Infosec - Where is your weakest link?

Information Security's Weakest Link in an Organization is the Human Factor.

The two most successful attacks that have the ability to cripple an organization.

- Social Engineering
- Technology Errors

What is Social Engineering?

- **Social Engineering is the art of human hacking.**

- **Social Engineering is broken down into two base attacks:**
  - Human based attacks “Employees”
  - Computer based attacks “Information Technology”

Human based attacks "Employees"

We often hear and read that humans are the greatest weakness in corporate, government, and even personal security. I do believe this is true.

Most Successful Human Base Attacks:

- Piggybacking, tailgating
- Identity theft, impersonation (via phone or personally)
- Shoulder surfing
- Ask for help from victims
- Give assistance or kindness to victims (and then ask for a favor
- of them)
- Bribe and intimidation
- Dumpster diving

Computer based attack types "Information Technology"

Hackers tend to use high-tech attacks, but they also know that the easiest is the Human factor.

- Spam and fake websites
- Phishing- attempting to obtain sensitive information such as usernames, passwords, and credit card details
- Smishing-is a security attack in which the user is tricked into downloading a Trojan horse, virus or other malware onto his cellular phone or other mobile device
- Whaling-a phishing attack that is specifically aimed at wealthier individuals. (Executives)
- Malwares, Trojan horses
- Baiting-is like the real-world Trojan Horse that uses physical media and relies on the curiosity or greed of the victim

Why Does “Social Engineering” Work?

All of the social engineering attack types are based on weaknesses of human factor. Most of the people have exploitable attributes; these can be sorted into three main categories.

- Behavior
- Job Function
- Human Factor

Why Does “Social Engineering” Work?

First one of these are the behavior attributes that depend on the personality.

- Helpful
- Naïve
- Open minded
- Curious
- Inquiring
- Friendly
- Social Networking

Why Does "Social Engineering" Work?

The second group is influenced by the job, the type of work. For example, employees working as "Helpdesk" assistants at a large company often work with colleagues unknown to them, they solve problems, answer questions, and help the coworkers.

- Young, new employee
- Working with unknown people often
- Dissatisfied with his/her work or colleagues
- Corruptible
- Easy to manipulate

Why Does "Social Engineering" Work?

The last group of attributes is based on the "moment," attitudes that are triggered by the circumstances.

- Tiredness
- Forgetful
- Overload work load
- Lazy
- On holiday and/or Illness
- Angry

Why Does "Social Engineering" Work?

"Social Engineering (SE) is a blend of science, psychology and art. While it is amazing and complex, it is also very simple." -http://www.social-engineer.org/

- Social Engineer Toolkit (SET)- Is a platform with advanced attacks against the human element.
- SearchDiggity 3.1-Uses Google Hacker Database
- Social Media-Twitter, LinkedIn and Facebook
- Google Earth
- Impersonation-Business Cards & Badges

Methods of Preventing Social Engineering

There is no full proof plan to prevent an attacker from gaining access to your network, facility, employees and proprietary information.

Tips to Prevent Social Engineering:

- Training, Training, Training!!!
- Improvement of Security Awareness-separate trainings for all “general” users, for management, and for the I.T. staff.
- Rules and Responsibilities
- Clean Desk Policy
- Internal Audits
- Hire a Third Party to Test Policies and Procedures

Technology Errors "Human Factor"

Essentially all Software, PCs, Servers, Websites and Network Devices are Designed and Maintained by a Human in some capacity.

The goal of technology security is to maintain the confidentiality, integrity, and availability of information resources in order to enable successful business operations.

Technology Errors "Human Factor"

What are there weaknesses?

- Website(s)-Was it built with the mindset of best practices and standards using Open Web Application Security Project (OWASP Top 10)?
- Software / Proprietary Software- Secure Coding & Bugs
- Communication Security- SSL/TLS and Perfect Forward Secrecy - Is PII, Credit Cards, ePHI and data secure in transit or at rest?
- Database Security-Practice the principle of least privilege
- System Configuration - Use Checklists, Software Management and Images for setting up network devices, servers and PC's
- Authentication and Password Management

Methods to Preventing Technology Errors

A bit different from social engineering but there are ways to secure an organizations technology but remember there is still a human factor involved, so there will be errors and weaknesses.

Tips to Prevent Technology Error(s):

- Don’t role out a new website or product with out testing and enforcing best practices and testing in a production environment.
- Use Tools to Maintain and Monitor Security.
- Think Security Minded when setting up and maintaining devices
- Internal Audits.
- Hire a third party to review policies, procedures and perform a security assessment.

Contact Information

Neil Gonsalves

Founder and CEO

www.AARC-360.com

Neil.Gonsalves@AARC-360.com

Tel: +1 (866) 576-4414 ext. 101

Cell: +1 (678) 458-0912

Christopher Berberich

Senior Information Security Consultant

www.AARC-360.com

Chris.Berberich@AARC-360.com

Tel: +1 (866) 576-4414 ext. 103

Cell: +1 (727) 287-8808

Questions