

More on Security

Computer Crime Laws (cyberlaw)

- Deals with
 - Unauthorized modification or destruction
 - Disclosure of sensitive information
 - Unauthorized access
 - Use of malware
- Three categories of crimes
 - Computer-assisted crime – computer is used as a tool.
 - Obtaining sensitive military info by attacking military system
 - Industrial espionage
 - Hacktivism
 - Could take place without a computer
 - Usually covered by criminal law, not necessarily considered a “computer crime”
 - Computer targeted crime – computer is a victim of attack.
 - DDOS
 - Capturing passwords
 - Installing malware
 - Buffer overflow in order to take control
 - Could not take place without a computer
 - Computer incidental crime – computer was involved when crime happened, but not as an attacker or a victim
 - Computer happened to be involved in a secondary manner, but significantly.
 - Obtaining and sharing child pornography.
 - Not an attacker, not being attacked, but used in a criminal act.

Some of US computer crime laws

- 18 USC 1029: Fraud and Related Activity in Connection with Access Devices
- 18 USC 1030: Fraud and Related Activity in Connection with Computers
- 18 USC 2510 et seq.: Wire and Electronic Communication Interception and Interception of Oral Communication
- 18 USC 2701 et seq.: Stored Wire and Electronic Communication and Transactional Records Access
- Digital Millennium Copyright Act
- Cyber Security Enhancement Act of 2002

USA Patriot Act of 2001

- The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001
- Deals with many issues:

- Reduces restriction on LE agency's ability to search phone, e-mail, financial and other records.
- Eases restriction on foreign intelligence gathering within US.
- Expands the definition of terrorism to include domestic terrorism, thus enlarging the number of activities to which the acts's expanded law enforcement powers can be applied.
- Made changes to Electronic Communication Privacy Act of 1986.

Steganography

- Method of hiding data in another media type so that the very existence of the data is concealed.
- Media files are ideal for message hiding.
- Message can be hidden in the following media:
 - Image
 - Wave file
 - Documents
- Messages are not always encrypted
- Security through obscurity
- Components
 - Carrier – file that has hidden payload in it
 - Payload – info that has to be concealed and transmitted
 - Stegomedium – medium in which info is hidden.
- Method to the madness
 - Use LSB to encrypt message.
 - Bmp file example.
 - Mp3 file example.

Physical and Environmental Security and Disaster preparedness

- Controlling Access to company assets.
- Dealing with personnel terminations and hires.
- Dealing with natural disasters.
- Dealing with sabotage/acts of vandalism.

System Hardening

- Security controls can be physical, administrative, and technical.
- "If I can put my hands on the computer, I own it".
- Physical
 - Wiring closets should be locked.
 - NW switches and hubs should be inaccessible (locked cabinets, cages, etc.)
 - NW ports in public places should be physically inaccessible.
 - Perimeter security, cameras, locks, gates, fences, etc.
- Technical
 - Services and apps that are not installed cannot be attacked.

- Uninstall rather than disable
- If unable to uninstall/disable, use most conservative settings
- Create a GM (Gold Master image)
 1. Determine what apps and services are needed
 2. Develop secure configuration for all software
 3. Ensure it still provides user functionality and interoperability with the rest of the network
 4. Subject GM to thorough vulnerability scanning and penetration testing
 5. Roll it out by cloning to all hard drives
 6. If changes are needed, go back to item 1.

Remote Access Security

- Require a VPN with 2-factor authentication
- Use encryption for data and commands, use ssh
- Strong authentication
- Critical systems should be administered locally, not remotely
- Only a small number of admins should be able to do remote system administration

Physical Access

- Perimeter control is the first line of defense
- Use layered security
 - To get to a secret barbeque sauce recipe an intruder should:
 - Cut a fence
 - Slip by a security guard
 - Pick a door lock
 - Circumvent biometric lock
 - Break into a safe where recipe is kept...
- Have diversity of controls
- Facility Access Control
 - Enforced thru physical and technical components
 - Physical component is id-ing a person
 - Who should have access to what areas
 - Different access points for different roles

Locks

- Inexpensive mechanism
- *Delaying* device, a challenge
- Should not be the only access mechanism
- Lock and key access is not logged
- Master and submaster keys
- Match type of the lock to the level of protection
- Several types
 - Warded lock

- Tumbler lock
 - Pin tumbler
 - Wafer tumbler
- Combination lock
 - Mechanical
 - Electronic
 - Programmable cypher locks
 - Door delay, key override, master keying, hostage alarm, individual codes
 - Smart locks
- Device locks
 - Switch controls for on/off switches
 - Port controls – block access to disk drives and unused ports
 - Cable traps – prevent i/o device removal by passing cable thru a lockable unit
- Circumventing locks
 - Each type has corresponding tools to pick it
 - Raking, bumping

Lock Strengths

- Grade 1: Commercial and industrial use
- Grade 2: Heavy-duty residential and light-duty commercial
- Grade 3: Residential/consumer

Personnel Access Controls

- Piggybacking – follow an authorized person closely
- User-activated readers – user has to do something – swipe a card, enter a pin, etc.
- Proximity readers

Internal Support Systems

- Facility needs to be fortified and compartmentalized
- Need lights, A/C and water!
- Power failure will be devastating
 - Storms
 - High winds
 - Lightning
 - Hardware failures
 - Accidents
- Smart Grid – technology embedded into grids to automate and optimize its functions.
- Our grid now is not smart!
 - Goals – self-healing, resistant to physical and cyber attacks, bidirectional communication capabilities, increased efficiency and better integration of renewable energy sources.

- Almost every component will need to be computerized in some way.
 - Smart meters, smart thermostats
 - Automated feedback loops, digital scheduling, load shifting
- More attack vectors, since most pieces will have some kind of technology embedded.

Power protection

- UPS – Uninterruptible Power Supply
- Some sustain critical operations for hours, some allow system to shut down gracefully
 - Online
 - use AC line voltage to charge a bank of batteries,
 - uses DC to AC inverter
 - power flows thru them all the time, detects and reacts quicker to power failures
 - costs more
 - Standby
 - Stay inactive until power fails
 - Small delay to switch to battery pack when power failure is detected
 - Less expensive
- Power line conditioners
 - Clean power has no interference (line noise) or voltage fluctuation.
 - Line noise
 - EMI (electro-magnetic interference) - created by difference between hot, neutral and ground wires and their magnetic field – lightning, motors.
 - RFI (radio frequency interference)- created by anything with radio waves, and fluorescent lighting.
 - Data processing should be on a different circuit than a device creating a *rush-in*.
 - Voltage regulators and line conditioners absorb extra current and store some power to add in case of power sag.
- Backup sources
 - Generators

Fire Prevention, Detection, Suppression

- Prevention – train employees how to react, provide proper equipment, design containment measures, non-combustible materials, etc.
- Detection – sensors and alarms
 - Smoke activated
 - Heat activated
- Suppression- manual or automated systems (sprinklers and CO2 discharge systems)
 - Fire Extinguishers
 - Sprinklers (many types)

Fire class	Type of Fire	Elements of fire	Suppression method
------------	--------------	------------------	--------------------

A	Common Combustibles	Wood, paper. Laminates	Water, foam
B	Liquid	Petroleum products, coolants	Gas, CO2, foam, dry powders
C	Electrical	Electrical equipment and wires	Gas, CO2, dry powders
D	Combustible Metals	Magnesium, sodium, potassium	Dry powder