترین نرم افزارهای توسعه نرم افزار دارند. در این بخش، به برخی از آن سازمانها خواهیم پرداخت و در ادامه تعدادی از مهمترین توصیه های آنها ذکر خواهد شد.

کنسرسیوم امنیت برنامه وب (WASC) Web Application Security Consortium

کنسرسیوم امنیت برنامه وب یا WASC سازمانی است که بهترین اپلیکیشن ها را برای برنامه های مبتنی بر وب به همراه منابع، ابزار و اطلاعات متنوعی فراهم می کند که سازمان ها می توانند در توسعه برنامه های وب از آنها استفاده کنند. یکی از کارکردهای انجام شده توسط WASC، نظارت مستمر بر حملات، منجر به تهیه لیستی از برترین روشهای حملات در حال استفاده است. این لیست می تواند تضمین کند که سازمانها نه تنها از جدیدترین روشهای حمله و چگونگی گسترش این حملات آگاه هستند بلکه می توانند به آنها در ایجاد تغییرات مناسب در برنامه های وب خود برای کاهش این نوع حمله کمک کنند.

(OWASP) Open Web Application Security Project

پروژه امنیت برنامه باز وب گروه دیگری که حملات را کنترل می کند، بخصوص حملات وب. OWASP لیستی از ۱۰ حمله برتر را بطور مداوم نگهداری می کند. این گروه همچنین جلسات منظم را در سرتاسر جهان برگزار می کند، منابع و ابزارهایی از جمله مراحل تست، مراحل بررسی کد و دستورالعمل های توسعه را ارائه می دهد.

BSI

وزارت امنیت میهن Department of Homeland Security (DHS) نیز درگیر ارتقاء بهترین شیوه های امنیتی نرم افزار شده است. ابتکار Build Security In (BSI) یک رویکرد فرایند متحد را ترویج می کند که توصیه های امنیتی را با توجه به معماری ها، روش های تست، بررسی کد و فرآیندهای مدیریت ارائه می دهد. برنامه تضمین نرم افزار DHS راه هایی برای کاهش آسیب پذیری ها، کاهش بهره برداری ها و بهبود روال توسعه و تحویل راه حل های نرم افزاری ارائه می دهد.

ISO / IEC 27000

سازمان بین المللی استاندارد سازی یا ISO و کمیسیون بین المللی الکتروتکنیک یا IEC استاندارد ۲۷۰۳۴ را ایجاد کردند که بخشی از استانداردهای بزرگتر به نام سری ISO / IEC 27000 است. این استانداردها سازمانها را برای ادغام امنیت در توسعه و نگهداری برنامه های نرم افزاری، راهنمایی می کنند. این پیشنهادات نه تنها به توسعه برنامه های داخلی، بلکه به استقرار و مدیریت ایمن راه حل های شخص ثالث در شرکت مربوط می شود.

امنیت محیط نرم افزار Software Environment Security

محیط نرم افزار که به آن به عنوان یک نرم افزار کتابخانه ای نیز گفته می شود شامل کد، کلاس ها، رویه ها، اسکرپت ها، داده های پیکربندی، زیرشاخه ها، تعریف های کلان، متغیرهای جهانی و فرمت ها هستند. نرم افزارهای کتابخانه باید با استفاده از روش های کدگذاری امن ساخته شده و به درستی اجرا شوند. همچنین، باید آنها را با بروزرسانی ها و پچ های امنیتی به روز نگه داشت. سرانجام، آنها باید یک ویژگی بازخورد را برای رفع مشکلات شناسایی شده در بر گیرند. کتابخانه های زبان برنامه نویسی رایج شامل C، ++C، کتابخانه کلاس Java (JCL) و استاندارد Ruby است.

متخصصان امنیت همیشه مهارت‌های لازم را ندارند تا مطمئن شوند که نرم افزار توسعه یافته دارای امنیت مناسب می‌باشد. به همین دلیل، آنها باید در جهت ارتقاء سطح آگاهی امنیتی و شناسایی متخصصانی که می‌توانند از رعایت نکات ایمنی برنامه نویسی مطمئن شوند، تلاش کنند.

اصول کد منبع Source Code Issues

ریشه بسیاری از مسائل امنیتی نرم افزار در روش‌های توسعه ضعیف هستند. با رعایت برخی اصول کدگذاری، می‌توان تعدادی از تهدیدها را به حداقل رساند. در این بخش، مباحث مربوط به کد منبع به همراه برخی از دستورالعمل‌های مربوط به فرآیندهای توسعه امن مورد بحث قرار می‌گیرد.

