General Security Concepts

Compare and contrast various types of security controls.

- **Categories of Security Controls**
  - **Technical Controls**
    - These involve hardware or software mechanisms designed to protect systems and data (e.g., Firewalls, IDS, encryption protocols).
  - **Managerial Controls**
    - Policies and procedures established by an organization's management to guide security efforts (e.g., Risk assessments, security planning, resource allocation).
  - **Operational Controls**
    - Day-to-day procedures and practices that ensure security policies are effectively implemented (e.g., User training programs, incident response protocols, regular data backups).
  - **Physical Controls**
    - Measures taken to protect the physical infrastructure and assets of an organization (e.g., Security guards, surveillance cameras, access control systems).

- **Types of Security Controls**
  - **Preventive Controls**
    - Aim to stop security incidents before they occur (e.g., Access control mechanisms, security policies, antivirus software).
  - **Deterrent Controls**
    - Designed to discourage potential attackers from initiating harmful actions (e.g., Warning signs, visible security cameras, legal disclaimers).
  - **Detective Controls**
    - Intended to identify and alert about security incidents as they happen or after they have occurred (e.g., Log monitoring, IDS, security audits).
  - **Corrective Controls**
    - Focus on restoring systems and data after a security breach or incident (e.g., Data restoration from backups, system patches, incident response procedures).
  - **Compensating Controls**
    - Alternative measures implemented when primary controls are not feasible or fail to provide sufficient protection (e.g., Increased monitoring when segregation of duty isn’t possible, additional authentication methods).
  - **Directive Controls**
    - Establish expected behaviors and actions through policies or guidelines (e.g., Acceptable use policies, security awareness training, standard operating procedures).

Summarize fundamental security concepts.

- **Confidentiality, Integrity, and Availability (CIA)**
  - **Confidentiality**
    - Ensures that sensitive information is accessible only to authorized individuals, preventing unauthorized disclosure.

    - **Integrity**
        - Maintains the accuracy and completeness of data, ensuring it remains unaltered during storage and transmission.
    - **Availability**
        - Guarantees that information and resources are accessible to authorized users when needed.

- **Non-Repudiation**
    - Prevents individuals from denying their actions, ensuring accountability. This is often achieved through digital signatures and audit logs.

- **Authentication, Authorization, and Accountability (AAA)**
    - **Authentication**
        - Verifies the identity of users or systems before granting access.
    - **Authorization**
        - Determines the permissions and resources an authenticated user or system can access.
    - **Accounting**
        - Tracks user activities to maintain record for auditing and compliance purposes.

- **Gap Analysis**
    - A process that identifies discrepancies between current security measures and desired security standards, helping organizations address vulnerabilities.

- **Zero Trust**
    - A security model that operates on the principle of not trusting any entity by default, whether inside or outside the network.
    - **Control Plane**
        - **Adaptative Identity**
            - Dynamically adjusts access controls based on user behavior and context.
        - **Threat Scope Reduction**
            - Minimizes potential attack surfaces by limiting access privileges.
        - **Policy-Driven Access Control**
            - Enforces access decisions based on predefined security policies.
        - **Policy Administrator**
            - Manages and implements security policies across the network.
        - **Policy Engine**
            - Evaluates access requests against policies to make authorization decisions.
    - **Data Plane**
        - **Implicit Trust Zones**
            - Segments of the network where trust is established based on strict verification.
        - **Subject/System**
            - Entities (users or devices) requesting access to resources.
        - **Policy Enforcement Point**
            - The component that enforces access decisions made by the policy engine.

- **Physical Security**
    - Measures designed to protect physical assets and facilities
    - **Bollards**
        - Physical barriers preventing vehicle intrusion.

- **Access Control Vestibule**
  - A secured entryway that verifies identity before granting access.
- **Fencing**
  - Perimeter barriers to deter unauthorized entry.
- **Video Surveillance**
  - Monitoring systems to detect and record activities.
- **Security Guards**
  - Personnel responsible for monitoring and responding to security incidents.
- **Access Badges**
  - Identification cards granting entry to authorized areas.
- **Lighting**
  - Illumination to deter unauthorized access or environmental changes, such as infrared, pressure, microwave, and ultrasonic sensors.

- **Deception and Disruption Technology**
  - Techniques used to mislead attackers and detect unauthorized activities.
  - **Honeypot**
    - A decoy system designed to attract attackers and study their methods.
  - **Honeynet**
    - A network of honeypots simulating a real network environment.
  - **Honeyfile**
    - Decoy files containing fictitious data to detect unauthorized access.
  - **Honeytoken**
    - Decoy data embedded within legitimate data to track unauthorized use.

Explain the importance of change management processes and the impact to security.

- **Business Processes Impacting Security Operations**
  - **Approval Process**
    - Before implementing any change, it's essential to have a formal approval process. This ensures that all modifications are reviewed for potential security implications and align with organizational policies.
  - **Ownership**
    - Clearly defining who is responsible for each change ensures accountability and proper oversight throughout the change lifecycle.
  - **Stakeholders**
    - Identifying and involving all relevant stakeholders ensures that diverse perspectives are considered, and potential security concerns are addressed.
  - **Impact Analysis**
    - Evaluating the potential effects of a proposed change on the organization's operations, security posture, and existing systems helps identify any risks or issues that need to be addressed.
  - **Test Results**
    - Conducting thorough testing before full-scale implementations ensures that the change functions as intended without introducing new vulnerabilities.

