CompTIA Security+ (SY0-701) Day 5

Domain 3.0 Security Architecture

Section 3.3 Compare and contrast concepts and strategies to protect data.

Data Types

- **Regulated**
  - Data governed by legal, contractual, or policy requirements
    - Personal Health Information (PHI)
    - Personally Identifiable Information (PII)
    - Credit Card Information (PCI DSS)
- **Trade Secret**
  - Confidential business information that provides a competitive edge.
  - Examples: Secret formulas, manufacturing processes, customer lists
- **Intellectual Property**
  - Creations of the mind, such as inventions, literary and artistic works, designs, symbols, names, and images.
    - Patents
    - Copyrights
    - Trademarks
- **Legal Information**
  - Data related to legal proceedings, advice, and other legal matters.
  - Examples: Contracts, litigation documents, legal correspondence
- **Financial Information**
  - Data concerning the financial transactions and status of individuals or organizations.
  - Examples: Credit card information, bank statements, tax records, investment details
- **Human and Non-Human Readable**
  - Encryption
  - Obfuscation
  - Tokenization

Data Classification

- **Sensitive**
  - Data that, while not top-secret, could be harmful if disclosed, requiring more protection than private data.
    - Examples: Internal communications, employee performance reviews, internal audits
- **Confidential**
  - Data intended to be kept secret within the organization, as its disclosure could cause harm or provide an advantage to competitors.
    - Examples: Trade secrets, client lists, non-public financial information, product roadmaps, M&A plans
- **Public**
  - Data that can be freely accessed and distributed without any risk of harm or breach of privacy.
    - Examples: Press releases, published government statistics
- **Restricted**
  - Highly restricted data that requires strict access controls and protection measures due to the potential for significant harm or legal repercussions if disclosed.
    - Examples: Classified government information, sensitive client data, high-value intellectual property, encryption private keys
- **Private**
  - Personal data related to an individual's personal life and not intended for public access.
    - Examples: Personal emails, contact details, social media activity, PHI, Social Security numbers
- **Critical**
  - Data essential to the functioning of an organization, whose loss or corruption would have severe consequences for business operations or security.
    - Examples: Real-time transaction ledgers, emergency response system data

Data States

- **Data in Transit** – Data actively moving from one location to another
- **Data at Rest** – Data stored on a physical medium and not actively being accessed or processed
- **Data in Use** – Data currently being processed, accessed, or manipulated by applications, users, or systems

Data Sovereignty

- Digital data is subject to the laws and governance structure of the country where it is stored.
    - **Key Considerations:**
        - Data residency (storing data within a country's borders)
        - Data localization (processing data within the country)

Geolocation

- Refers to the collection, processing, and use of data related to the physical location of individuals or devices.
- Raises concerns about privacy, security, and compliance with regulations.

Methods to Secure Data

Geographic Restrictions

- **Concept:** Controlling where data is stored, processed, and accessed based on geographic locations.
- **Purpose:** To comply with legal and regulatory requirements, manage data sovereignty, and enforce privacy controls.
- **Strategies:**
    - **Geofencing** – Implement virtual boundaries for data access.
    - **Data Residency Compliance** – Adhere to national laws governing data storage and processing.
    - **IP Address Filtering** – Restrict access based on geographical IP addresses.

Encryption

- **Concept:** Transforming data into a coded format that can be deciphered only with a specific key.
- **Purpose:** To protect data confidentiality during storage and transmission.
- **Strategies:**
    - **At Rest Encryption:** Encrypt data on hard drives and databases.
    - **In-Transit Encryption:** Use SSL/TLS for data transmitted over networks.
    - **Digital Signatures:** Provide authenticity and integrity by encrypting with the private key and verifying with the public key.

Hashing

- **Concept:** Converting data into a fixed-size hash value (string) through a one-way transformation.
- **Purpose:** To validate data integrity and authenticity.
- **Strategies:**
    - Store strong password hashes in a database.
    - Verify the integrity of stored data.
    - Validate data integrity after transmission.

Masking

- **Concept:** Replacing sensitive data with a non-sensitive equivalent that maintains the same data type and format.
- **Purpose:** To protect sensitive information while still allowing functional use of data without exposing actual sensitive content.
- **Strategies:**
    - **Dynamic Masking:** Mask data on-the-fly during access.
    - **Static Masking:** Mask data stored in databases.