سرریز بافر Buffer Overflow

همانطور که در فصل ۵ مورد بحث قرار گرفت، بافر منطقه‌ای از حافظه است که در آن دستورات و داده‌ها قرار می‌گیرند تا زمانی که توسط CPU پردازش شوند. سرریز بافر وقتی اتفاق می‌افتد که داده‌های زیادی به عنوان ورودی یک فرآیند خاص پذیرفته می‌شوند. هکرها می‌توانند با ارسال داده‌های بیش از حد از این پدیده استفاده کنند، اگر هکرتواند محلی را پیدا کند که در آن بتواند دستورات را اجرا کند، می‌تواند خطایی ایجاد کند یا در برخی موارد دستورات را بر روی دستگاه اجرا کند. همه حملات برای اجرای دستورات طراحی نشده‌اند. برخی فقط رایانه را قفل کرده و از آنها به عنوان حمله DoS استفاده می‌شود. بسته‌ای که حاوی یک رشته طولانی از دستورالعمل‌های بدون عملیات یا NOP (No-Operation instructions) است که به دنبال آن یک دستور می‌آید، معمولاً نشان دهنده‌ی نوع حمله سرریز بافر به نام اسلاید NOP است. هدف این است که CPU را در وضعیتی برای یافتن مکانی که بتواند یک فرمان اجرا کند، قرار دهد. در زیر نمونه‌ای از بسته‌ای است که از یک اسنیفر مشاهده شده که در آن می‌توان یک رشته طولانی ۹۰ ثانیه را در وسط بسته مشاهده کرد که به بسته چسبیده و باعث غلبه بر آن بافر شود:

```
TCP Connection Request
---- 14/03/2015 15:40:57.910
68.144.193.124: 4560 TCP Connected ID = 1 ---- 14/03/2015 15:40:57.910
Status Code: 0 OK
68.144.193.124: 4560 TCP Data In Length 697 bytes MD5 =
19323C2EA6F5FCEE2382690100455C17
---- 14/03/2004 15:40:57.920 0000 90 90 90 90 90 90 90 90 90 90 90 90 .....
0010 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
```



```

0020 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
0030 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
0040 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
0050 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
0060 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
0070 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
0080 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
0090 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
00A0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
00B0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
00C0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
00D0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
00E0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
00F0 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
0100 90 90 90 90 90 90 90 90 90 90 90 4D 3F E3 77 .....M?.w 0110 90 90 90 90 FF 63 64 90
90 90 90 90 90 90 90 .....cd.....
0120 90 90 90 90 90 90 90 90 90 90 90 90 90 90 .....
0130 90 90 90 90 90 90 90 90 EB 10 5A 4A 33 C9 66 B9 .....ZJ3.f.
0140 66 01 80 34 0A 99 E2 FA EB 05 E8 EB FF FF FF 70 f..4.....p
0150 99 98 99 99 C3 21 95 69 64 E6 12 99 12 E9 85 34 .....!id.....4 0160 12 D9 91 12 41 12 EA A5
9A 6A 12 EF E1 9A 6A 12 ....A....j....j.
0170 E7 B9 9A 62 12 D7 8D AA 74 CF CE C8 12 A6 9A 62 ...b....t.....b
0180 12 6B F3 97 C0 6A 3F ED 91 C0 C6 1A 5E 9D DC 7B .k..j?.....^.{ 0190 70 C0 C6 C7 12 54 12
DF BD 9A 5A 48 78 9A 58 AA p....T....ZHx.X.
01A0 50 FF 12 91 12 DF 85 9A 5A 58 78 9B 9A 58 12 99 P.....ZXx..X..
01B0 9A 5A 12 63 12 6E 1A 5F 97 12 49 F3 9A C0 71 E5 .Z.c.n...I...q.
01C0 99 99 99 1A 5F 94 CB CF 66 CE 65 C3 12 41 F3 9D ....f.e..A..
01D0 C0 71 F0 99 99 99 C9 C9 C9 C9 F3 98 F3 9B 66 CE .q.....f.
01E0 69 12 41 5E 9E 9B 99 9E 24 AA 59 10 DE 9D F3 89 i.A^...$.Y....
01F0 CE CA 66 CE 6D F3 98 CA 66 CE 61 C9 C9 CA 66 CE .f.m...f.a...f.
0200 65 1A 75 DD 12 6D AA 42 F3 89 C0 10 85 17 7B 62 e.u...m.B.....{b 0210 10 DF A1 10 DF A5
10 DF D9 5E DF B5 98 98 99 99 .....^.....
0220 14 DE 89 C9 CF CA CA CA F3 98 CA CA 5E DE A5 FA .....^...
0230 F4 FD 99 14 DE A5 C9 CA 66 CE 7D C9 66 CE 71 AA .....f..f.q.
0240 59 35 1C 59 EC 60 C8 CB CF CA 66 4B C3 C0 32 7B Y5.Y.`....fK..2{ 0250 77 AA 59 5A 71 62
67 66 66 DE FC ED C9 EB F6 FA w.YZqbgff.....
0260 D8 FD FD EB FC EA EA 99 DA EB FC F8 ED FC C9 EB .....
0270 F6 FA FC EA EA D8 99 DC E1 F0 ED C9 EB F6 FA FC .....
0280 EA EA 99 D5 F6 F8 FD D5 F0 FB EB F8 EB E0 D8 99 .....
0290 EE EA AB C6 AA AB 99 CE CA D8 CA F6 FA F2 FC ED .....
02A0 D8 99 FB F0 F7 FD 99 F5 F0 EA ED FC F7 99 F8 FA .....

```

در بسیاری موارد، کلید جلوگیری از حملات سرریز بافر اعتبارسنجی ورودی Input validation است. این روش نیاز دارد که قبل از استفاده، هر ورودی از لحاظ فرمت و طول بررسی شود. سرریزهای بافر و خطاهای مرزی (وقتی ورودی از مرزهای اختصاص یافته برای ورودی فراتر رود) به عنوان یک خانواده از شرایط خطا به نام خطاهای اعتبارسنجی ورودی در نظر گرفته می‌شوند.

ورودی ناهنجار Malformed Input دسته‌ای است که در آن تمام حملات سرریز بافر جای می‌گیرد. ورودی ناهنجار هر حمله‌ای است که در آن ورودی به روشی غیرمعمول تنظیم می‌شود.

افزایش امتیازات Escalation of Privileges

فرآیند سوءاستفاده، یک اشکال یا ضعف در یک سیستم عامل است تا به کاربران اجازه دهد امتیازهایی را که نسبت به آنها حقی ندارند، دریافت کنند. از این امتیازات می‌توان برای پاک کردن فایل‌ها، مشاهده اطلاعات خصوصی یا نصب برنامه‌های ناخواسته مانند ویروس‌ها استفاده کرد.

درب پستی Backdoors

در گذر چندین بار در این کتاب، از Backdoors و Trapdoors ذکر شده است (برای مثال، فصل ۵). Backdoor یک قطعه نرم افزاری است که توسط یک هکر با استفاده از یکی از مکانیسم‌های تحویل که قبلاً در مورد آن صحبت شده نصب شده است که به وی اجازه می‌دهد تا بعداً بازگشته و به رایانه متصل شود بدون اینکه فرایند احراز هویت عادی را پشت سر بگذارد. یک درب پستی معمولاً از اقدامات کنترل دسترسی عبور می‌کند. بعضی از اپلیکیشن‌های تجاری سهواً شامل Backdoors هستند زیرا برنامه نویسان فراموش می‌کنند که آنها را قبل از انتشار به بازار حذف کنند. در بسیاری موارد، این برنامه به تعداد پورت خاصی گوش می‌دهد، و هنگامی که مهاجم سعی در اتصال به آن پورت را داشته باشد، اجازه دارد بدون احراز هویت، به آن وصل شود. به عنوان مثال Back Orifice 2000 (BO2K)، یک اسب Trojan در سطح برنامه که برای دسترسی به شبکه از حمله Backdoors استفاده کرد.

