THE SECURITY STANDARD™

September 13-14, 2010 > Marriott Brooklyn Bridge > New York, NY

Produced by

CSO

Defending the Fortress:
New Threats Meet New Defenses

Proactive Protection Policies:
Thwarting Social Engineering and Other Identity Challenges

Alan Lustiger

Director of Information Security

GAIN Capital

What we will cover

- What is social engineering?
- Categories of SE attacks
- Targets of SE attacks
- How to protect your data from SE attacks

Who am I?

- Alan Lustiger
- 15 years of information security experience
- Previous positions at AT&T, E&Y and TD Ameritrade
- 10 years of speaking at security conferences
- *But **do you believe me?***

What is social engineering?

- Definition: *The process of deceiving people into giving away access or confidential information*
- Shorter definition: *Hacking people*
- Social engineering is **the greatest security risk facing large companies** *(Gartner 2004)*

What vectors can social engineers use?

- Face to face
- Phone
- Email (phishing and email worms are SE attacks)
- Websites, including ads
- Faxes
- Dumpster diving

What vectors can social engineers use?

- Social networking sites
- Electronic message boards
- Newspaper/online classifieds
- Job interviews
- Contests
- Twitter

*All of these methods can establish **trust***

What information do social engineers want?

- Any and every bit of information is valuable
- Ultimate goal – access to systems, usually by getting people to trust them
- How much information do you already give out about yourself?

Facebook/LinkedIn are goldmines!

- Without meeting you, the social engineer can often know:
  - Nicknames, family member names, your friends, your pets, your hobbies, your religion, your sports teams, your vacation schedule, your job title, your company, your birthday, your age, your location, your coworkers, **your face** …
  - Because **you published them**!

Blended attacks

- Most companies still have good perimeter IT defenses but poor internal controls
- Social engineers use a combination of human and computer hacking to take advantage
- Once they get internal access to your network they are often 90% there

Gaining remote access to your network

- Fool someone into:
  - Inserting a USB key/CD
  - Opening an infected spreadsheet or program
  - Reveal a password
- *USBs in the parking lot*
- *CDs labeled "Payroll"*

Gaining remote access to your network

- Use SE techniques to:
  - Connect directly to your network
  - Install a wireless AP
  - Take backup tapes/disks
  - Hacking local desktops/servers is much easier than hacking remotely!

The bad news

- It is nearly impossible to defend against a motivated social engineer with unlimited time
  - He could become an employee or a contractor (or a janitor)
  - What if he/she became your DBA or sysadmin?
  - Think international espionage

The good news

- You can slow them down and increase your chances of catching them

Three layers of defense

- People
- Process
- Technology

People

- **Awareness**! Teach with **specific** examples.
  - A pretty woman can get a guy to do anything ☺
- Balance helpfulness with wariness
- Consequences of making a mistake
- The same tools can help them in their own personal lives
  - Why does this website need to know my birthday?

Specific defenses to teach people

- Don’t allow piggybacking through doors
- Ask people for their IDs
- Don’t let guests walk without an escort
- Don’t trust what people say without proof
- When in doubt, don’t allow it – and escalate to your supervisor

Physical and Data Security Processes

- Create specific procedures and policies for all conceivable situations
  - Example: Verifying a caller in a support center
- Escalate grey areas, resolve them, and add them to the policy
- **Teach people to blame the policy!**
- **Test** the policies/procedures/processes

Technology

- Don’t assume that the internal network is secure
  - Implement least privilege, defense in depth
  - Create security zones within the company
  - Consistent equipment, configurations, patching
  - Secure builds
  - Turn off auto-run, macros, scripting languages if not needed

Technology

- Positive security model: define what is allowed, not what is disallowed
- Assume that bad guys are already in your network when architecting it
  - Internal IDS/IPS, Firewalls
  - DLP/Honeypots
  - AV as a last resort – don't rely on it
  - Audit everything relevant!

Conclusion

- Social engineering is easy to perform, hard to defend against
- It can be slowed down with thorough application of basic security principles inside your perimeter
- People, process and technology all are critical components in a defense strategy

Questions?