CompTIA Security+ (SY0-701) Day 4

Section 2.5: Explain the Purpose of Mitigation Techniques Used to Secure the Enterprise

Segmentation

Dividing a computer network into smaller parts to improve network performance and security.

- Separating resources
- Containment of risks
- Malicious spread reduction
- Focused monitoring

Isolation

Enforcing strict, unidirectional boundaries between IT components so that no traffic or trust can flow unchecked.

- **Multi-layer defense** – Deploy dedicated firewalls, DMZs, or sandboxes to slow down, detect, and contain breaches.
- **Reduced blast radius** – By fully separating critical assets, you prevent an attacker from reconnoitering or moving laterally.
- **Minimal attack surface** – Only the bare-minimum ports and protocols are permitted; all other paths are blocked.

Access Control

Ensuring the right people have the correct level of access to the right resources.

ACLs

- Sets of rules used to control access and enforce security policies.

  - Permit, Deny
- Regulate all data packets (traffic) as they enter or exit a zone, network, or device.

Permissions

- Define the type of access that is granted to a user or group for a resource.
  - Read, Write, Execute, Delete

Application Allow List

A list of approved applications and application components that are allowed to run on an organization's systems.

- Executable programs
- Software libraries
- Configuration files

Purpose

- Prevent malware
- Control applications
- Maintain software inventory

Patching

The process of identifying, testing, and applying updates.

- To software, operating systems, applications, and more
- Serves as a proactive defense mechanism against known vulnerabilities
- Minimizes exposure and avoids preventable compromises

Encryption

Protects sensitive information from unauthorized access and maintains confidentiality, integrity, and authenticity.

- Ensures that only authorized users can access and read the data
- Ensures that the data received originates from a trusted source

Monitoring

Provides continuous oversight and visibility into the organization’s systems.

- Continuous surveillance, threat detection, incident response, compliance management, proactive security, and performance optimization
- Continuously tracks and records security-related events and activities
- Detects and identifies security threats
- Provides valuable information for investigating and containing incidents

Least Privilege

Limits access and permissions granted to individuals, systems, and applications to the minimum necessary for them to perform tasks.

- Reduces the attack surface
- Minimizes the potential impact of security breaches and insider threats

Configuration Enforcement

Ensures that all systems, devices, and software components are configured in a secure and consistent manner.

- Maintains a secure baseline for all systems and software components
    - Prevents security vulnerabilities
    - Reduces attack surfaces
    - Maintains a strong security posture

Decommissioning

Safely retires or removes systems, devices, software, and data that are no longer needed or have reached the end of their lifecycle.

- Helps organizations reduce security risks
- Protects data
- Ensures compliance
- Maintains data privacy
- Manages IT assets effectively

Hardening Techniques

Used to strengthen the resilience of a system or network against potential vulnerabilities and threats.

- Encryption
- Installation of endpoint protection
- Host-based firewall

- Host-based intrusion prevention system
- Disabling ports/protocols
- Default password changes
- Removal of unnecessary software
- Domain 3.0 Security Architecture

Section 3.1: Compare and Contrast Security Implications of Different Architecture Models

On-Premises Security Implications

Managing, monitoring, and maintaining all resources in your own environment.

- Control and responsibility
- Customization and compliance
- Resource intensive
- Physical security requirements
- Scalability challenges

Cloud Security Applications

Offers a flexible, scalable, and cost-effective solution for storing, processing, and managing data over the internet.

- Shared Responsibility Model
- Advanced security measures
- Elasticity and scalability
- Data security concerns
- Dependence on CSP
- Access management

Cloud Security Implications

Responsibility Matrix

- **Shared Responsibility Model** – Framework used to delineate the responsibilities of CSPs and their clients.

Hybrid Considerations

- A computing environment that combines a mix of on-premises, private cloud, and public cloud services with orchestration between the platforms.
- Complex security management
- Increased attack surface
- Flexibility in security approaches
- Compliance and data sovereignty
- Network security
- Vendor diversity

Third-Party Vendors

- Diverse security standards
- Supply chain risks
- Compliance and data handling
- Vendor management

Infrastructure as Code (IaC) Security Implications

Managing and provisioning infrastructure through code.