برنامه نویسان سرکش Rogue Programmers

برای کاربران عادی رایانه که اسکریپت‌هایی برای انجام کارهای روزمره خود ایجاد می‌کنند رایج است. متأسفانه، این برنامه نویسان سرکش، مسائل امنیتی را که با استفاده از چنین ابزارهایی ایجاد می‌شود، کاملاً درک نمی‌کنند. در صورت امکان، یک سازمان باید استفاده از هرگونه اسکریپت‌ها و ابزارهایی (Utilities) را که توسط برنامه نویسان آموزش دیده ایجاد نشده است، ممنوع کند. اما، اگر سازمانی گاهی به برنامه نویسی اجازه دهد، متخصصان امنیت باید مطمئن

شوند که افرادی که در حال نوشتن ابزارها و اسکریپت ها هستند، آموزش های مناسب را در شیوه های توسعه سیستم دریافت کرده اند.

کانال مخفی Covert Channel

کانال مخفی هنگامی رخ می دهد که دو فرایند، اطلاعات را به روشی منتقل می کنند که خط سیاست امنیتی سیستم را نقض می کند. دو نوع کانال پنهان ممکن است رخ دهد:

- ذخیره سازی Storage: خواندن مکان ذخیره سازی مستقیم یا غیرمستقیم توسط چندین فرآیند را درگیر می کند. این حالت معمولاً در یک مکان حافظه یا بخش مشترک دیسک در دو موضوع در سطح امنیتی مختلف رخ می دهد.
- زمان بندی Timing: یک فرآیند را قادر می سازد تا بر نرخ تأثیر بگذارد که فرایند دیگر بتواند CPU، حافظه یا منابع I/O را بدست آورد.

استفاده مجدد از شی Object Reuse

حافظه به یک فرآیند اختصاص داده می شود، مجدداً به یک فرآیند اختصاص داده می شود و سپس به یک فرآیند دیگر اختصاص می یابد. بعضی اوقات داده ها از روند قدیمی عقب می ماند و این باعث نقض امنیت می شود. اگر حافظه توسط سیستم عامل خاموش یا رونویسی نشده باشد، این داده های باقیمانده به یک فرآیند جدید منتقل می شوند و ممکن است مورد استفاده مجدد قرار بگیرند. استفاده مجدد از شی همچنین می تواند روی یک هارد دیسک یا صفحه گذاری Paging یا مبادله فایل رخ دهد.

کد سیار Mobile Code

همانطور که قبلاً نیز گفته شد، کد سیار محتوای اجرایی است که از یک منبع راه دور به یک میزبان محلی در سراسر شبکه منتقل می شود و در میزبان محلی اجرا می شود. کد سیار می تواند از منابع مختلفی از جمله صفحات وب و پیام های ایمیل تهیه شود. امروزه اجرای محلی کد منبع از راه دور یک دغدغه امنیتی برای هر سازمان است. کد سیار مسئله امنیتی بی نظیری را ارائه می دهد زیرا اغلب یک موضوع به نمایندگی از خودش یا به نمایندگی از دیگری عمل می کند. برای تعریف اینکه کدام یک از این درخواست ها مجاز یا رد می شوند باید کنترل های امنیتی انجام شود.

زمان بررسی / زمان استفاده (TOC / TOU) Time of Check/Time of Use

حمله TOC یا TOU هنگامی رخ می‌دهد که یک کنترل بین زمان تغییر محتوای یک متغیر و زمان استفاده متغیر تغییر کند. به عنوان مثال، کاربر صبح وارد سیستم می‌شود و تمام مجوزهای مورد نیاز خود را برای ورود به سیستم به وی می‌دهد. بعداً در همان روز، کاربر به موقعیت دیگری در شرکت منتقل می‌شود و مجوزهای وی در سیستم تغییر می‌یابد. با این حال، کاربر از سیستم خارج نمی‌شود، بنابراین او همچنان مجوزهای قدیمی را بر اساس ورود اصلی خود دارد. برای جلوگیری از بروز این نوع مشکل، متخصصان امنیت باید تأیید هویت اجباری دوره‌ای را انجام دهند تا اطمینان حاصل شود که کاربران و سیستم‌ها در فواصل منظم در طول روز مجدداً تأیید می‌شوند.

ابزارهای تجزیه و تحلیل کد منبع Source Code Analysis Tools

ابزارهای تجزیه و تحلیل کد منبع یا نسخه‌های کامپایل شده کد را برای تعیین نقص امنیتی تجزیه و تحلیل می‌کنند. در حالی که این ابزارها معمولاً هر نقص امنیتی را پیدا نمی‌کنند و اغلب برخی از عناصر را که عیب نیستند، عیب می‌دانند، اما هنوز هم در هدف قرار دادن کد مربوط به امنیت به برنامه نویسان کمک می‌کنند. متخصصان امنیت باید با برنامه نویسان همکاری نزدیکی داشته باشند تا مطمئن شوند از ابزارهای تحلیل کد منبع در کل چرخه عمر توسعه نرم افزار استفاده می‌شود.

ابزارهای تجزیه و تحلیل کد منبع با انواع مختلفی از نرم افزار کار می‌کنند و اغلب قابل اجرا هستند. آنها در تشخیص مسائل متداول مانند سرریز بافر و تزریق SQL بسیار خوب عمل می‌کنند. آنها همچنین فایل‌های منبع دقیق و شماره‌های خطی را که نقص‌های احتمالی در آن قرار دارند برجسته می‌کنند. با این حال، همیشه همه مسائل امنیتی را نمی‌یابند، زیرا بسیاری از مسائل به سختی قابل تشخیص است. این ابزارها همچنین تعداد زیادی از موارد مثبت کاذب را گزارش می‌دهند. ابزارهای تجزیه و تحلیل کد منبع معمولاً مسائل مربوط به پیکربندی را پیدا نمی‌کنند. بسیاری از ابزارهای تجزیه و تحلیل کد منبع نمی‌توانند کدی را که نمی‌تواند گردآوری شود، تجزیه و تحلیل کنند.

