The Dynamics of Social Engineering and Cybercrime in the Digital Age

Dr. Nabie Y. Conteh

Assistant Professor of Computer Information Systems
Department of Computer Information Systems,
College of Business & Public Administration
Southern University at New Orleans,
6801 Press Drive, Suite 108, Louisiana 70126
USA

DeAngela "Dee" Sword

University of Maryland University College
Adelphi, Maryland
USA

Abstract

Social engineering attacks have emerged to become one of the most problematic tactics used against businesses today. Social engineers employ both human based and computer based tactics to successfully compromise their targeted networks. This paper will discuss the basics of social engineering and what it means today.It will explain some common attack methods like baiting, phishing, pretexting, quid pro quo, tailgating and dumpster diving. It will then highlight the impact social engineering has had on the rise in cybercrime and why threat actors have grown more innovative. Finally, this paper will discuss what Multi-Layer Defense or Defense in Depth is and offer countermeasures that can be enforced to defend against social engineering attacks.

Keywords: Social Engineering, Phishing, Multi-Layer Defense, Cybercrime*, *pretexting, quid pro quo, tailgating and dumpster diving

The Re-Emergence of Social Engineering in the 21st Century

Introduction

Social engineering, also known as human hacking, is the art of tricking employees and consumers into disclosing their credentials and then using them to gain access to networks or accounts. It is a hacker's tricky use of deception or manipulation of people's tendency to trust, be corporative, or simply follow their desire to be explore and be curious. Sophisticated IT security systems cannot protect systems from hackers or defend against what seems to be authorized access. People are easily hacked, making them and their social media posts high-risk attack targets. It is often easy to get computer users to infect their corporate network or mobiles by

luring them to spoof websites and or tricking them into clicking on harmful links and or downloading and installing malicious applications and or backdoors.

Around the year 1250 $_{B.C}$, the Trojan War between the people of Troy and the Greeks had begun. It was not until 10 years later when the Trojan horse was erected and left outside of the city of Troy. The Trojans accepted the horse as a peace offering and pulled the mysterious gift into the city. A small group of Greek warriors laid awake inside of the horse as the city of Troy erupted in celebration. Once the city grew quiet, the Greeks climbed out of the wooden horse to let the rest of the army into the city. The Greeks wereable to siege the entire city putting an end to the Trojan War before anyone could be alerted (Peters, 2015). Nearly 3,000 years later similar tactics are being used to exploit weaknesses in human behavior to achieve personal gains. Cybercriminals are capitalizing on people's tendencies to be helpful, trustful, and/orlazy with intention of gaining access to desired information or controlled areas. (Thapar, n.d.). Over the span of 5 years, companies like RSA, Target, and Twitter have been victims of sophisticated social engineering attacks. Each company has spent or lost millions of dollars in effort to recuperate from such attacks. As the Digital War between Cybersecurity professionals and Cybercriminals wages on. It is now more advantageousfor organizations to understand the various types of social engineering attacks, how social engineering has stimulated cybercrime and incorporate countermeasures to prevent social engineering attacks than it has ever been before.

Social Engineering Defined

Social Engineering is a form of deception that hackers use to acquire sensitive information, access tounauthorized infrastructure and facilities. There are two main categories under which all social engineering attempts can be classified either technology based deception or human based deception (Thapar, n.d.). With technical tactics, the social engineer uses computer applications to trick users into carrying out a specific action. On the other hand, human based tactics are performed by attackers who understand flaws in human psychology. Businesses should be conscious of both categories of social engineering tactics because each approach could lead to a compromised network. The following are various types of social engineering attacks but attackers are not limited to only these methods:

Baiting: A hacker preloads malware onto external storage devices (i.e. CDs or USBs) and strategically leaves them in public areasof the targeted business. Unsuspecting employees then pick up these CDs or USBs labeled company info and plugs it into their computers.

Phishing: Social engineers send fraudulent emails that may look legitimate to recipients. The email may request an action such as disclosing sensitive information or clicking a malicious link.

Pretexting: The malicious actors use dishonesty to retrieve valuable information about the person or company. The attacker calls an employee and request him or her to validate their username and password for security purposes.

Quid pro quo: The social engineer preforms a good deed for the victim in hopes of gaining their gratitude. The victim is then more likely to return the favor with a favor.

Tailgating: The malicious actor waits near an entrance until authorized personnel enters and follows the employee into the controlled area.

Dumpster Diving: Attackers rummage through a company's dumpster or trash cans with hopes of finding useful information about the company, its employees and the network.