Tokenization

- **Concept:** Substituting sensitive data with non-sensitive placeholders (tokens).
- **Purpose:** To secure sensitive data, such as credit card numbers, while maintaining usability in business processes.
- **Strategies:**
    - **Data Vaulting:** Store original data securely and use tokens in operational systems.
    - **Format-Preserving Tokenization:** Use tokens that maintain the format of the original data.

Obfuscation

- **Concept:** Making data or code deliberately ambiguous or unclear.
- **Purpose:** To protect sensitive information in a way that remains usable but not easily interpretable.
- **Strategies:**
    - **Code Obfuscation:** Make code difficult to understand to protect intellectual property.
    - **Data Anonymization:** Remove or alter identifying details within data.

Segmentation

- **Concept:** Dividing a network or data environment into smaller, distinct parts.
- **Purpose:** To reduce the attack surface and limit the spread of breaches.
- **Strategies:**
    - **Network Segmentation:** Divide networks into subnetworks.
    - **Database Segmentation:** Store different data types in separate databases.

Permission Restrictions

- **Concept:** Controlling who can access or manipulate data.
- **Purpose:** To ensure only authorized individuals have access to specific data, maintaining confidentiality and integrity.
- **Strategies:**
    - **Role-Based Access Control (RBAC):** Assign permissions based on organizational roles.
    - **Least Privilege Principle:** Give users the minimum level of access required for their roles.

Section 3.4: Explain the Importance of Resilience and Recovery in Security Architecture

High Availability (HA)

- **Concept:** Ensuring that systems and services remain accessible and functional despite failures.
- **Goals:**
    - Maintain uptime during hardware failures, software crashes, or other disruptions.
    - Minimize downtime and maintain business continuity.

- **Key Concepts:**
    - **Load Balancing:** Distribute workload across multiple servers or paths to prevent overloading and improve performance.
    - **Clustering:** Combine multiple servers to function as a single entity for redundancy and resilience.

Site Considerations

- **Hot Site:** Fully equipped backup location, ready within minutes.
- **Cold Site:** Space and utilities only, no hardware; ready in days to weeks.
- **Warm Site:** Some hardware present but not fully operational; ready in hours to days.

Geographic Dispersion

- **Concept:** Avoid keeping all data in a single region to reduce risk from localized disasters.

Platform Diversity

- **Concept:** Use a variety of technology platforms and systems.
- **Benefits:**
    - Reduce vendor-specific vulnerabilities.
    - Minimize single points of failure.
    - Improve resilience against targeted attacks.
    - Avoid vendor lock-in.
    - Encourage best-of-breed approaches.
    - Support compliance and regulatory requirements.

Multi-Cloud Systems

- **Concept:** Diversify application and cloud usage across multiple providers.
- **Benefits:**
    - Enhanced resilience and redundancy.
    - Avoid vendor lock-in.
    - Improve compliance and data sovereignty.
    - Diversify security postures.
    - Support scalability and flexibility.
    - Enable innovation and access to new technologies.

Continuity of Operations (COOP)

- **Concept:** Ensure critical functions continue during disruptions.
- **Goals:**
    - Build resilience against disruptions.
    - Protect critical business functions.
    - Maintain data integrity and availability.
    - Ensure compliance with regulatory requirements.
    - Minimize financial losses.

Capacity Planning

- **Concept:** Assess, forecast, and manage organizational resources to meet current and future demands.
- **Areas:**
    - People
    - Technology
    - Infrastructure

Testing

- **Tabletop Exercises:** Discussion-based role-play of potential disasters or emergencies.
    - Test incident response plans.
    - Involve key personnel in decision-making.
    - Identify gaps in existing plans.
- **Simulations:** Mimic real-world scenarios to test responses to specific threats (e.g., network breach, power failure).

Failover

- **Concept:** Switch automatically to a backup system when the primary fails.
- **Goals:**
    - Ensure business continuity.
    - Test redundancy and recovery.
    - Schedule testing to minimize operational impact.

Parallel Processing

- **Concept:** Run systems in parallel to handle load balancing and distribute processing tasks effectively.
- **Importance:**
    - Critical in high-availability environments.

