Armaan Shamsaasef

Physical Security

Notes: Physical Security (SY0-701 - 1.2)

Core Concept: Physical security involves the protection of people, data, equipment, and facilities from physical threats. It is the first layer of defense and is just as critical as digital security.

Key Physical Security Controls

1. Access Control Vestibule (Mantrap)

- Definition: A small space with two sets of interlocking doors. The second door only opens once the first door has closed and the person inside has been verified.
- Purpose: To prevent tailgating (unauthorized persons following an authorized person into a secure area).
- Example: A data center entrance where you badge in, enter a small room, the outer door locks, and then you must badge again or provide a second factor to open the inner door.

2. Fencing and Bollards

- Fencing: Establishes a perimeter. Height and material determine its security level (e.g., 3-4 ft. indicates a boundary, 8+ ft. with razor wire is a serious barrier).
- Bollards: Heavy posts, often concrete or steel, placed to prevent vehicles from ramming into a building or crashing through entrances.

3. Cameras (Video Surveillance)

- Purpose: To monitor, record, and deter activity.
- Key Types:
    - CCTV (Closed-Circuit Television): A private, self-contained video system.

    - IP Cameras: Digital cameras that send video over a network, allowing for remote viewing and management.

4. Access Control Systems

- Definition: Methods to grant or deny physical entry.
- Common Methods:
    - Badge Readers: Using RFID or smart cards.
    - Biometrics: Fingerprint, retina, or palm scanners.
    - Keypad/PIN Codes: Something you know.
    - Multi-factor Authentication: Combining methods (e.g., a badge + a PIN).

5. Alarms

- Intrusion Detection Systems: Sensors (on doors, windows, or monitoring motion) that trigger a local or remote alarm when a breach is detected.
- Purpose: To alert security personnel to an active incident.

6. Lighting

- Purpose: A primary and low-cost deterrent. Criminals are less likely to operate in well-lit areas.
- Application: Placed around the perimeter of a building, in parking lots, and other dark areas to increase visibility and surveillance capabilities.

7. Sensors

- Motion Detection: Uses infrared, microwave, or acoustic technology to detect movement in a space.
- Noise Detection: Sensors that trigger an alarm if a certain decibel level is exceeded (e.g., breaking glass, an explosion).
- Proximity Readers: A type of sensor used in badge readers to detect a credential from a short distance.

8. Guest and Visitor Management

- Process: Logging all visitors, often requiring them to present an ID, wear a temporary badge, and be escorted by an authorized employee while on the premises.

Key Principles

- Defense in Depth: Use multiple, layered physical security controls (e.g., a fence, then a guard, then a badge reader, then a mantrap).
- Deter, Detect, Delay, Deny: The goals of a physical security plan are to deter intruders, detect their presence, delay their progress, and ultimately deny them access to critical assets.

Key Takeaway

Physical security is the foundation of overall security. A network can be perfectly secure, but if an attacker can physically walk out with a server, all technical controls are irrelevant. These controls work together to protect an organization's most critical physical assets.