Rise in Cybercrime

Cybersecurity incidents are not only increasing in number, they are also becoming progressively destructive and target a broadening array of information and attack vectors (Beard, Mickelberg, Stapf, &Ulsch, 2015). Similar to business networks that are investing in technologies, sharing intelligence and training their employees so are cybercriminals. Malicious actors are persistently improving their tactics, techniques and procedures (TTPs) to become more effective at what they do. These threat actors have recognizedhow lucrative the cybercrime market is and are allocating resources to add more sophistication to their strategy. Social engineering enhances attack vectors by offering apolymorphic disguise that isdetrimental to information security.Attackers incorporate social engineering techniques to execute initial reconnaissance, penetration, gaining a foothold, appropriating privileges and internal reconnaissance (Kostadinov, 2013).This allow perpetrators to exploit more weaknesses and sustain a longer presence on a compromised network. Both of which have contributed to a spike in success rates and increase in cybercrime. Below are some statistics presented in the 2015 ISACA and RSA Conference Survey that identifies the types of threat actors and successful attacks reported in 2014.

Threat actors of 2014*(636 Respondents)*

- 45.6% Cybercriminals
- 40.72% Non-malicious insiders
- 40.09% Hackers
- 28.62% Malicious insiders
- 19.81% Hacktivists
- 17.45% Nation State

Successful Attack Types of 2014 *(704 Respondents)*

- 68.32% Phishing
- 66.48% Malware
- 50.14% Hacking attempts
- 46.45% Social engineering
- 43.89% Loss of mobile devices
- 25.28% Insider theft

- 21.88% SQL injections
- 11.08% Man-in-the-Middle attacks
- 7.53% Watering hole

Preventing Social Engineering

It is evident that regardless of how technologically secure a network seems the human element will always be a vulnerability. The success rate and number of cybercrimes are steadily on the rise due to the level of anonymity social engineering offers malicious actors. Businesses have to remain cognitive of the various threat actors and their plethora of attacks so they are able respond accordingly. There are technical and non-technical safeguards that can be implemented to lower the risk associated with social engineering to a tolerable level. Companies are adding multiple layers to their security schemes so that if the mechanism in the outer layer fails, a mechanism in at least one inner layer can help prevent a threat from turning into a disaster (Risk Mitigation). This concept is known as Multi-Layer Defense or Defense in Depth. A good Defense in Depth structure includes a mixture ofthe following precautionary measures:

Security Policy: A well written policy should include technical and nontechnical approaches that is downward driven by executive management. Every organization should integrate security into their operational objectives.

Education and Training: Employees ought to be required to attend initial training during orientation and recurring refresher trainings. This builds awareness by exposing users to commonly employed tactics and behaviors targeted by a social engineer.

Network Guidance: The organization have tosafeguard the network by whitelisting authorized websites, using Network address translation (NAT), and disabling unused applications and ports. Network users have to maintain complex passwords that are changed every 60 days.

Audits and Compliance: Organizations have to actively verify that theirsecurity policy is being adhered to. Some detective controls include reviewing network logs, validatingemployees' permissions, and checking desktop configurations at least bi-monthly.

Technical Procedures: The network should have multiple layers of defense to protect data and core infrastructure. Software like Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS) and firewalls should be installed onevery device. Demilitarized Zones (DMZ), web filters and Virtual Private Network (VPN) should be installed on all external facing services.

Physical Guidance: There are a range of options that can be implemented to protect physical assets. Using a combination of security guards, mantraps and security cameras to deter intruders from entering the premises is beneficial. In places where physical hardware is located businesses should employ multifactor authentication, biometrics or access control list before access is granted.

Conclusion

In summary, social engineering is not something that is new but is a skill of deception that has been used for years. The world continues to grow technologically dependent and malicious actors are anxious to exploit this dependencyin order to gain the monetary profit or recognition they desire. The expansion of smartphones and social media has provided cybercriminals with new avenues of attack which they have taken full advantage of. Cyberattacks have become so prevalent because social engineering is hard to detect and can be added to various attack vectors.Both sides are investing lots of time, money and other resources in effort to defeat one another in a Digital War wherethe environmentis ever changing. Unfortunately, social engineering has reemerged and has proven to be just as effective in the 21stCentury as it was in the past.

Reference:

Beard, C., Mickelberg, K., Stapf, E., &Ulsch, D. (2015, July). US cybersecurity: Progress stalled. *PWC*, pp. 3. Retrieved from http://www.pwc.com/cybersecurity

Course Material: Risk Mitigation: Defense in Depth, University of Maryland University College. Retrieved from https://learn.umuc.edu/d2l/le/content/133521/viewContent/4176011/View

Information Systems Audit and Control Association &Rivest Shamir Adleman. (2015). State of cybersecurity: Implications for 2015. *Cybersecurity Nexus*. Retrieved from http://www.isaca.org/cyber/Documents/State-of-Cybersecurity

Kostadinov, D. (2013, March 22). The cyber exploitation life cycle. *InfoSec Institute*. Retrieved from http://www.resources.infosecinstitute.com

Peters, S. (2015, March 17). The 7 best social engineering attacks ever. *InformationWeek*, pp. 1. Retrieved from http://www.darkreading.com

Rouse, M. (2014, November). Social engineering definition. *TechTarget*. Retrieved from http://searchsecurity.techtarget.com

Thapar, A. (n.d.). Social Engineering - An attack vector most intricate to tackle. *CISSP*. Retrieved from http://www.infosecwriters.com