ابزارهای متداول تجزیه و تحلیل کد منبع باز شامل FxCop و PreFast برای مایکروسافت، Google CodeSearchDiggity و FindBugs برای Java است. ابزارهای تجاری نیز موجود می باشد.

امنیت مخزن کد Code Repository Security

متخصصان امنیت باید در هنگام تهیه، استفاده و ذخیره در شرکت، به امنیت کد توجه داشته باشند. متخصصان امنیت باید اقدامات امنیتی را برای تأمین امنیت فیزیکی، امنیت سیستم، امنیت عملیاتی و امنیت نرم افزار ایجاد کنند. علاوه بر این، باید دستورالعمل های ارتباطی ایجاد شود، از جمله دستورالعمل های استفاده از رمزگذاری. تهیه نسخه پشتیبان باید به طور مرتب و ایمن ذخیره شود. تعداد محدودی از کارمندان باید به مخزن کد دسترسی پیدا کنند.

واسط امنیت برنامه نویسی برنامه کاربردی Application Programming Interface Security

حتی مطمئن ترین دستگاه ها نوعی واسط برنامه نویسی برنامه کاربردی API دارند که برای انجام کارها استفاده می شود. متأسفانه، افراد غیر قابل اعتماد از همان API ها برای انجام کارهای نامشخص استفاده می کنند. API ها در اینترنت اشیاء IoT استفاده می شوند تا دستگاه ها بتوانند با کاربر صحبت کرده بدون اینکه کاربران حتی بدانند که در آنجا هستند. API ها برای کنترل و نظارت بر مواردی که هر روز از آن استفاده می کنیم، از جمله باند Fitness، ترموستات خانگی، روشنایی و اتومبیل استفاده می شود.

امنیت جامع باید از طیف دستگاه های موجود در محیط کار دیجیتال، از جمله برنامه ها و API ها محافظت کنند. امنیت API برای سازمانی که در بحران دارایی های دیجیتال است، بسیار مهم است.

دستورالعمل های ارائه امنیت API شامل موارد زیر است:

- از همان کنترل های امنیتی API ها برای هر برنامه وب در شرکت استفاده شود.
- از کد تأیید پیام براساس هش (HMAC) استفاده شود.
- هنگام عبور از کلیدهای ایستا از رمزگذاری استفاده شود.
- برای اجرای راه حل های امنیتی برای API از یک چارچوب یا یک کتابخانه موجود استفاده شود.

- رمزگذاری گذر واژه به جای تأیید هویت مبتنی بر کلید، پیاده سازی شود.

تهدیدات نرم افزار Software Threats

تهدیدات نرم افزار یا نرم افزارهای مخرب نیز می توانند به شیوه کد نویسی یا توسعه نرم افزار ایجاد شوند. پیروی از توسعه بهترین شیوه ها می تواند به جلوگیری از ایجاد ناخواسته مسائل امنیتی هنگام ایجاد نرم افزار کمک کند. تهدیدهای نرم افزاری همچنین از طریق بدافزار قابل معرفی است. در این بخش، موارد رمزگذاری بدافزار و نرم افزار و همچنین گزینه هایی برای کاهش تهدید مورد بحث قرار می گیرد.

بد افزار Malware

نرم افزار مخرب Malicious software (یا بدافزار) هر نرم افزاری که به رایانه آسیب می رساند، داده ها را حذف می کند، یا اقداماتی که کاربر اجازه نداده را انجام می دهد. بدافزار شامل طیف گسترده ای از انواع نرم افزارهای مخرب، می باشد. احتمالاً درباره ویروس ها شنیده اید که باید از آنها آگاه باشید.

بدافزارها موارد زیر را شامل می شود:

- ✓ ویروس Virus
- بخش بوت ویروس Boot sector virus
- ویروس انگلی Parasitic virus
- ویروس مخفی کاری Stealth virus
- ویروس پلی مورفیک Polymorphic virus
- ماکرو ویروس Macro virus
- ویروس چند طرفه Multipartite virus
- ✓ کرم Worm
- ✓ اسب تروجان Trojan horse
- ✓ بمب منطقی Logic bomb
- ✓ جاسوسی / نرم افزارهای تبلیغاتی مزاحم Spyware/adware
- ✓ Botnet
- ✓ باج افزار Ransomware

Rootkit ✓

ویروس Virus

ویروس یک برنامه خود تکرار است که نرم افزار را آلوده می کند. از یک برنامه میزبان برای تولید و تحویل بار خود استفاده می کند و به طور معمول خود را به یک فایل متصل می کند. از این نظر با کرم متفاوت است که معمولاً به کاربر نیاز دارد تا برای گسترش آن در سایر رایانه ها کمک کند. لیست زیر انواع ویروس را به همراه شرح مختصری از هریک نشان می دهد.

- **بخش بوت Boot sector:** این نوع ویروس بخش بوت رایانه را آلوده می کند و فایل ها را رونویسی می کند یا کدها را در این بخش نصب می کند تا ویروس در هنگام راه اندازی سیستم شروع شود.
- **انگلی Parasitic:** این نوع ویروس خود را به یک فایل، معمولاً یک فایل اجرایی متصل می کند و سپس هنگام استفاده از برنامه، بار Payload را تحویل می دهد.
- **مخفیکاری Stealth:** این نوع ویروس اصلاحاتی را که در سیستم انجام می دهد پنهان می کند تا از تشخیص جلوگیری کند.
- **چندشکل Polymorphic:** این نوع ویروس نسخه هایی از خودش را ایجاد کرده و سپس در آن نسخه ها تغییراتی ایجاد می کند. این کار را به امید جلوگیری از شناسایی توسط آنتی ویروس انجام می دهد.
- **ماکرو Macro:** این نوع ویروس برنامه های نوشته شده در Word، Basic، Visual Basic یا VBScript را که برای خودکار سازی عملکرد استفاده می شود، آلوده می کند. این ویروس ها فایل های مایکروسافت آفیس را آلوده کرده و به راحتی ایجاد می شوند زیرا زبان اصلی برای استفاده ساده و قابل مشاهده است. این نوع ویروس ها خیلی خطرناک هستند زیرا سیستم عامل خود را آلوده می کنند. آنها همچنین می توانند بین سیستم عامل های مختلف منتقل شوند زیرا زبانها پلتفرم مستقل هستند.
- **چند جزئی Multipartite:** در ابتدا، این ویروس ها می توانند فایل های برنامه و بخش های بوت را آلوده کنند. این اصطلاح اکنون به معنای این است که ویروس می تواند بیش از یک نوع شیء را آلوده کند و یا می تواند بیش از یک راه را آلوده کند.

