Threats in Information Security

John Dennett

Professor Adams

Saint Leo University

COM 416

Threats in Information Security

Information in today’s world is continuously under some form of threat. Those threats, whether it be social engineering, phishing, or even bring your own device (BYOD), are constantly present with a continuous need for preventive maintenance. Threats to information security can be incredibly broad in scope, so for research purposes, social engineering will be the focus.

Social Engineering

Data breaches tend to occur through a business first. Usually businesses that handle sensitive information such as credit card numbers are the targets, and the breaches are to benefit the attacker. There are many ways a business and its data can be compromised. The methods, as mentioned before, include phishing and BYOD. Greitzer explains the concept of what social engineering is in the following passage:

> Social engineering represents a type of confidence scheme aimed at gathering information, committing fraud, or gaining computer system access. Social engineering, almost by definition, capitalizes on human psychology, such as cognitive limitations and biases, which attackers exploit to deceive the victim (Greitzer 2014)

According to Greitzer (2014) and his findings, many researchers break social engineering up into two different categories: human based and technology based. Some attacks can be described as a hybrid of the two categories, where it is human based through the use of technology, such as phishing, spear phishing, and ransomware. An example of a human-based social engineering attack would be shoulder surfing or following an employee behind a locked door. These methods retrieve information without the attacker necessarily having to use technology to acquire it, whereas technology-based methods require the utilization of technology at some point or another in order to retrieve the desired information, such as phishing or other deliberate attempts to rob an individual or company of private information.

Phishing

Touching on the first concept that falls under social engineering includes the malicious attack called phishing. Phishing can be relatable to fishing in the bait-and-hook sense, where the attacker lures a victim to proceed with a specific action, usually with an e-mail. Zielinska describes phishing as “a social engineering tactic used to trick people into revealing personal information” (Zielinska 2016). Phishing is a serious threat when it comes to the security of data. From a business standpoint, while the victim may have no intention of purposely releasing sensitive information, procedures are still needed to prevent accidents made on human error.

> The insider threat is recognized as a major security risk by computer and organization security professionals, more than 40% of whom report that their greatest security concern is when employees accidentally jeopardize security through data leaks or similar errors (Greitzer 2014).

With phishing being a serious threat, businesses must look for ways of mitigating the damage caused by human error on their part with their employees by keeping them informed. Some of the factors that contribute to this human error are job and time pressure, prolonged workloads, and high email loads. Stress and workload contribute to workplace fatigue, making an employee susceptible to becoming a victim to a phishing attack. A single overworked employee who opens a malicious email could jeopardize the entire company.

Some of the proposed mitigation strategies to avoiding these factors include starting with creating “productive and healthy work environments” (Greitzer 2014). This strategy involves management strategies to reduce employee stress and workload and keeping the employees alert and aware of the various attacks. Greitzer provides other mitigation strategies that include “developing automated defense tools to better recognize email threats and applying data loss prevention software to recognize possible harmful sites” (Greitzer 2014).

Spear Phishing

Another variation of phishing to consider is Spear Phishing. Spear phishing’s objective is to retrieve information from one specific person. The methods of attack are changed depending on the target. For example, an email could be sent to someone working in a specific position within a company. This phishing email would contain information pertaining specifically to the receiver in hopes of retrieving the desired resources. Various social engineering strategies could easily equip the attacker with the knowledge necessary to make the attack appealing to the target. While this method may be more effective, it doesn’t reach as wide of an audience as the standard phishing method would bring.

Bring Your Own Device

What some may deem perfectly fine, but what is also slowly becoming a social engineering threat to businesses and their information, is the practice of ‘bring-your-own-device’, or BYOD. BYOD is straightforward in its definition; employees belonging to a business are allowed to bring their electronics and, depending on the business, these electronics could include anything from phones, tablets, and laptops to flash drives, external hard drives, and CDs.

Mobile Device Security

Mobile devices, such as smartphones and laptops, present a prolific and easily accessible avenue for attackers to gain entrance into a corporation with malicious intent; they also open the doors for attacks against the individual owners of the devices. Mobile devices, including smartphones, are susceptible to many of the same threats that exist with non-mobile devices and networks; however, most users do not protect against these threats, and many are not even aware of the threat. The social engineering aspect of data security is given a leg up with the addition of mobile devices: “Mobile systems are especially vulnerable to direct attacks, because hackers can locate and observe potential victims in person, and have more opportunities to intercept insecure wireless network traffic” (Friedman & Hoffman, 2008, p. 165). Social engineering hackers can refine their approach when choosing which tactic will make the target more likely to open a malicious email or even text. Once that message is open or link is clicked on, the phone falls into the possession of the hacker.

Corporations that utilize a BYOD policy create an environment in which employees may walk into the door carrying a hacker in their pocket. Once a phone has been corrupted through phishing or another malicious attack, the phone can then be utilized to gain access to corporate information such as email lists and passwords, and the phone or laptop can be used as a tool through which the hacker can attack the corporations’ firewalls from inside the building.

Ransomware

Ransomware is another form of attack that is making it more difficult for BYOD to be viable in a business setting. Ransomware involves a malicious intrusion on an operating system that will usually lock or encrypt the user’s files. After the data has been compromised, it is then held for ‘ransom’. Lump sums of money are then demanded for the attacker to decrypt the data that is at risk. Hilarie Orman gives a quick definition and examples of victims to ransomware in the next passage:

> The evil code encrypts all your files, deletes your backups, and asks for a Bitcoin payment in exchange for the decryption key. Hospitals, police departments, small businesses, and ordinary individuals have been faced with the choice of abandoning their data or paying the ransom. (Orman 2016)

Conclusion

When it comes to protecting information from a business standpoint, it is truly in the hands of the business itself and their employees to educate themselves on potential everyday threats. Just as technology changes rapidly, so do the mechanisms available to criminals who wish to utilize technology and the information contained within to their own gains. Constant vigilance and refinement of the mitigation strategies of phishing is required for all companies and employees, or anyone using technology for that matter, to realize the danger of simple gestures and follow policies. These same strategies can be applied for most other forms of social engineering threats, and it is important for all users of technology to become generally aware of the possible dangers of its operation.

References

Friedman, J., & Hoffman, D. V. (2008). Protecting data on mobile devices: A taxonomy of security threats to mobile computing and review of applicable defenses. *Information Knowledge Systems Management*, *7*(1/2), 159-180.

Greitzer F. L. et al., (2014) Unintentional insider threat: Contributing factors, observables, and mitigation strategies, doi: 10.1109/HICSS.2014.256

Greitzer, F., Strozer, J., Cohen, S. (2014). Analysis of unintentional insider threats deriving from social engineering exploits, doi: 10.1109/SPW.2014.39

Orman, H. (2016). Evil offspring – ransomware and crypto technology, doi: 10.1109/MIC.2016.90

Zielinska, O., Welk, A., Mayhorn, C., Murphy-hill., E. (2016). The persuasive phish: Examining the social psychological principles hidden in phishing emails, doi: 10.1145/2898375.2898382