ASA

Risk Consultants

Research Note

The Art of Social Engineering

By: Devin Luco

Keywords: Cyber Attacks, Cyber Criminals, Cyber Risks, Cybersecurity, Cyber Threats, Information Protection, Social Engineering, Vulnerabilities

Abstract – This research note defines social engineering and discusses how it negatively affects organizations. It also provides recommendations on how to defend and protect against attackers using social engineering techniques.

ASA

Risk Consultants

Introduction

In today's information age, cyber threats are very real and will continue to be a concern for organizations. Cyber threats expose vulnerabilities in an organization's security infrastructure to gain valuable information, usually for financial gain. Cyber attacks can cause system disturbance and uncover information such as credit card numbers, passwords, and proprietary documents that can cost individuals and organizations from hundreds to billions of dollars. Sometimes cyber attacks are motivated by a personal vendetta or retaliation. For example, in late March 2013, a Dutch-firm retaliated with a global denial-of-service attack that caused a web disruption for millions of users after the company was placed on an anti-spam blacklist.[1] Regardless of the motivation, not all threats are considered technical or require expert knowledge in a particular coding program. In fact, a very popular threat that is used by cyber criminals is one that is non-technical and more so psychological. This form of security threat is one that plays on the emotions of humans and takes advantage of our natural desire to be trusting. According to Forbes.com, the number one security threat of 2013 that has been identified: *social engineering*.[2]

What is Social Engineering?

There are different ways to define social engineering. The following definition of social engineering was given to IT professionals during a 2011 global survey:[3]

> *"Social Engineering is the act of breaking corporate security by manipulating employees into divulging confidential information. It uses psychological tricks to gain trust, rather than technical cracking techniques. Social Engineering includes scams such as obtaining a password by pretending to be an employee, leveraging social media to identify new employees more easily tricked into providing customer information, and any other attempt to breach security by gaining trust."*[4]

The purpose of this survey, which included IT professionals in the United States, United Kingdom, Canada, Australia, New Zealand, and Germany, was to understand the overall industry awareness of social engineering incidents and how it affects organizations.[5] The results demonstrate an issue that still plagues organizations today. The survey showed that 97% of security professionals were aware that social engineering is considered a threat and 43% of those individuals claim they or their organization have been a victim of social engineering tactics.[6] Clearly, attackers are using and will continue to use social engineering to gain valuable information from others.

Social engineers use four basic philosophies:

1. Being confident and attracting attention rather than hiding and looking suspicious.[7]
2. Giving you something and building trust.[8]
3. Using humor as a common tool to get people's guard down.[9]
4. Requesting and then providing a reason that sounds legitimate.[10]

A social engineering attack can occur at any time and any place. It does not just impact businesses but it can also impact individuals. Regardless if a potential target thinks he or she may not contain any valuable information, individuals are targeted for a reason. They have something valuable that attackers want. Criminals using social engineering techniques can gain valuable insight such as passwords, user names, addresses, phone numbers, and much more. With one small piece of information, an attacker using social engineering can create an entire portfolio on a target. Before you know it, he or she may have your entire identify to use at his or her disposal.

Impact to Organizations

What does this mean for an organization? Many organizations have security measures, such as passwords, encryptions, and locks, in

place to protect company software and hardware. At the very least, many organizations use badge readers, keys, and front desk receptionists to secure entry and deter unauthorized personnel from entering.

These measures often do not protect against social engineers. For example, have you ever held a door open for someone while entering a building? Often in buildings that require an electronic key or badge to enter, criminals using social engineering tactics will wait outside until someone enters the building. At that time he or she will ask you to hold the door open because "I forgot my badge (key) at my desk" or another reason similar to this. The natural thing to do is feel empathy and let this person in without much thought. However, this is what a social engineer is hoping for. Once the unauthorized person is in the building, they have access to whatever is inside and, if desired, let additional unauthorized people through the door to help with the crime. Chris Nickerson, founder of a Colorado-based security consultancy firm, states that this tactic of following others into a building is known as "tailgating."[11] Nickerson has conducted a number of security penetration tests using social engineering practices. He also states "a cigarette is a social engineer's best friend."[12] Many of his tests begin by

joining a "fellow" co-worker in a common break area outside, usually a designated smoking area.[13] While Nickerson gains the trust of employees outside, he is rarely asked for identification when break is over and it's time to enter the building. Most employees assume he is just another employee, rather than a consultant who is testing the company's security procedures.