- *آلوده کننده فایل* یا سیستم *File or systems infector*: آلوده کننده فایل ها فایل های برنامه ها را آلوده می کنند، و آلوده کننده سیستم فایل های برنامه سیستم را آلوده می کنند.
- *همراه* *Companion*: این نوع ویروس از لحاظ فیزیکی فایل مورد نظر را لمس نمی کند. از آن به عنوان ویروس تخم ریزی *Spawn virus* نیز یاد می شود.
- *ایمیل* *Email*: این نوع ویروس به طور خاص از یک سیستم ایمیل برای گسترش خود استفاده می کند زیرا از عملکرد سیستم ایمیل آگاهی دارد. آگاهی از عملکردهای این نوع ویروس امکان استفاده از تمام قابلیت های سیستم ایمیل را می دهد.
- *اسکرپت* *Script*: این نوع ویروس یک فایل مستقل است که توسط یک مفسر قابل پیاده سازی می باشد.

کرم Worm

کرم نوعی بدافزار است که می تواند بدون کمک کاربر گسترش یابد و یک برنامه کوچک است که، مانند ویروس، برای تحویل بار *Payload* استفاده می شود. یک راه برای کمک به کاهش اثرات کرمها، تعیین محدودیت هایی در به اشتراک گذاری، نوشتن و اجرای برنامه ها است.

اسب تروجان Trojan Horse

اسب تروجان یک برنامه یا اپلیکیشن سرکش است که به نظر می رسد که برای انجام یک کار می باشد اما در واقع قصد دیگری با اجرای آن دارد. به عنوان مثال، آنچه که به نظر می رسد برنامه محافظ صفحه نمایش است، واقعاً ممکن است یک اسب تروجان باشد. هنگامی که کاربر ناخواسته از برنامه استفاده می کند، بار *Payload* خود را اجرا می کند، که می تواند حذف فایل ها یا ایجاد پشتیبان باشد. *Backdoors* روش های جایگزینی برای دسترسی به رایانه ای که در آینده تشخیص داده نمی شود، می باشد.

یک نوع از اهداف تروجان، تلاش برای دسترسی و استفاده از کارتهای هوشمند است. یک اقدام متقابل برای جلوگیری از این حمله، استفاده از معماری "دراپور تک دسترسی دستگاه - Single Access Device Driver" است. با استفاده از این روش، سیستم عامل تنها به یک برنامه اجازه می دهد تا در هر زمان معینی به دستگاه سریال (کارت هوشمند) دسترسی داشته باشد. راه دیگر برای جلوگیری از حمله استفاده از کارت هوشمند است که یک سیاست الگوی "یک استفاده از

کلید خصوصی برای ورود PIN را اعمال می کند. در این مدل، کاربر باید هر بار که از کلید خصوصی استفاده می کند، پین خود را وارد کند، در نتیجه اسب Trojan به این کلید دسترسی پیدا نخواهد کرد.

بمب منطقی Logic Bomb

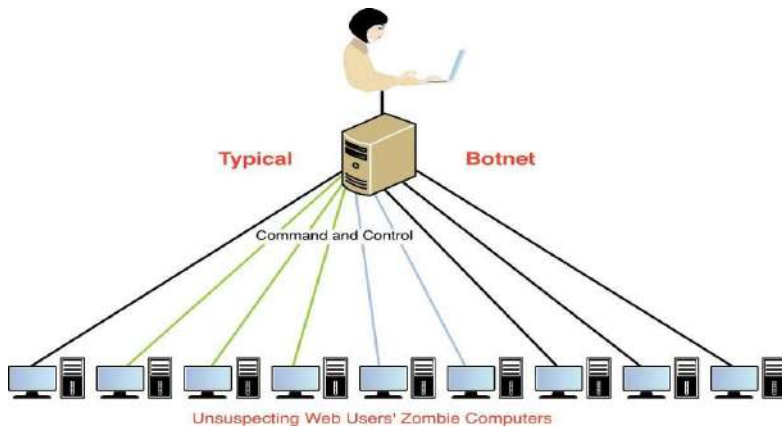
بمب منطقی نوعی بدافزار است که هنگام وقوع یک رخداد خاص، اجرا می شود. به عنوان مثال، این رخداد می تواند زمانی از روز یا یک تاریخ خاص باشد یا اولین باری باشد که شما Notepad.exe را باز می کنید. برخی از بمب های منطقی هنگام انجام جرم شناسی رایانه ای اجرا می شوند، و در این صورت ممکن است بمب تمام مدارک دیجیتالی را حذف کند.

ابزار جاسوسی / ابزارهای تبلیغاتی Spyware/Adware

ابزارهای تبلیغاتی مزاحم واقعاً چیزی را سرقت نمی کنند، اما مصرف اینترنت شما را دنبال کرده و در تلاش برای تنظیم تبلیغات و ارسال ایمیل های ناخواسته با توجه علایق شما هستند. Spyware همچنین فعالیتهای شما را ردیابی می کند و همچنین می تواند اطلاعات شخصی را که می تواند منجر به سرقت هویت شود، جمع آوری کند. در برخی موارد، ابزار جاسوسی حتی می تواند رایانه را برای نصب نرم افزار و تغییر تنظیمات راهنمایی کنند.

Botnet

باتنت نوعی بدافزار است که از طریق ایمیل های آلوده، دانلود از وب سایت ها، اسب های تروجان و رسانه های مشترک، خود را بر روی تعداد زیادی رایانه نصب می کند. پس از نصب، ربات قابلیت اتصال مجدد به رایانه هکر را دارد. پس از آن، سرور وی تمام ربات های مستقر در این ماشین ها را کنترل می کند. در زمان تعیین شده، هکر ممکن است رباتها را برای انجام برخی کارها هدایت کند، از جمله برای هدایت کلیه دستگاهها برای ارسال پیامهای اسپم، حمله DoS یا انجام فیشینگ یا هر تعدادی عملیات مخرب. به مجموعه رایانه هایی که با هم فعالیت می کنند Botnet گفته می شود و رایانه های شخصی را زامبی zombie می نامند. شکل ۸-۸ این رابطه را نشان می دهد.