- Automated configuration and deployment
- Rapid patch management and updates
- Version control and auditing
- Scalability and responsiveness
- Security as code

Serverless

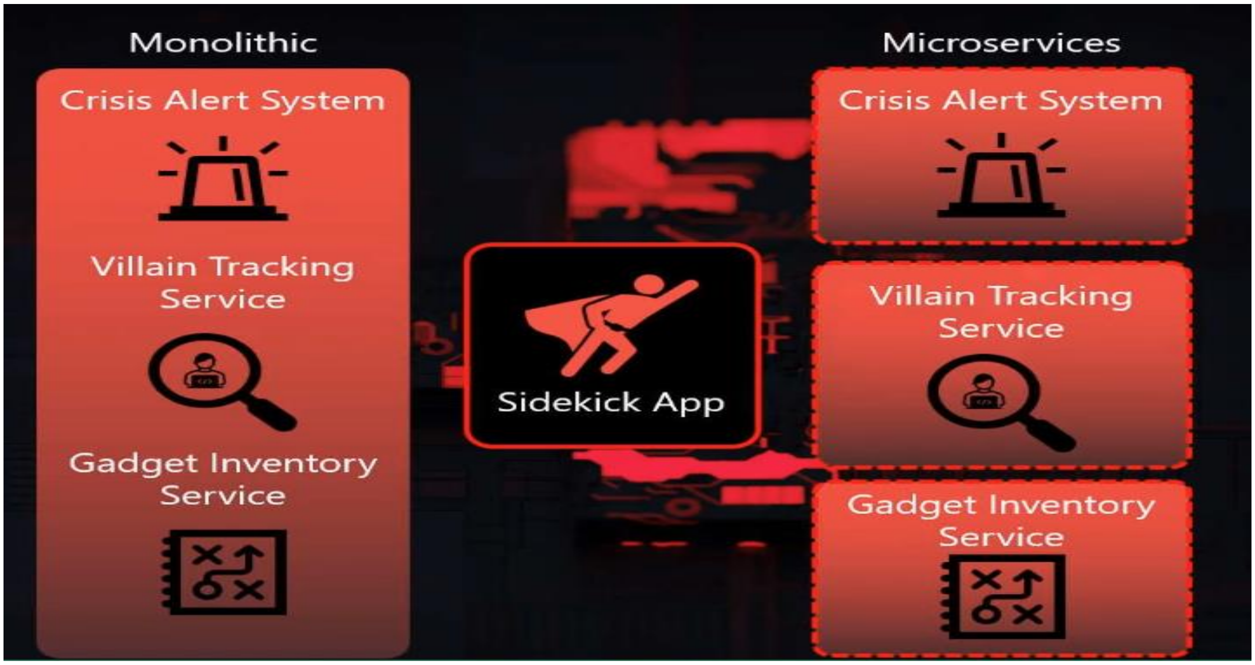
A cloud computing model where the cloud provider manages the execution of code by dynamically allocating resources as needed.

- Allows you to run applications and services without managing, monitoring, or maintaining servers or networks

Microservices Security Implications

A design approach in software development where an application is structured as a collection of loosely coupled services that are small, modular, and independently deployable, each responsible for specific functionality.

- Provides flexibility and scalability
- Security challenges include service-to-service authentication, data protection, and securing APIs



Network Infrastructure Security Implications

- **Physical Isolation**
  - Air-gapped – Physically separating secured network from less secure network (often the internet)
- **Logical Segmentation**
  - A security strategy that involves dividing a computer network into smaller, distinct subnetworks or segments to improve security, performance, and manageability.
- **Software-defined Network (SDN)**
  - A networking approach where the control plane is decoupled from the data plane, allowing network administrators to manage network services through abstraction of lower-level functionality.
  - **Security Implications:** Centralized policy enforcement improves security visibility, but creates a potential single point of failure if the SDN controller is compromised.

Centralized

- Focus on central authority, usually in a single location
- Simplifies management and oversight
- **Implication:** Easier to monitor and enforce policies, but a compromise at the central point could impact the entire network.

Decentralized

- Enhances resiliency by spreading authority across multiple units or locations
- **Implication:** Reduces risk of a single point of failure but may complicate coordination and policy enforcement.

Virtualization and Containerization Security Implications

- **Virtualization Risks:** Hypervisor attacks, VM escape, resource contention, and improper isolation between virtual machines.