There are other ways social engineering can harm an organization. Attackers can also use the phone as a primary means to gain information. Sal Lifrieri, a social engineering specialist for Protective Operations, describes methods social engineers use to lure targets into giving information.[14] According to Sal, social engineers learn the corporate jargon and may call posing as an employee of the same company or an authoritative organization.[15] One trick social engineers use over the phone is recording the music that is played when placed on hold.[16] This will gain the trust of the target and will be willing to provide information with little effort from the attacker.

Recommendations

Defending yourself against social engineering is not a perfect science. However, the first step to protection is awareness. Of course, being aware will not keep you safe as statistics show that most security

professionals are already aware of social engineering. However, knowing how to identify what an attack looks like and being cautious will also help in your defense. For organizations, conducting and keeping up-to-date awareness training for employees will be essential for security.[17] Lifrieri states in his trainings "…you always need to be slightly paranoid and anal because you never really know what a person wants out of you."[18] This attitude will need to be reiterated in staff awareness trainings to form an understanding that security is important.

In addition to awareness training, employees should always follow procedure in regards to releasing information.[19] Employees should be trained to question when someone is making a request and should not be hesitant to ask for identification. Treat the information at your organization as your own and be sure to inform a manager or supervisor when a request for information seems out of the ordinary.[20]

Continuous monitoring and testing are additional ways for an organization to fight against social engineering.[21] Monitoring company systems and conducting internal tests using social engineering strategies will reveal where a company's vulnerability points are. When vulnerabilities are identified, an organization can properly assess how a

solution will be implemented.

Conclusion

Heading through the year 2013 and beyond, cybersecurity will continue to be a rising concern. Social engineering is considered one of the top cybersecurity threats of the year, mostly due to the fact that it does not require technical knowledge. People will be targeted because human error and vulnerability is the easiest to take advantage of. It will be important for organizations to train employees to be aware of these attacks and be cautious when things do not feel right. There is not a perfect way to defend against this particular attack; but understanding what social engineering looks like and listening to your gut will be key in helping keep yourself and your company safe.

ASA

Risk Consultants

References

[1] Warman, Matt and agencies. "Web slows under 'biggest attack ever.'" The Telegraph. 27 Mar 2013. Web. 4 Apr 2013. <http://www.telegraph.co.uk/technology/internet-security/9957063/Web-slows-under-biggest-attack-ever.html>

[2] Teller, Tomer. "The Biggest Cybersecurity Threats of 2013." *Forbes.com*. 5 Dec 2012. Web. 4 Apr 2013 <http://www.forbes.com/sites/ciocentral/2012/12/05/the-biggest-cybersecurity-threats-of-2013-2/>

[3] Check Point. "The Risk of Social on Information Security: A Survey of IT Professionals." *Dimensional Research*. 1 Sept 2011. Web. 4 Apr 2013. <http://www.checkpoint.com/press/downloads/social-engineering-survey.pdf>

[4] Check Point, n. pag.

[5] Check Point, n. pag.

[6] Check Point, n. pag.

[7] Goodchild, Joan. "Social Engineering: The Basics." *CSO Security and Risk*. 20 Dec 2012. Web. Apr 5 2013. <http://www.csoonline.com/article/514063/social-engineering-the-basics>

[8] Goodchild, n. pag.

[9] Goodchild, n. pag.

[10] Goodchild, n. pag.

[11] Goodchild, n. pag.

[12] Goodchild, n. pag.

[13] Goodchild, n. pag.

[14] Goodchild, n. pag.

[15] Goodchild, n. pag.

[16] Goodchild, n. pag.

[17] Goodchild, n. pag.

[18] Goodchild, n. pag.

[19] Olavsrud, Thor. "9 Best Defenses Against Social Engineering Attacks." *eSecurity Planet*. 19 Oct 2010. Web. 6 Apr 2013. <http://www.esecurityplanet.com/views/article.php/3908881/9-Best-Defenses-Against-Social-Engineering-Attacks.htm>

[20] Olavsrud, Thor, n. pag.

[21] IT Business Edge. "Five Ways to Protect Your Organization Against Social Engineering." *IT Business Edge*. 2012. Web. 6 Apr 2013. <http://www.itbusinessedge.com/slideshows/show.aspx?c=81193>