شکل ۸-۸ Botnet

Rootkit

مجموعه‌ای از ابزارهایی است که هکر می‌تواند بعد از اینکه موفق به دستیابی و دسترسی به امتیازات خود ادمین شد، از طریق رایانه از آنها استفاده کند. این نام از حساب root، قدرتمندترین حساب در سیستم عامل‌های مبتنی بر UNIX دریافت شده است. ابزارهای Rootkit ممکن است شامل در پشتی Backdoor برای دسترسی هکرها باشد. Rootkit یکی از سخت‌ترین نوع بدافزارها برای از بین بردن می‌باشد و در بسیاری از موارد فقط با بازسازی دیسک سخت به طور کامل می‌تواند آن را حذف کرد.

موارد زیر برخی از کارهایی است که یک Rootkit می‌تواند انجام دهد:

- نصب یک Backdoor
- حذف همه ورودی‌ها از log امنیتی (پاک کردن log)
- ابزارهای پیش فرض با نسخه‌های اصلی جایگزین شود (برنامه‌های Trojaned)
- تغییرات هسته مخرب صورت گیرد.

Ransomware

بدافزاری است که از دسترسی کاربران به سیستم‌های خود جلوگیری کرده یا آنها را محدود می‌کند. از این لحاظ باج افزار Ransomware نامیده می‌شود زیرا قربانیان خود را مجبور می‌کنند از طریق برخی از روش‌های پرداخت آنلاین، باج بدهند تا مجدداً به سیستم‌های خود دسترسی پیدا کنند یا داده‌های خود را پس بگیرند.

محافظت از بدافزار Malware Protection

به طور کلی سازمان ها و افراد در مبارزه با بدافزار کاملاً درمانده نیستند. برنامه ها و عملکردها می توانند به کاهش آسیب های بدافزار کمک کنند. در این بخش برخی از راه های محافظت از شبکه در برابر بدافزارها مورد بحث قرار گرفته است.

نرم افزار آنتی ویروس Antivirus Software

اولین خط دفاعی نرم افزار آنتی ویروس است. این نرم افزار برای شناسایی ویروس ها، تروجان ها و کرم ها و حذف آنها یا حداقل قرنطینه کردن آنها تا زمان حذف آنها طراحی شده است. این فرایند شناسایی مستلزم آن است که به طور مکرر فایل های تعریف نرم افزار را به روز کنید زیرا این فایل ها امکان شناسایی آخرین ویروس ها را برای نرم افزار فراهم می کند. اگر ویروس جدیدی ایجاد شده باشد که هنوز در لیست مشخص نشده باشد حفاظت نمی شود، وقتی حفاظت صورت می گیرد که فایل جدید که حاوی لیست جدید ویروسها می باشد دانلود شود.

نرم افزار ضد بدافزار Anti-malware Software

تقریباً مربوط به بسته نرم افزاری و یا در بعضی موارد بخشی از همان بسته نرم افزاری است، نرم افزارهای ضد بدافزار روی انواع دیگر بدافزارها، مانند نرم افزارهای تبلیغاتی مزاحم و نرم افزار جاسوسی متمرکز شده اند. روشی برای کمک به جلوگیری از آلودگی بدافزار، آموزش کاربر با رفتار مناسب هنگام استفاده از اینترنت است. به همین دلیل، آموزش کاربر در شیوه های ایمن بخشی ضروری برای جلوگیری از بدافزار است که باید بخشی از سیاست های امنیتی باشد.

انواع اسکن Scanning Types

سه نوع عمده اسکن برای بدافزارها یا ویروس ها رخ می دهد: اسکن امضا شده شناخته شده Known Signature Scanning، نظارت بر فعالیت Activity Monitoring و تشخیص تغییر Change Detection. با اسکن امضا شناخته شده، پایگاه داده از امضاهای بدافزار نگهداری می کند. هنگامی که اسکن ها اتفاق می افتد، به دنبال مطابقت با امضا در پایگاه داده هستند. ناظر با نظارت بر فعالیت، فعالیت مشکوک را مشاهده می کند. با تشخیص تغییر، ردیابی فایل ها و پیکربندی را

بررسی کرده، اطلاعات را ذخیره کرده و اطلاعات ذخیره شده را در برابر پیکربندی با تاریخ بعدی مقایسه می‌کند. معمولاً مقادیر مجموع Checksum Values را شامل می‌شود.

سیاست‌های امنیتی Security Policies

سیاست‌های امنیتی به طور مفصل در فصل ۱، "امنیت و مدیریت ریسک" آورده شد، اما ذکر این نکته حائز اهمیت است که تشویق و یا نیاز به مرور امن Safe browsing و شیوه‌های دست زدن به داده‌ها باید در سیاست امنیتی سازمان تنظیم شود. اهمیت مواردی که در این سیاست تأکید می‌شود و شاید در آموزش برای کاربران گنجانده شود شامل:

- بروزرسانی‌های آنتی ویروس و ضد بدافزار
- گزارش هرگونه خطای مربوط به عدم بروزرسانی در دستگاه کاربر
- گزارش هرگونه رفتار عجیب رایانه‌ای که ممکن است نشان دهنده آلوده شدن توسط ویروس باشد.

