CS 465

Social Engineering

Last Updated: Dec 14, 2017

Social Engineering

Source:

The Art of Deception
Controlling the Human Element of Security

By Kevin Mitnick and William Simon

Information Security Awareness and Training

- No technology in the world can prevent social engineering attacks
- Some authorities recommend 40% of an overall security budget be targeted to awareness training

Train Your Employees

A company can spend hundreds of thousands of dollars on firewalls, encryption and other security technologies, but it an attacker can call one trusted person within the company and that person complies, and if the attacker gets in, then all that money spent on technology is essentially wasted.

Kevin Mitnick

Six Tendencies of Human Nature

- Authority
  - Comply with a request from someone of authority
- Liking
  - Comply with a request from someone we like
- Reciprocation
  - Comply with a request when we are promised or given something of value
- Consistency
  - Comply after we have committed to a specific action
- Social Validation
  - Comply when doing something in line with what others are doing
- Scarcity
  - Comply when we believe the object sought is in short supply and others are competing for it, or it is available for a short period of time

Common Social Engineering Methods

- Posing as a fellow employee
- Posing as an employee of a vendor, partner company, or law enforcement
- Posing as someone in authority
- Posing as a new employee requesting help
- Posing as a vendor or systems manufacturer calling to offer a system patch or update
- Offering help if a problem occurs, then making the problem occur, thereby manipulating the victim to call the attacker for help

Common Social Engineering Methods

- Sending free software or patch for a victim to install
- Sending a virus or Trojan Horse as an email attachment
- Using a false pop-up window asking the user to log in again or sign on with password
- Capturing victim keystrokes with expendable computer system or program
- Leaving a USB drive around the workplace with malicious software on it

Common Social Engineering Methods

- Using insider lingo and terminology to gain trust
- Offering a prize for registering at a Web site with username and password

Top 5 Soc Eng Techniques

- Familiarity exploit
  - Act like you belong there
- Create a hostile situation
- Gathering useful information
  - Social media
  - Cars
  - Dumpster diving
- Get a job there
- Body language

Source: http://www.pcworld.com/article/182180/top_5_social_engineering_exploit_techniques.html

5 Attacks to Watch Out For

- Phishing
- Pre-texting
  - Lie to obtain sensitive information
  - https://www.washingtonpost.com/news/the-intersect/wp/2014/10/07/forget-celebgate-hackers-are-gunning-for-the-nude-photos-of-ordinary-women-and-underage-girls/?utm_term=.c3fd0fd1a3c5
- Baiting
  - http://www.darkreading.com/attacks-breaches/social-engineering-the-usb-way/d/d-id/1128081?
- Quid pro quo
  - Office workers gave away pw for pen or chocolate
- Tailgaiting
  - http://www.computerworlduk.com/security/how-a-man-used-social-engineering-to-trick-a-ftse-listed-financial-firm-14706/

Source: https://www.tripwire.com/state-of-security/security-awareness/5-social-engineering-attacks-to-watch-out-for/

Warning Signs of an Attack

- Refusal to give a callback number
- Out-of-ordinary request
- Claim of authority
- Stresses urgency
- Threatens negative consequences of noncompliance
- Shows discomfort when questioned
- Name dropping
- Compliments or flattery
- Flirting

Common Targets of Attacks

- Unaware of value of information
  - Receptionists, telephone operators, admin assistants, security guards
- Special privileges
  - Help desk or technical support, system admins, computer operators, telephone sys admins
- Manufacturer/Vendor
  - Computer hardware, software manufacturers, voice mail systems vendors
- Specific departments
  - Accounting, human resources

Factors that Make Companies More Vulnerable to Attacks

- Large number of employees
- Multiple facilities
- Information on employee whereabouts left in voice mail messages
- Phone extension information made available
- Lack of security training
- Lack of data classification system
- No incident reporting/response plan in place

Foiling Attacks

- Most attacks could be foiled if the victim simply follows two steps
  - Verify the identity of the person making the request
  - Verify whether the person is authorized

Social Engineering at BYU

- http://universe.byu.edu/2002/02/28/women-charged-with-theft-of-students-credit-card-numbers/

Advanced Persistent Threat

- Usually targets organizations for business or political motives
- Advanced: sophisticated techniques to exploit vulnerable systems
- Persistent: External command and control that monitors over an extended period of time
- Threat: Human involvement in orchestrating the attack
- Claim: most US corporations have had their sensitive data stolen
  - Financial, Oil, Security, Defense

Advanced Persistent Threat

- Social engineering is the catalyst for many Advanced Persistent Threat (APT) attacks
  - Stuxnet was assisted through USB drives
    - https://www.youtube.com/watch?v=6WmaZYJwJng
  - Penetration testers gain a foothold using social engineering
    - Research VPs and send targeted emails with infected pdf files
    - Pose as cleaning crew inspector and plant infected USB drives

Resources

- http://en.wikipedia.org/wiki/The_Art_of_Deception
- http://en.wikipedia.org/wiki/Social_engineering_(security)
- http://www.social-engineer.org/