Physical Security

Information Security

Dr Hans Georg Schaathun

Høgskolen i Ålesund

Autumn 2011 – Week 7

Learning Outcomes

After this week, students should

- be able to identify threats and useful controls in the physical environment of an information system

Zoning systems

Building divided into areas with different security controls.

- Why may this be a good idea?
- Assets with different
  - value
  - criticality
  - user access requirements
- Staff with various access requirements
- Other people with various access requirements

The following is an example. Different operation will have very different needs.

Zone 1

Open areas

- Outer areas
  - Outdoor, maybe reception area
- Typical controls:
  - good fence
  - CCTV

Zone 2

Main offices

- Most staff work here
- Typical controls:
  - locks and alarms on doors and windows

Zone 3

Restricted access

- Few staff require regular access
- Typical controls:
  - locks and alarms on doors and windows
  - reinforced windows (security glass)
  - access control with identification and logging

Zone 4

Data centres and inner sanctums

- Only very few staff require access
- Typical controls:
  - locks and alarms on doors
  - should not have windows
  - access control with identification and logging
  - motion sensors
  - assault alarms

Question

What threats are we concerned with when we design the physical rooms to host a server rack or mainframe?

Typical Threats

- Unauthorised, physical access (incl. burglary)
- Interuptions of power supply
- Fire
- Flood (rainwater or broken water pipes)
- Temperature (too high or too low)
- Humidity, dust, air particles etc.
- Radiation
- Peaking

Dedicated server room

Why is a dedicated server room a good idea, even for a local LAN server?

- Threats by human error:
- Disconnecting
  - Stumbling in a network cable
  - Moving cables to clean the floor
- Mistaking the server for a workstation
  - e.g. turning it off at night

A dedicated server room is a good control, reducing the strain faced in rooms that are in continuous use.

The context

Consider the physical access control to enter a room (e.g. server room).

Authorisation versus Identification

- What do we mean by
  1. *Identification*?
  2. *Authorisation*?
  3. *Authentication*?

Identification and Authentication

Identification establishing the identity of the person, linking a physical person to a personell record.

Authentication verifying the correctness of the identification

Why do we use identification in access control?

- Authorisation — privileges specified in personnel record.
- Audit logs — recording access for audit trail

Authorisation

Authorisation refers to determining what a given individual is permitted to do.

- Authorisation does not require identification
- A mechanical key authorises someone to enter a locked room.
- The authority is linked to the key
  - not the identity of the person carrying it
- Mechanical locks give authorisation without identification

To identify or not to identify

- Two *separate* controls:
  - Access control (authorisation)
  - Access logging (identification)
- What challenges are related to logging?
- Privacy
- Privacy legislation
- What are the advantages of logging?
- Trace abuse

Formal agreement between employer and employee can help get acceptance.

Principles of identification

- Something carried
  - a key, a keycard, an identity card, a uniform
- Something known
  - a password, PIN, pass phrase
- Something one is
  - fingerprint, palmprint, iris scan, facial recognition
  - voice recognition, signature recognition (behaviourlal)

Or any combination of the above

Something carried

Advantages and disadvantages?

- simple
- relatively cheap
- loss and theft

Something known

Advantages and disadvantages?

- very cheap
- difficult to remember
    - leading to human errors and possible compromising

Biometrics

Advantages and disadvantages?

- relatively expensive
    - but getting cheaper
- imperfect authentication
    - but getting better
- simple for the user
    - nothing to bring, nothing to remember
- difficult to forge or steal

Privilege Management

- Consider many groups of users
  - rank and file staff
  - technical staff
  - specially vetted staff
  - permanent contractors
  - temporary contractors
  - visitors
- Privilege management is complex
  - *who needs what?*

Power related threat events

What threat events may happen relating to power?

- Variations in voltage or frequency
- Pulses
- Power glitches
- Blackout

What happens to the equipment in these cases?

Controls

UPS Uninterupted power supply. Prevents loss from glitches and short outages.

Generators Prevents loss from blackout. Does not protect against glitches as they take time to start.

Transformers Evens out instability to avoid damage from voltage or frequency variations, and from pulses

- Needs depend on local mains quality
- Workstations and printers may not require controls
- Be aware of power instability in the case of inexplicable hardware fault

Cabling

- Cables have to be tidy
  - to avoid interuption when installations are upgraded
  - to avoid human error
- Patch panels 10cm above floor level
  - to avoid damage in case of (minor) flooding
- Separate, locked areas
  - to avoid casual contact and accidents

Climate

- Cooling is critical.
  - and the cooling system must be sufficiently reliable
- Other threats
  - Dust
  - Static electricity

Fire

- Fire detectors
- Fire alarms
  - alert fire brigade
  - open escape routes and close fire doors
  - control lifts
  - close vents and stop fans
- Fire extinguishers
  - remember: right type for the situation
- *Collaboration with fire brigade is useful*

Flooding

- Risks include
  - leakage from higher floors
  - leakage from cooling system
  - leaks from pressurised pipes in adjacent rooms
  - floods — and land slides

Watch — surveillance — alarm

- Guards (expensive, especially 24/7)
- Response teams
- Surveillance
- Monitoring
  - incident reports
  - flagging of unusual incidents
  - risk reviews

Radiation

- EMR — electromagnetic radiation
  - allows eavesdropping
  - can be shielded (Faraday cage)
- EMP — electromagnetic pulse
  - attack
  - knocks out equipment

Laptop controls

- Burglar alarms
- Anti-theft software — reporting location to a server
- Invisible markings
- Cable lock
- Backup

Telecommuting

Heimekontor

What challenges arise when staff work from home?

- How do you deal with it?
  - additional security at home?
  - restricted information access for home work?
- Solutions
  - VPN — Virtual Private Networks
  - *per service* remove access