مکانیسم‌های محافظت از نرم افزار

در سال ۱۹۷۲، مرکز مطالعات برنامه ریزی فناوری امنیت رایانه، به منظور تشریح الزامات پایه‌ای و اساسی امنیت سیستم‌های خریداری شده توسط دولت آمریکا مأمور شد. سرانجام این امر منجر به معیارهای ارزیابی سیستم رایانه‌ای معتبر یا کتاب نارنجی شد (که با جزئیات بیشتر در فصل ۳، "مهندسی امنیت" مورد بحث قرار گرفت). در این بخش برخی از اصول اصلی در کتاب نارنجی تعریف شده است:

- پایگاه کامپیوتری قابل اعتماد *Trusted computer base (TCB)*: شامل مؤلفه‌هایی (سخت افزاری، سیستم عامل یا نرم افزار) است که به آنها برای اجرای سیاست‌های امنیتی سیستم اعتماد می‌شود و در صورت به خطر افتادن، ویژگی‌های امنیتی کل سیستم را به خطر می‌اندازد. ناظر مرجع یک مؤلفه اصلی TCB است. این اصطلاح از کتاب نارنجی گرفته شده است. کلیه تغییرات در TCB باید ممیزی و کنترل شوند که نمونه‌ای از کنترل مدیریت پیکربندی است.
- محیط امنیتی *Security perimeter*: مرز تقسیم کننده بین قسمت‌های قابل اعتماد سیستم و قسمت‌های غیر قابل اعتماد است. طبق بهترین شیوه‌های طراحی امنیت،

مؤلفه هایی که در این مرز قرار دارند (بدان معناست که آنها در TCB قرار دارند) هرگز نباید به مؤلفه هایی غیرمستقیم اجازه دسترسی به منابع مهم را به روشی ناامن بدهند.

- **ناظر مرجع** *Reference monitor*: یک ناظر مرجع یک مؤلفه سیستم است که کنترل های دسترسی را روی یک شی انجام می دهد. این یک مفهوم کنترل دسترسی است که به یک ماشین انتزاعی *Abstract Machine* اطلاق می شود که واسطه همه دسترسی به اشیاء توسط موضوعات است. این کار برای دور زدن مشکلات در رویکردهای کلاسیک به امنیت رایانه با محدود کردن خسارات ناشی از برنامه های مخرب معرفی شده است. ریسک امنیتی ایجاد شده توسط یک کانال مخفی *Covert Channel* اینگونه می باشد که عملکردهای ناظر مرجع را دور می زند. ناظر مرجع باید ایزوله بودن، کامل بودن و صحت را نشان دهد. جداسازی به دلیل موارد زیر ضروری است:

ناظر مرجع برای دسترسی عمومی نمی تواند موجود باشد. هرچه میزان دسترسی کمتر باشد، بهتر است.

ناظر مرجع برای ارائه کل اطلاعات و چرخه پردازش باید دارای حس کامل بودن باشد.

ناظر مرجع باید قابل تأیید باشد تا عملکردهای امنیتی، ممیزی و حسابداری را ارائه دهد.

- **هسته امنیتی** *Security kernel*: هسته امنیتی سخت افزار، سیستم عامل و عناصر نرم افزاری TCB است که مفهوم ناظر مرجع را پیاده سازی می کند. این یک مفهوم کنترل دسترسی است و نه یک مؤلفه فیزیکی واقعی. هسته امنیتی باید تا حد امکان کوچک باشد تا به راحتی اثبات باشد. هسته امنیتی روابط دسترسی مجاز بین موضوعات و اشیاء سیستم را مطابق با ناظر مرجع تنظیم می کند. در حین انجام این نقش، همه دسترسی ها باید با تدبیر صورت گیرد، و از قابل تغییر بودن و معتبر بودن محافظت شود.

ارزیابی اثربخشی امنیت نرم افزار Assess Software Security Effectiveness

علیرغم اینکه یک برنامه نرم افزاری از طرف شخص ثالث خریداری شده یا در خانه توسعه یافته است، امکان بررسی و اثبات چگونگی امنیت برنامه می تواند مفید باشد. دو روش برای دستیابی به این امر، ممیزی در مورد عملکرد برنامه و تعیین اینکه آیا وی این اقدامات نا امن را انجام می دهد یا ارزیابی آن از طریق یک فرایند رسمی است. این بخش دو رویکرد رسمی را در بر می گیرد.

ممیزی و ورود به سیستم Auditing and Logging

رویکرد دیگر و روشی که پس از معرفی نرم افزار به محیط باید ادامه یابد، ممیزی مداوم از عملکردهای آن و بررسی منظم داده‌های ممیزی است. با نظارت بر فایل‌های ممیزی، می‌توان نقاط ضعف امنیتی را که در ابتدا آشکار نبوده یا ممکن است تاکنون گزارش نشده باشند، شناسایی کرد. علاوه بر این، هرگونه تغییر و تحول توسط log ممیزی ثبت می‌شود و سپس می‌توان آن را بررسی کرد تا اطمینان حاصل شود که هیچ گونه مسئله امنیتی با تغییر ایجاد نشده است.

تجزیه و تحلیل و کاهش ریسک Risk Analysis and Mitigation

تجزیه و تحلیل و مدیریت ریسک به طور کامل در فصل ۱ پوشش داده شده است. از آنجا که مدیریت ریسک یک فرایند در حال انجام است، باید به عنوان بخشی از هرگونه توسعه نرم افزار نیز گنجانده شود. تجزیه و تحلیل ریسک خطرات ایجاد شده را تعیین می‌کند، در حالی که کاهش ریسک برای کاهش اثرات ریسک‌های شناسایی شده اقدام می‌کند. متخصصان امنیت باید موارد زیر را به عنوان بخشی از تجزیه و تحلیل ریسک توسعه نرم افزار و استراتژی کاهش انجام دهند:

ادغام تجزیه و تحلیل ریسک و کاهش در چرخه عمر توسعه نرم افزار.
از روشهای تحلیل ریسک کیفی، کمی و هیبریدی بر اساس روشهای استاندارد ریسک پذیزی استفاده شود.
نقاط ضعفی را که در ارزیابی ریسک، مدیریت تغییر و نظارت مداوم کشف شده است، ردیابی و مدیریت شود.

از آنجا که نرم افزار غالباً دارای آسیب پذیری هایی است که تا زمان عملی شدن این نرم افزار کشف نمی‌شوند، متخصصان امنیت باید مطمئن شوند که در صورت لزوم یک فرایند مدیریت پیچ مستند شده و به منظور کاهش ریسک اجرا می‌شود، و شامل استفاده از یک فرایند کنترل تغییر، آزمایش هرگونه پیچ، نگه داشتن نسخه پشتیبان کار، زمانبندی خرابی تولید و ایجاد یک برنامه برگشت است. قبل از استقرار هرگونه پیچ، باید به پرسنل راهنما و مرکز خدمات و گروههای اصلی کاربر اطلاع داده شود. هنگامی که پیچها مستقر می‌شوند، رایانه‌ها و دستگاهها با حداقل بحران ابتدا باید پیچ را دریافت کنند و از طریق سلسله مراتبی حرکت کرده تا اینکه مهمترین رایانه‌ها و دستگاهها بهم متصل شوند.

