CompTIA Security + 3.0 Architecture and Design

Filename: comptia-secplussy0501-3-9-importance_of_security_controls
Title: Importance of Physical Security
Subtitle: CompTIA Security+ (SY0-501)

3.9 Importance of Physical Security

- 3.9 Explain the importance of physical security controls.
  - Lighting
    - Illumination of important areas such as entry-control points
    - Perimeters of buildings and fences
    - Not a psychological deterent
    - Relatively inexpensive to maintain
    - Assist guards and camera-based systems
    - Should have power backup, or UPS support
  - Signs
    - Authorized entry points(public access point to secured access)
    - Controlled entry points(public access point to customer area)
    - Warning signs around perimeters
    - Physical hazard areas
  - Fencing/gate/cage
    - Fencing is the most common phyiscal security component
    - Example
      - United States Geological Physical Security Handbook 440-2H
      - http://bit.ly/2oDQtCc
  - Security guards
    - Real-time monitoring
    - Reacting in realtime to intrusion events
    - Human element is more adaptable to events that IDS systems
    - SANS Reading Room Whitepaper 37120
    - http://bit.ly/2okpYhW
  - Alarms
  - Safes
  - Secure cabinets/enclosures
  - Protected distribution/Protected cabling
    - PDS or Protected Distribution Systems
    - Protection of wireline and optical fiber PDS to tranmit unencrypted information
    - National Security Telecommunication and Information Security Instruction (NSTISSI) No. 7003 standardized PDSs to tranmit unencrypted National Security Information
    - Stress the need for continued phyiscal security integrity
  - Airgap
  - Mantrap
  - Faraday cage
    - Time for the tin foil hat
    - Side-channel attack is a form of reverse enginneering in which circuitry leaks EM fields making it possible for capture. The attacker is able to deduce the information or data that is being processed.
    - van Eck phreaking
    - Embedded System
      - Types
        - IC
        - SoC
        - IoTs,are susceptible
    - http://bit.ly/2oNwdif (Wikipedia)
    - http://amzn.to/2p8krjr (Amazon)
  - Lock types
    - Traditional
      - Deadbolts
      - Padlock
      - Knoblock
      - Leverlock/Latchllock
    - Keyless-entry/Electronic
      - Pin-code lock
        - http://bit.ly/2okpJDr
      - RFID, proximity
      - Keyfob, card-access
        - http://bit.ly/2p8aH8S
      - Biometrics
        - http://bit.ly/2pqZbCn
    - Multfactor Authenticatio/MMA

- Biometrics
  - Types
    - Fingerprint readers
    - Hand geometry scanners
    - Retinal scanners
    - Face recognition
    - Voice recognition
- Barricades/bollards
  - Guides traffic away from an area
  - Prevents from vehicle intrusions
  - Can be static or hydraulic (think Gunter's AFB)
  - Can be crash rated to within vehicular impacts
  - Types
    - Jersey Barriers
    - http://bit.ly/2pqNOdJ
- Tokens/cards
  - Mentioned throughout, keyfobs,smartcards, RFID
- Environmental controls
  - HVAC
  - Hot and cold aisles
  - Fire suppression
    - National Fire Protection Agency or NFPA-75
    - Standard for the Fire Protection of Information Technology Equipment
    - http://bit.ly/2pqTWTh
  - Management Systems
    - https://avtech.com/
  - Vendor Recommendations
    - Cisco = http://bit.ly/2p8eu61
- Cable locks
  - Kabilt
  - Keningston
  - Keningston Security Slots
  - Targus
- Screen filters
  - Prying eyes
  - Privacy Filters
  - Privacy Screens
  - http://amzn.to/2okAg1n
- Cameras
- Motion detection
  - Radar-waves relying on reflection back to a sensor
  - Photo-sensitive detects using lasers and light sensor
  - Passive Infrared or PiR using abrupt changes in the infrared energy.
- Logs
  - Vistor access
    - Being able to uniquely identify and record individual's access 24/7
  - Event monitoring
  - Log retention for auditing or review purposes
  - Securely storing logs
- Infrared detection
  - Most IR bem sensors come with one to three beams
  - More beams, larger coverage area or creating taller beam that is harder to bypass
- Key management
  - Key falling into the hands of an unauthorized
  - Gives unathorized person or persons
  - Data breachs
  - Corrupted keys can render data unreadable