Backups

- **Concept:** Essential for ensuring data availability and integrity in the face of threats.
- **Protection Against:**
    - Hardware failures
    - Human errors
    - Cyberattacks
    - Natural disasters

Types of Backup

- **Full Backup:**
    - Backs up all the data on the volume.

- **Incremental Backup:**
  - Backs up only files modified or created since the last full or incremental backup.
- **Differential Backup:**
  - Backs up only files modified or created since the last full backup.
- **Snapshot:**
  - Captures the entire state of the system, sometimes including memory and configurations, at a specific point in time.

Onsite vs. Offsite Backups

- **Onsite Backups:**
  - Stored within the same physical location as the original data; faster recovery but vulnerable to local disasters.
- **Offsite Backups:**
  - Stored at a different location; protects against site-wide events but recovery may take longer.

Frequency

- **Concept:** Frequency determines the potential data loss window (Recovery Point Objective, RPO).
  - More frequent backups mean less data loss but may increase storage and processing overhead.

Encryption

- **Concept:** Vital for protecting sensitive data from unauthorized access.
    - Ensures that even if backup data is accessed, its contents cannot be deciphered.
    - Especially important for offsite and cloud-based backups to meet compliance requirements.

Recovery

- **Concept:** Ability to efficiently restore data from backups.
    - Plans should be tested regularly to ensure functionality.
    - The time it takes to recover data, known as the **Recovery Time Objective (RTO),** is a critical metric.

Replication

- **Concept:** Continuously copying data to another location in real-time or near real-time.
    - Ensures an up-to-date copy of data is always available.
    - Supports high availability but should not be confused with traditional backups.

Journaling

- **Concept:** A system that tracks changes to data or the file system.
    - Allows for quicker recovery by replaying logged changes.
    - Important for maintaining consistency and data integrity.

Power Redundancy

- **Generators:**
  - Provide continuous power during extended outages.
- **Uninterruptible Power Supplies (UPS):**
  - Battery-based systems that activate during short-term outages to prevent immediate shutdowns.

Domain 4.0 Security Operations (28%)

Section 4.1 Given a Scenario, Apply Common Security Techniques to Computing Resources

Secure Baselines

- **Definition:** Standardized security settings and configurations applied to software, hardware, and networks.
  - Ensure a consistent and minimum level of security across all systems.
- **Establishing:**
  - Identify and document standard security settings.
  - Set default password policies, firewall configurations.
  - Incorporate industry-specific requirements (HIPAA, PCI DSS, GDPR).
- **Deploying:**
  - Automate deployment to ensure consistency and efficiency.
  - Provide training and documentation for specific requirements.
  - Perform quality assurance and compliance checks before deployment.
- **Maintaining:**
  - Regularly review and update baselines.
  - Adjust baselines in response to new threats.
  - Train staff on baseline adherence and changes.

Hardening Targets

- **Definition:** The process of strengthening systems, applications, or networks to reduce vulnerabilities and resist attacks.
- **Examples:**

- **Mobile Devices:** Encryption, biometrics, regular updates, VPN, app whitelisting.
- **Workstations:** Antivirus, firewall, access controls, OS hardening, patching.
- **Switches:** Port security, VLANs, disable unused ports, secure protocols, ACLs, patching.
- **Routers:** Disable unused ports, secure protocols, ACLs, patching.
- **Cloud Infrastructure:** IAM, encryption, segmentation, logging, compliance audits.
- **Servers:** Hardened OS, regular scans, file integrity monitoring, backups, patching.
- **ICS/SCADA:** Segmentation, physical security, strict access, patching, logging.
- **Embedded Systems:** Secure boot, minimal OS, read-only config, encryption, firmware updates.
- **RTOS:** Minimal functionality, memory protection, access control, secure comms, audits.
- **IoT Devices:** Authentication, secure comms, firmware checks, segmentation, disable unused features.

Wireless and Mobile Solutions Security

Site Survey and Heatmaps

- **Site Survey:** An assessment to plan wireless networks.
- **Heatmap:** A visual representation of wireless coverage and strength.
- **Purposes:** Optimal AP placement, prevent leakage, detect rogue APs, reduce interference, integrate with physical security, maintain compliance.