  - **Backout Plan**
    - Establishing a contingency plan allows the organization to revert to a previous state if the change leads to unforeseen issues, minimizing potential security risks.

- **Maintenance Window**
  - Scheduling changes during designated maintenance periods reduces the impact on operations and allows for focused attention on the implementation.
- **Standard Operating Procedure (SOP)**
  - Developing and following SOPs ensures consistency in how changes are implemented and reduces the likelihood of security oversights.

- **Technical Implications**
  - **Allow Lists/Deny Lists**
    - Updating these lists ensures that only authorized entities have access, maintaining system security.
  - **Restricted Access**
    - Defining and enforcing restricted activities prevents unauthorized actions that could compromise security.
  - **Downtime**
    - Planning for and managing system downtime during changes ensures that security monitoring and controls remain effective.
  - **Service/Application Restart**
    - Properly managing restarts ensures that security configurations are correctly applied and that systems return to a secure state.
  - **Legacy Applications**
    - Assessing the impact of changes on older applications is crucial, as they may have inherent vulnerabilities or compatibility issues.
  - **Dependencies**
    - Understanding and managing dependencies between systems ensures that changes do not inadvertently compromise security elsewhere in the environment.

- **Documentation**
  - **Updating Diagrams**
    - Maintaining current system diagrams aids in understanding the environment and identifying potential security impacts of changes
  - **Updating Policies/Procedures**
    - Reflecting changes in organizational policies and procedures ensures that security practices remain aligned with the current operational environment.

Explain the importance of using appropriate cryptographic solutions.

- **Public Key Infrastructure (PKI)**
  - **Public Key and Private Key**
    - PKI utilizes asymmetric encryption, involving a pair of keys (a public key for encryption and a private key for decryption). This mechanism ensures that only the intended recipient can access the encrypted information.
  - **Key Escrow**
    - This involves storing a copy of encryption keys with a trusted third party, allowing data recovery in case of key loss, while maintaining security protocols.

- **Encryption Levels**
  - **Full-Disk Encryption (FDE)**
    - Encrypts all data on a disk, protecting information at rest.

- **Partition and Volume Encryption**
    - Targets specific sections of a storage device, offering flexibility in securing sensitive data.
- **File and Database Encryption**
    - Encrypts individual files or entire databases, ensuring data remains protected during storage and access.
- **Record Encryption**
    - Encryptions specific records within a database, providing granular security control.

- **Transport/Communication Encryption**
  - **Asymmetric Encryption**
    - Uses a pair of keys (public and private) for secure data transmission, commonly employed in SSL/TLS protocols.
  - **Symmetric Encryption**
    - Utilizes a single key for both encryption and decryption, suitable for encrypting large data volumes due to its efficiency.
  - **Key Exchange**
    - The process of securely exchanging encryption keys between parties, essential for establishing secure communications.
  - **Algorithms and Key Length**
    - The choice of encryption algorithms and key lengths directly impacts security strength; longer keys generally offer enhanced security.

- **Cryptographic Tools**
  - **Trusted Platform Module (TPM)**
    - A hardware-based security module that stores cryptographic keys securely, enhancing platform integrity.
  - **Hardware Security Module (HSM)**
    - A dedicated hardware device designed to manage and safeguard digital keys, ensuring high levels of data protection.
  - **Key Management System**
    - A framework for managing cryptographic keys, including their generation, distribution, storage, and destruction, ensuring keys are handled securely throughout their lifecycle.
  - **Secure Enclave**
    - An isolated hardware-based environment that securely processes sensitive data and operations, protecting them from unauthorized access.

- **Obfuscation Techniques**
  - **Steganography**
    - Conceals information within other non-secret data, adding an additional layer of security.
  - **Tokenization**
    - Replaces sensitive data with non-sensitive equivalents (tokens), reducing the risk of data exposure.
  - **Data Masking**
    - Alters data to conceal sensitive information, allowing the use of realistic data sets in non-secure environments.

- **Additional Cryptographic Concepts**
    - **Hashing**
        - Transforms data into a fixed-size hash value, ensuring data integrity by detecting alterations.
    - **Salting**
        - Adds random data to inputs before hashing, protecting against precomputed attacks like rainbow tables.
    - **Digital Signatures**
        - Provide authentication and non-repudiation by verifying the sender's identity and ensuring message integrity.
    - **Key Stretching**
        - Enhances weak keys by processing them through algorithms to increase their complexity, making them more resistant to attacks.
    - **Blockchain and Open Public Ledger**
        - Utilize cryptographic techniques to create secure, decentralize records of transactions, ensuring transparency and immutability.

- **Certificates and Trust Management**
    - **Certificates Authorities (CAs)**
        - Trusted entities that issue digital certificates, validating the identity of entities and enabling secure communications.
    - **Certificate Revocation Lists (CRLs) and Online Certificate Status Protocol (OCSP)**
        - Mechanisms to check the validity of certificates and ensure they have not been revoked.
    - **Self-Signed and Third-Party Certificates**
        - Self-signed certificates are issued by the entity itself, while third-party certificates are issued by trusted CAs, providing varying levels of trust.
    - **Root of Trust**
        - A trusted component that serves as the foundation for establishing trust in a cryptographic system.
    - **Certificate Signing Request (CSR) Generation**
        - The process of creating a request for a digital certificate, containing the entity's public key and identity information.
    - **Wildcard Certificates**
        - Certificates multiple subdomains under a single domain, simplifying certificate management.