Penetration Testing and Incident Response

March 24, 2022

Chapter 4

**Physical Security**

* Physical security is just as important as technical
* Basic Equipment Controls
  + Basic equipment controls are defensive measures placed on the front lines of security
    - Passwords
    - Hard drive encryption
    - VoIP telephone systems
* Hard Drive and Mobile Device Encryption
  + PGP, TrueCrypt, BitLocker
  + Encrypting File System (EFS)
  + Organizations should implement appropriate media controls for CDs, DVDs, hard drives, mobile devices, and more
  + Sanitization is the process of clearing all identified content so that no data remnants can be recovered
    - Drive wiping
    - Zeroization
    - Degaussing
      * Powerful magnet
  + Software and hardware utilities to destroy data
    - Shred-it
    - Darik’s Boot and Nuke
    - Etc.
* Fax Machines and Printers
  + Faxes were not designed with security in mind
    - transmit information unprotected
* VoIP
  + Place telephone calls over the internet and computer networks
* Physical Area Controls
  + Look at the perimeter
  + Fences
  + Perimeter Intrusion Detection and Assessment Systems (PIDAs)
    - Fencing
  + Gates
    - Residential, commercial, industrial, restricted area
  + Bollards
    - Stop cars from ramming into building
* Facility Controls
  + Protect the entry points
    - Doors, windows, roof access, fire escapes, etc.
  + Doors, mantraps, and turnstiles
    - Use solid core doors (not hollow ones)
    - Be concerned with flow in and out of the facility
  + Walls, ceilings, and floors
    - Be aware of drop ceilings
      * People can get through the plenum space
  + Windows
    - Can be tinted or shatterproof
  + Guards and Dogs
    - Good deterrents
    - Good background checks on guards
    - CCTV
  + Construction
    - Where is the building being built
    - Redundancy measures
    - Vulnerability to crime
* Personal Safety Controls
  + Security plan must address the protection and security of personnel
    - Lighting, alarms, CCTV/remote monitoring
  + Lighting
    - Continuous, standby (randomly turned on to indicate activity), movable, emergency
  + Alarms and intrusion detection
    - Can only detect, not prevent
  + CCTV
    - In conjunction with guards to watch what is going on
* Physical Access Controls
  + Any mechanism by which an individual can be granted or denied physical access
  + Locks
    - Mechanical and cipher
    - Locks can be picked
  + Tokens and Biometrics
    - Active electronic
    - Electronic circuit
    - Magnetic stripe
    - Contactless cards
  + Biometrics
    - False rejection rate
    - False acceptance rate
  + Avoiding common threats to physical security
    - Natural, human, and technical threats
      * Human threats: theft, vandalism, destruction, terrorism, accidental
    - Physical keystroke loggers and sniffers
    - Bluetooth
      * Bluejacking
  + Defense in Depth
    - Layering controls to protect assets