Wireless Security Settings

- **WPA3:** Stronger encryption, brute-force protection, forward secrecy, public network protection, Easy Connect.
- **RADIUS (AAA):** Centralized management, enhanced security, scalability, interoperability, compliance.
- **Cryptographic Protocols:** Confidentiality, integrity, non-repudiation, secure key exchange, attack protection.

- **Authentication Protocols:** Secure network access, protect sensitive data, support compliance, maintain integrity, enable accountability, secure remote access.

Mobile Solutions

- **Mobile Device Management (MDM):** Enforces policies, pushes updates, enables remote wipe, ensures compliance, segregates personal/corporate data.
- **Deployment Models:** BYOD, COPE, COBO, CYOD.
- **Connection Methods:**
    - **Cellular:** Use VPN, avoid sensitive transactions on untrusted networks, require SIM PINs.
    - **Wireless:** Use secure Wi-Fi, disable auto-connect, use VPN.
    - **Bluetooth:** Disable when not in use, use latest versions.

Application Security and Sandboxing

- **Application Security:** Measures to protect apps from threats and vulnerabilities.
    - Protects sensitive data, maintains trust, ensures compliance.
- **Input Validation:** Prevents SQL injection, mitigates XSS, ensures data integrity.
- **Secure Cookies:** Protect against eavesdropping, XSS, CSRF; ensure integrity.
- **Static Code Analysis:** Finds vulnerabilities before execution, enforces standards, improves maintainability.
- **Code Signing:** Digital signatures ensure authenticity, integrity, compliance, and user trust.
- **Sandboxing:** Isolates threats, tests suspicious code safely, minimizes zero-day impact.
- **Monitoring:** Continuous system observation for breaches, unauthorized access, anomalies, compliance, and performance.

Section 4.2 Explain Security Implications of Proper Hardware, Software, and Data Asset Management

Acquisition / Procurement Process

- **Definition:** Steps to obtain goods, services, or works externally.
- **Stages:** Needs identification, specification, supplier research, solicitation, negotiation, awarding, order management, inspection, payment, record keeping.

- **Risks:**
    - **Hardware:** Unauthorized access, tampering, supply chain attacks, compliance.
    - **Software:** Malware, vulnerabilities, license compliance, compatibility.
    - **Data Assets:** Breaches, integrity loss, availability, regulatory compliance.

Assignment / Accounting

- **Purpose:** Maintain security by tracking and managing assets.
- **Assignment:** Account tracking, access control, optimized utilization.
- **Accounting:** Inventory management, lifecycle management, loss/theft management.

Monitoring / Asset Tracking

- **Continuous Monitoring:** Detection of anomalies and unauthorized use; real-time assessment of security posture.
- **Asset Tracking:** Location and utilization tracking, lifecycle management.
- **Inventory Management:** Comprehensive asset visibility, verification of security controls, support for incident response.
- **Enumeration:** Identification of network-connected devices; software and service enumeration; dependency mapping.

Disposal / Decommissioning

- **Concept:** Securely and systematically removing hardware, software, and data assets from active use in an organization.
- **Requirements:** Ensures all data is securely removed, assets are disposed of irreversibly, and all actions are certified in line with legal and regulatory requirements.
    - Note: Deleting data via the operating system is insufficient, as it persists on nonvolatile media until overwritten.

Sanitization

- **Definition:** Removing data from a storage device to prevent unauthorized access when the device is reused or disposed of.
    - **Pros:** Allows for reuse or resale of devices.

    - **Cons:** Time-consuming; risk of incomplete data removal if not performed properly.

Destruction

- **Definition:** Physically destroying the storage device to ensure data cannot be recovered.
    - **Pros:** Provides high assurance of data irrecoverability; quick and effective for small quantities.
    - **Cons:** Prevents reuse or resale of devices.

Certification

- **Definition:** Verification by a third party that data destruction or sanitization has been completed according to standards.
    - **Pros:** Formal assurance of data disposal; useful for regulatory compliance and audits.
    - **Cons:** Typically, more expensive.

Data Retention

- **Definition:** Storing data for a set period as per legal or policy requirements before disposal.
    - **Pros:** Ensures compliance with legal and policy requirements; data can be accessed if needed for audits or legal reasons.
    - **Cons:** Requires secure storage and management until disposal; potential risk if data is retained longer than necessary.