CERT'S PODCASTS: SECURITY FOR BUSINESS LEADERS: SHOW NOTES

Getting in Front of Social Engineering

Key Message: Helping your staff learn how to identify social engineering attempts is the first step in thwarting them.

Executive Summary

Social engineering attacks are often used in combination with other attack methods to gain unauthorized access. They are difficult to detect (and thus defend against) because the type of information that attackers seek is often identical to information requests from legitimate inquiries. People are the greatest source of vulnerability, given that human beings tend to be trusting by nature. But there are techniques that you can use to better arm your frontline staff to identify, report, and therefore thwart these types of attacks.

In this podcast, Gary Hinson, an IT governance specialist with expertise in building security awareness, discusses social engineering and how to mitigate the risks caused by this form of attack. Gary also manages two popular websites: NoticeBored.com and ISO27001security.com.

PART 1: WHY WE'RE SUSCEPTIBLE

Social Engineering Defined

According to Kevin Mitnick, social engineering "is a form of hacking that relies on influencing, deceiving, or psychologically manipulating unwitting people to comply with a request."

Why Social Engineering Is Difficult to Detect

Social engineering attacks are difficult to detect (and thus defend against) because the type of information that attackers seek is often identical to information requests from legitimate inquiries, such as those made to a help desk or call center.

Social engineers exploit human beings' tendency to be quite trusting – they use information that makes them seem legitimate and credible Each call, even unsuccessful ones, adds to their knowledge – for the next call.

Social Engineering and Security Breaches

Social engineering is likely a part of most directed attacks where the attacker is targeting a particular company or person. Phishing is a classic example where the attacker seeks personal information through what looks like a legitimate email. Spear phishing is a more targeted version of this type of attack.

Fundamentally, we all are social engineers, using a variety of approaches to obtain information from others. Attackers who use social engineering can be paid to obtain information or may use social engineering with criminal motives such as identity theft.

People are the primary source of vulnerabilities when it comes to social engineering as most are trained to be helpful when in a customer service role. Attackers can use pressure tactics such as "I need this information right now. I've got the chief exec waiting on the phone. Do you want to keep him waiting?"

Information that is susceptible to social engineering includes user IDs, passwords, and other account and identifying information. Social engineers seek information that will build their credibility, such as:

- general information about the company and its employees
- name of projects and names of physical sites
- company lingo, terms for the way things are done, and the names of procedures
- company IDs' structure (first name, last name; last name, initial)
- physical maps of company facilities and locations
- telephone directories and a list of user names
- emails with a long carbon copy (cc) list

Inquiries of this type can sound quite innocent when coming from a skilled attacker.

PART 2: IDENTIFYING SOCIAL ENGINEERING ATTEMPTS AND ATTACKS

Training Is Key

Raising awareness and conducting regular training are key, given that the only truly effective control is through people. It is imperative to:

- make people aware of the possibility that they might be socially engineered
- give them tools and techniques to identify social engineering attempts and attacks
- make sure they know who to contact if they receive a suspicious inquiry
- have clear, enforced policies and procedures in place

Use the Experience of Your Frontline Staff

Frontline staff such as personal assistants, secretaries, and call center staff deal with unknown callers all of the time. They are in the best position to be trained on detecting social engineering attempts, given their expertise with screening calls.

An effective social engineering training technique is to treat suspicious callers as though they were a pushy sales representative – and then try to deflect them by asking for more information, asking them to call back later, or asking them to send an email to verify that they are a legitimate caller. This, in effect, turns the tables on them.

A legitimate caller will take the time to provide more information.

PART 3: DETECTIVE, CORRECTIVE, AND PREVENTIVE ACTIONS

Getting a Handle on Social Engineering

People don't realize that they've been fooled – and when they do, they don't like to admit it. It is likely hard to detect an attack in progress based on an isolated event. A serious social engineer will make a number of attempts over days and weeks.

People don't realize that they've been fooled – and when they do, they don't like to admit it. It is likely hard to detect an attack in progress based on an isolated event because a serious social engineer will make a number of attempts over days and weeks.

However, if you train people to report suspicious calls to a central point and then correlate this information, there is an opportunity to identify an attack that is underway and send out an alert.

This helps raise awareness, even if it is a false alarm. Moreover, this process can serve as a preventive control.

An organization's incident response process can be used for managing social engineering attempts and attacks.

Creative Approaches to Training

Periodic, mandatory training approaches are not very effective. The content just doesn't stick for very long.

Approaches that result in much more regular contact with employees include:

- A topic of the month delivered in person (seminars, lunch meetings), via newsletters, and posted on the company intranet. This practice:
  - continuously reinforces the selected topic over a 30-day period,
  - recognizes different people's communications preferences, and
  - ensures monthly topics refer to and enforce one another.
- Case studies and scenarios – getting staff members involved in determining what they would do in a given social engineering situation.
- Puzzles, crosswords, and competitions - they can make any topic more fun to learn about.

Resources

Hinson, Gary. "Social Engineering Techniques, Risks, and Controls." EDP Audit, Control, and Security Newsletter (EDPACS), April 2008.

Mitnick, Kevin & Simon, William. The Art of Deception: Controlling the Human Element of Security. Wiley, October 2003.

Mitnick, Kevin & Simon, William. The Art of Intrusion: The Real Stories Behind the Exploits of Hackers, Intruders & Deceivers. Wiley, 2005.

Winkler, Ira. Spies Among Us: How to Stop the Spies, Terrorists, Hackers, and Criminals You Don't Even Know You Encounter Every Day. Wiley, 2005.

NoticeBored.com

CERT's research and case studies on insider threat.