- **Containerization Risks:** Insecure container images, container breakout attacks, shared kernel vulnerabilities, and lack of proper image scanning.
- **General Benefits:** Efficient resource use, rapid deployment, and scalability, but increased complexity requires strong monitoring and patching practices.

Internet of Things (IoT) Devices

- IoT architecture consists of any device embedded with electronics, software, sensors, actuators, and connectivity which enables these objects to connect and exchange data.
    - **Security Implications:**
        - Device security
        - Network security
        - Scalability of security measures
        - Data privacy and integrity
        - Patch management and updates
        - Heterogeneity of devices
        - Physical security
        - Lifecycle management
        - Interconnectivity risks (e.g., weak authentication, default credentials, poor patching)

ICS and SCADA Security Implications

- Critical infrastructure targeting
- Legacy systems and vulnerabilities
- Network connectivity risks
- Lack of regular updates
- Physical and remote access
- Insider threats
- Compliance and regulatory challenges
- Interdependency risks
- Data integrity and availability
- Highly targeted by nation-state actors
- Consider air gapping for critical components

Real-Time Operating System (RTOS) Security Implications

- A specialized operating system designed to manage hardware resources and host applications that process data as it comes in.
- Typically used in scenarios with strict time constraints where processing must be done within a defined time period.
    - **Examples of Embedded Systems Using RTOS:**
        - Medical equipment
        - Robotics
        - AI cards
- Ensures tasks are executed in a predictable and timely manner, where delay or time variance could lead to failure or hazards.
- **Security Implications:**
    - Target for specific attacks
    - Limited resources for security
    - Real-time constraints
    - Physical access and tampering
    - Network connectivity and exposure
    - Embedded system vulnerabilities

    - Compliance and certification challenges
    - Dependency on third-party components
    - Data privacy concerns

Embedded Systems Security

- A specialized computing system that performs specific functions and is integrated within a larger device or system.
- **Examples:** Automotive control systems, smart home devices, medical devices.
- **Security Implications:** Limited resources for security, difficulty in patching, reliance on vendor updates, and potential physical tampering risks.

High Availability Security Implications

- High availability ensures that a system or service remains available and operational with minimal downtime, even in the event of failures or maintenance activities.
    - Increased Attack Surface
    - Complexity of Management
    - Dependency on Network Security
    - Balance Between Availability and Security
    - Data Redundancy and Privacy Concerns

Considerations of Different Architecture Models

- **Availability** - Ensures reliable, continuous access to services and resources.
    - Vital for user experience, business continuity, and reputation.
- **Resilience** - Capacity to withstand and quickly recover from disruptions
    - Key for operational integrity and long-term system stability
- **Cost** - Encompasses both initial and ongoing expenditure
    - Balances financial constraints with performance and growth needs
- **Responsiveness** - Speed at which systems react to user inputs or requests
    - Influences user satisfaction and overall system efficiency
- **Scalability** - Ability to adapt to increased/decreased demands by scaling resources
    - Essential for handling growth and fluctuating workloads

- **Ease of Deployment** - Simplicity and speed in implementing and integrating systems
  - Reduces operational downtime and accelerates time to market
- **Risk Transference** - Shifting potential risks to third parties
  - Manages unforeseen incidents, legal, and compliance issues
- **Ease of Recovery** - Capability to quickly restore operations post-disruption
  - Crucial for minimizing downtime and data loss
- **Patch Availability** - Regular availability of updates for security and performance
  - Ensures ongoing system integrity and risk management
- **Inability to Patch** - Challenges in applying critical updates
  - Increases vulnerability and requires alternative security measures
- **Power** - Energy requirements and efficiency of the system
  - Impacts operational costs and environmental sustainability
- **Compute** - Processing power needed for tasks and applications
  - Determines performance capabilities and resource allocation

Section 3.2 Given a scenario, apply security principles to secure enterprise

Device Placement

- Place critical devices in secure, controlled-access areas
- Ensure devices are positioned to facilitate effective network segmentation.

Security Zones

- Create security zones based on the sensitivity and function of devices
- Control and monitor traffic between zones

Attack Surface

- Minimize the attack surface by reducing the number of exposed services and entry points
- Regularly update and patch all devices to close known vulnerabilities.

Connectivity

- Secure network connections using encryption and secure protocols.
- Monitor network traffic for unusual or unauthorized activity.

