CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-1-best_practices_and_secure_configuration_guides
Title: Best Practices and Secure Configuration Guides
Subtitle: CompTIA Security+ (SY0-501)

3.1 Best Practices and Secure Configuration Guides

- 3.1 Explain use cases and purpose for frameworks, best practices and secure configuration guides.
    - Industry-standard frameworks and reference architectures
        - Regulatory
            - Sarbanes-Oxley(SOX)- passed as a countermeasure to fraud (Eron, WorldCom,Tyco_
                - Security requirements for applications and financial data processing systems
                - Access managements, general IT controls...etc
            - Payment Card Industry-Data Security Standard
                - Protects the security of creditcard holders
                - Made up of multiple levels
                - Standards enforced are based on the PCI-DSS level
            - Health Insurance Portability and Accountability Act
                - Safe guards medical information
                - Protects personal health information or PHI
            - COBIT
                - Control Objectives for Information and Related Technology
                - is a framework developed in the mid-90s by ISACA,
                - Used to achieve Sarbanes-Oxley Compliances
            - ISO 27000 Suite
                - ISO
    - Benchmarks/secure configuration guides
        - Non-regulatory
            - NIST SP 800-***
                - National Institute of Standards and Technology
                - First published in the 90s
                - NIST 800-53 complies with the Federal Information Processing Standards
        - National vs. international
            - Governing Bodies
                - ANSI(National, promotes internationally)
                - ISO (International)
                - BSI(National+
                - British Electrotechnical Committee
                - (NERC)North American Electric Reliability Corporation (National)
            - Standards Example
                - ANSI (National)
                - ISO 27002 (International)
                - BS7799(Later adopted by ISO)
        - Industry-specific frameworks
            - Banking, Financial and Insurance
                - (IFW for Data, Process, Services)
            - Healthcare (Data)
            - Telecommunications (Data)
            - Retail (Data)
        - Platform/vendor-specific guides
            - Web server
                - Windows IIS = https://technet.microsoft.com/en-us/library/jj635855(v=ws.11).aspx
                - Linux = https://access.redhat.com/solutions/393403
                - SCW and Technet = https://technet.microsoft.com/en-us/security/jj720323.aspx
            - Operating system
            - Application server
            - Network infrastructure devices
                - Cisco = http://www.cisco.com/c/en/us/support/docs/availability/high-availability/13601-secpol.html
        - General purpose guides
    - Defense-in-depth/layered security
        - Layers
            - Layer 1 = Policies, Procedures, Awareness
            - Layer 2 = Physical Security
            - Layer 3 = Perimeter Security
                - Border Routers, Firewalls, DMZs, IDS/IPS,
            - Layer 4 = Network Security
                - Access control(NAC), network-based firewalls, anti-malware gateway, network segmentation, wireless security
            - Layer 5 = Host Security
                - Anti-malware, host-based firewalls, host-based IPS, patch management, backups

        - Layer 6 = Application Security
            - Application layer firewalls
            - Application Configuration Baselines
            - Input validation(server-side/client-side)
        - Layer 7 = Data Security
    - Vendor diversity
    - Control diversity
        - Administrative
            - Implemented through policies, procedures and quidelines
        - Technical
            - Implemented through technology
            - Firewalls, anti-malware, IDS/IPS
        - Physical(Objective 5.7)
        - Preventative(Objective 5.7)
            - Any controls that stop something from happening
            - Locks, biometric devices, mantraps
        - Deterrent(Objective 5.7)
            - Any type of control that warns an attacker to stay away and not attack
            - Lighting, Security Guards, strobe lights, security cameras
        - Detective(Objective 5.7)
            - The purpose is to uncover violations
            - Anti-malware, IDS/IPS, motion sensors
            - Alarms triggered when a door is opened
        - Corrective(Objective 5.7)
            - Restores a system or systems to the state prior to the event
            - They seek to minimize the impact to the company
            - Backup sofware, backups, snapshots, OS upgrades
        - Compensating(Objective 5.7)
            - These controls come to the assistance of controls that fail
            - Signs are deterrents but alarms compensate signs,
            - Emergency exit with sign(both are deterrents, however if and alarms are triggered then the alarm is a compensating control)
            - UPS, DR Sites
- User training