Social Engineering

IT 444 – Network Security Administration II

Human Weakness

- Security breaches are common even when an organization employs antivirus systems, IDS…
- Human-based social engineering
  - Giving a false identity and ask for sensitive information
  - A friend of an employee ask him/her to retrieve information that a bedridden employee supposedly needs
  - Posing as an important user: assuming the identity of an important employee in order to add element of intimidation.
    - People will do something outside their routine for someone they perceive to be in authority
  - Posing as technical support: posing as a hardware vendor, a technician or a computer-related supplier when approaching the victim

Human-based SS techniques

- **Eavesdropping:** An authorized listening to conversations or reading of messages
- **Shoulder surfing:** Looking over someone's shoulder as he/she enters information into the devices
- **Dumpster diving:** Searching for sensitive information in a company's trash bins -- or on or under desks
  - Phone bills
  - Contact information
  - Financial data
  - Operations-related information

More human-based techniques

- **In-person attack:** Try to *visit* a target site and physically *survey* it for information
- **Third-party authorization:** Represent themselves *as agents* authorized by authority figures to obtain information *on their behalf*
- **Tailgating:** An unauthorized person closely *follows* an authorized person into a secured area
- **Piggybacking:** An unauthorized person *convinces* an authorized person to allow him/her into a secured area

Computer-based Social Engineering

- **Pop-up Windows:** A window appears on the screen informing the user that they have lost their network connection -- and therefore need to re-enter their credentials (*i.e., username/password*)
- **Mail attachments:**
  - Attachment with malicious code, *hidden in a file*
  - A hoax email asking users to *delete legitimate files*.
  - Sending a false warning email regarding a virus...and asking targeted users to *forward* the mail messages to friends

Computer-based Social Engineering

- **Web sites:** Getting an unwitting user to *disclose sensitive data* such as password used at work
- **Instant messenger:** *Chatting* to gather personal information
- **Phishing:** Sends an email or provides a link falsely claiming to be from a *legitimate* site.

Insider attack & the prevention

- Attacks may steal *sensitive data*, bring down an organization
- 60% of attacks occur from *behind* the firewall
- Insider attacks are easy to launch and difficult to prevent
- Prevention:
  - Separation of duties
  - Rotation of duties
  - Restricting privileges
  - Controlling access
  - Logging and auditing
  - Legal policies
  - Archiving critical data

Social engineering threats

- Online threats
- Telephone-based threats
- Personal approaches
- Reverse social engineering: a perpetrator assumes the role of a person in authority and has ask employees asking him or her for information

What make companies vulnerable

- Insufficient security training and awareness
- Multiple organizational units make system management ore combersome
- Lack of appropriate security policies
- Providing easy access to information

Why social engineering is effective

- Can't prevent *people* from being socially engineered
- Difficult to *detect* social engineering attempts
- No *one* method can guarantee *complete* security from social engineering attacks
- No hardware or software is available to *defend* against social engineering

Warning signs of an attack

- Unwilling to give a valid callback number
- Making informal requests
- Claiming authority
- Showing haste
- Giving complements or praise excessively
- Dropping a phone name inadvertently
- Threatening negative consequences if information is not provided

Impact on an Organization

- Economic losses
- Damage of goodwill
- Loss of privacy
- Dangers of terrorism
- Lawsuit and arbitration
- Temporary or permanent closure