Failure Modes

- How systems respond to failures or security breaches
    - **Fail-open**
        - System remains operational, defaulting to maximum accessibility
        - Applied when uninterrupted service is critical
            - Risk - Potential exposure of sensitive data during system failures
    - **Fail-closed**
        - System shuts down, restricting access during failure
        - Used to protect sensitive data and resources
            - Risk - Potential disruption in services and operations

Device Attributes

- **Active** - Interact and intervene in network traffic as it occurs
- **Passive** - Monitoring and analyzing network traffic
- **Inline** - Situated directly in the path of network traffic
    - Actively inspect and modify traffic in real-time
- **Tap/Monitor**
    - Situated outside the direct path of network traffic
    - Used for traffic analysis and monitoring

Network Appliances

- **Jump Server (Bastion Host)**
    - A device set up in a DMZ/Screened Subnet to enhance remote access security.
        - Remote to the Jump Box and then connect to other devices.
- **Proxy Server** - Intermediary devices that sit between a client requesting a resource and a server providing a resource
    - Mask the identity of the client from the server
    - Relay the client request to the server

  - Cache content for clients, making future requests faster
  - Filter content requests and responses
  - Increase scalability, performance, resilience, and security of the back-end
  - Maintain session persistence with the back-end

IDS vs. IPS

- Inspect traffic flows and determine if there is anything abnormal or malicious
  - **IDS** just detects and monitors.
  - **IPS** intercepts and drops packets.
- **Signature-based** - Looks for telltale signs of known attacks
- **Stateful Protocol Analysis** - Looks for abnormal protocol use
- **Anomaly-Based/Heuristic** - Looks for unusual behavior patterns

Load Balancing

- Distributes network or application traffic across multiple servers to ensure no single server becomes overwhelmed.
  - Improves availability, fault tolerance, and overall performance.
  - Can also help mitigate denial-of-service (DoS) attacks by spreading traffic load.

Sensors

- Detect and respond to changes in an environment
- Often used for traffic analysis, intrusion detection, or environmental monitoring.

Port Security

- Implement 802.1X for network access control, ensuring only authenticated devices can connect to the network
- Use EAP as a framework for secure authentication when users access the network.

Firewall Types

- A firewall is a device that filters traffic as it moves from one area of your network to another or to an external network.

    - **Web Application Firewall (WAF)** - Protects web applications by monitoring and filtering HTTP traffic between a web application and the Internet.
    - Specifically targets application layer attacks such as SQL injection, cross-site scripting (XSS), and file inclusion.
    - Also protects against buffer overflow attacks.

Layer 4 vs. 7 Firewalls

- **Layer 4** - Primarily handle data traffic based on source/destination IP addresses, ports, and protocols.
    - Ideal for basic network security and filtering.
- **Layer 7** - Capable of inspecting and controlling application-specific traffic.
    - Provides in-depth content filtering, including the ability to block specific content within applications

Next-Generation Firewalls (NGFW)

- Evolution of Traditional Firewalls
- Traffic filtering based on applications, users, and content, not just IP addresses and ports.

Unified Threat Management (UTM)

- Provides a comprehensive security solution by combining multiple security tools (anti-malware, firewall capabilities, etc.) into a single appliance.

Secure Communication Access

Virtual Private Networks (VPNs)

- Provide encrypted connections across untrusted networks to ensure confidentiality, integrity, and authentication.

Site-to-Site VPN

- Creates secure tunnels between networks, typically used to connect branch offices to headquarters.
- Uses **IPSec** as the primary protocol suite:

    - Confidentiality with encryption
    - Integrity with hashing
    - Authentication with RSA
    - Anti-replay with sequencing

Transport Layer Security (TLS) aka Clientless VPN

- Encrypts data between web servers and clients
    - HTTPS uses TLS on top of HTTP
    - SSL is the precursor of TLS

Software-Defined Wide Area Network (SD-WAN)

- A technology that utilizes software-defined networking principles to manage and optimize the distribution of network traffic across a wide area network (WAN).
- Offers the ability to dynamically route and prioritize network traffic based on factors such as application types, network conditions, and business policies.

Secure Access Service Edge (SASE)

- Architecture that combines SD-WAN with additional security features:
    - Firewall-as-a-Service (FWaaS)
    - Secure Web Gateway (SWG)
    - Cloud Access Security Broker (CASB)
    - Data Loss Prevention (DLP)
    - Zero Trust Network Access (ZTNA)