پس از یکبار استقرار کاهش ها، معمولاً به عنوان بخشی از تضمین کیفیت و تست، مورد آزمایش و تأیید قرار می گیرند. هرگونه کاهش ریسک که به اتمام رسیده باید توسط یک گروه مستقل تأیید شود که توسعه دهنده یا مالک سیستم نیستند. برای اطمینان از یکپارچگی کد، برای تعیین اینکه چه کسی کد را ایجاد کرده است و تعیین هدف آن، باید از توسعه دهندگان استفاده شود تا از امضای کد استفاده کنند. گواهینامه های امضا شده با کد، گواهی های دیجیتالی هستند که تضمین می کنند کد تغییر نکرده است. با امضای کد، سازمانها می توانند تشخیص دهند که آیا کد توسط یک نهاد غیر از امضاکننده اصلی اصلاح شده است یا خیر. امضای کد در درجه اول کد در حال اجرا را پوشش می دهد، نه کد ذخیره شده. در حالی که امضای کد، یکپارچگی کد را تأیید می کند، نمی تواند آزادی در برابر آسیب پذیری های امنیتی را تضمین کند یا اینکه یک برنامه در حین پیاده سازی کد ناامن یا بدون تغییر را بار گذاری load کند.

آزمون رگرسیون و پذیرش Regression and Acceptance Testing

هرگونه تغییر یا اضافه کردن به نرم افزار باید تحت آزمون رگرسیون و پذیرش قرار بگیرد. آزمون رگرسیون تأیید می کند که نرم افزار همانطور که باید رفتار می کند. آزمون رگرسیون حفره هایی را که ممکن است به طور تصادفی در کاندیدای جدید ساخت یا انتشار، معرفی شده باشد، بدست می آورد. آزمون پذیرش تأیید می کند که آیا نرم افزار کاری را انجام داده که کاربر نهایی انتظار دارد آن را انجام دهد. آزمون پذیرش از نظر ماهیتی رسمی تر است و در واقع عملکرد کاربران را بر اساس یک داستان کاربر آزمایش می کند.

تأثیر امنیتی نرم افزارهای اکتسابی Security Impact of Acquired Software

سازمانها معمولاً برای توسعه نرم افزارهای سفارشی، نرم افزارهای تجاری خریداری می کنند یا با سازمانهای دیگر قرارداد می بندند. متخصصان امنیت باید مطمئن شوند که سازمان تأثیر امنیتی هر نرم افزار خریداری شده را درک می کند.

فرآیند دستیابی به نرم افزار دارای چهار مرحله زیر است:

- ۱- برنامه ریزی Planning: در طی این مرحله، سازمان نیازها را ارزیابی می کند، نیازهای نرم افزاری را توسعه داده، استراتژی اکتساب را ایجاد کرده و معیارهای ارزشیابی و برنامه را تدوین می کند.

- ۲- *پیمانکاری Contracting*: پس از اتمام برنامه ریزی، سازمان درخواستی را برای طرح پیشنهادی (Request for proposal (RFP یا سایر فرم‌های درخواست تهیه کننده ایجاد کرده، پیشنهادات تهیه کننده را ارزیابی می‌کند و با فروشنده منتخب در مورد قرارداد نهایی مذاکره می‌کند.
- ۳- *نظارت و پذیرش Monitoring and accepting*: پس از انعقاد قرارداد، سازمان برنامه کار قرارداد را تعیین می‌کند، رویه‌های کنترل تغییر را اجرا کرده و تحویل نرم افزار را بررسی و قبول می‌کند.
- ۴- *پیگیری Follow-up*: وقتی نرم افزار در دسترس است، سازمان باید نرم افزار را از جمله در موارد مدیریت ریسک و تغییرات حفظ کند. در بعضی از موارد ممکن است لازم باشد سازمان نرم افزار را رد کند.
- یک متخصص امنیت باید در فرایند تضمین نرم افزار شرکت کرده تا از خطاهای غیر عمدی، کد مخرب، سرقت اطلاعات و تغییرات غیرمجاز محصول یا عوامل درج شده مطمئن شود.

روبین آبرناتی و تروی مک میلان

امنیت سیستم های اطلاعاتی



مرجع کامل آزمون **CISSP**

ترجمه: دکتر سید سامان کریمی

امنیت سیستم های اطلاعاتی
(مرجع کامل آزمون CISSP)

ترجمه: دکتر سید سامان کریمی



آزمون و مدرک بین المللی CISSP مخفف Certified Information Systems Security Professional متعلق به کنسرسیوم امنیت اطلاعات International Information Systems Security Certification Consortium, Inc² (ISC) می باشد. این شرکت در سال ۱۹۸۹ به عنوان یک کنسرسیوم غیر انتفاعی از پیشروان صنعت و با هدف عرضه مدارک بین المللی در زمینه امنیت اطلاعات در هر سطح و گرایشی آغاز به کار نمود. در سال ۱۹۹۲ کنسرسیوم مذکور اقدام به طرح مدرکی به نام CISSP نمود که به عنوان مدرکی بسیار کاربردی و مفید در شاخه امنیت اطلاعات، استراتژی های تأمین امنیت شبکه را ارائه می نماید. مدرک CISSP به دلیل عدم وابستگی آن به محصولی خاص، به عنوان یک عنصر کلیدی در ارزشیابی داوطلبان کار در مؤسسات بزرگ و سیستم های سازمانی شناخته می شود. افراد دارای مدرک CISSP دارای توانایی لازم در طراحی و پیاده سازی سیاست های کلان امنیتی می باشند. این افراد دارای درک کامل و مستقلی از مسائل مربوط به مهندسی اجتماعی بوده و قادر به ایجاد امنیت اطلاعات در یک سازمان با ارائه خط مشی ویژه با سیاست های خاص امنیتی آن سازمان می باشند.

ارشدن

ISBN: 978-622-251-767-0



9 786222 517670