Social Engineering & Network Security

Saint Leo University

COM 450 – Network Defense & Security

Instructor: Dr. Omar

Skye Cerrito

April 15, 2020

Social Engineering & Network Security

Abstract

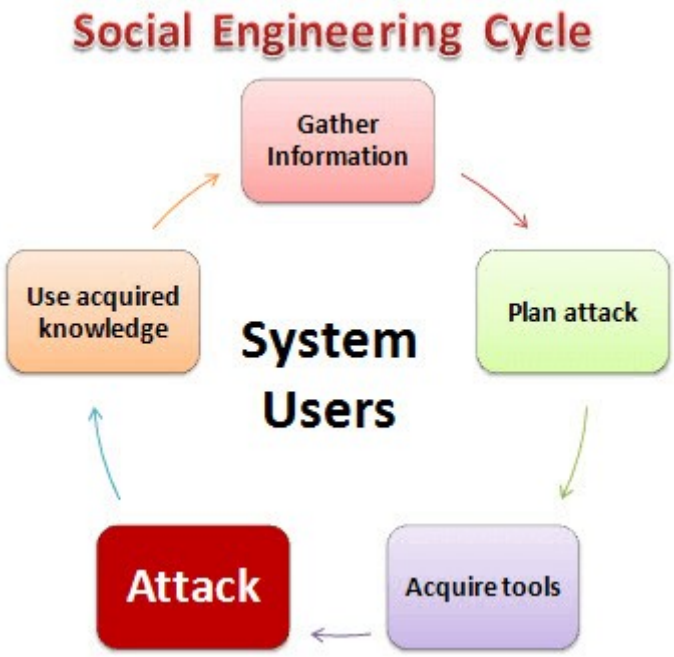
Social engineering has been the cause of many devastating data breaches in the past few decades and, unfortunately, this is not an attack solved by a simple technical fix. One could have all the latest security technology and preventative measures in place, but all it takes is one person to use your instinctive want to trust to infiltrate your system. This paper will be discussing social engineering and its effect on network security. It will go over what social engineering is, how the attack works, what it looks like, how to protect oneself from it and possibly prevent it altogether. This paper will also go over various techniques and methods used, as well as famous social engineering attacks.

Introduction

The term ‘social engineering’ was popularized by Kevin Mitnick, a world-famous hacker and author of the book, ‘The Art of Deception’ (Cihodariu, 2019). According to one source, the definition of social engineering is “an attack which needs human interaction and manipulation in order to succeed in accessing network locations, confidential information, etc.” (Cihodariu, 2019). Another source states that “social engineering is the art of manipulation, influencing, or deceiving you in order to gain control over your computer system (KnowBe4). Therefore, it would be safe to define social engineering as an attack done by the manipulation of people with the goal of obtaining confidential information, whether that be getting the information directly or getting access to the system with the information itself. Like most forms of malicious attacks, social engineering has a plethora of methods that are used on trusting victims. This, unfortunately, makes it difficult to prevent attacks as it cannot be prevented by a technical fix, due to it exploiting the victim’s trust as opposed to the victim’s machine. On the opposing end, hackers use social engineering because it is easier to exploit one’s trust than finding new methods of hacking software and devices (Webroot).

How Social Engineering Attacks Work

Keeping in mind that any attack involving psychological manipulation in order to exploit others is considered social engineering, we will now go into how these attacks work (Cihodariu, 2019). To do this, here is an example modeled by one found online (Goodchild, 2009). The attacker is attempting to gather information from a company via social engineering. Currently, the city in which the company resides, there is a holiday event that the people of the city have a tradition of doing.



(Cihodariu, 2019).

Continuing with the example, the first step of the attack would be to gather information. The attacker learns of the holiday event and believes that people who work at the company would either take the day off or be allowed to leave early to attend it. The attacker also used social media, such as LinkedIn, to find more information pertaining to the employees working there, and from there, may be able to gather the employee's other social media, i.e. Facebook, Instagram, etc. After finding these, the attacker can find out more on which employees plan to attend the event, what time they are leaving if they are not taking the whole day off, etc. The attacker may also gather information around the company, such as what other places of business there are, when the streets are busy and when they are not, etc.

Knowing this information, the attacker will then plan the attack. In this case, the attacker will plan to do so on the day of the holiday event. The attacker would keep track of the employees leaving the office; names, times they are leaving, positions. They

would also keep track of the area around the company and which times line up with the safest time for the attacker to perform the attack.

The next step, acquiring tools, can involve hacking tools once one gets into a system. However, it can mean many other tools as well. Remembering the example and that this attack revolves around exploiting trust, the attacker decides to find a cheap shirt with the company logo of a security company, say Fortinet, on it.

The next step is the attack itself. The attacker finds the optimal time to go to the company, shortly prior to one of the employees they had been keeping tabs on leaving for the holiday event. The attacker heads into the company and asks for the employee by name, fully knowing that the employee is in a meeting, which will end shortly, after which the employee will be in a rush to leave for the event. The employee at the front desk says the wanted employee is at a meeting, which will then prompt the attacker to find another way in. They say that they knew because the employee had been keeping in touch with them, then asks if there is a place nearby to eat. Fully knowing that the nearest restaurant was at least a few miles away, the employee states that the attacker can eat in their cafeteria. The attacker does so, then other employees allow him to go into the main office areas, and eventually the attacker was able to use the tools brought to steal information from the vacant offices. The attacker then plans their leave in time with the employee they were supposed to be meeting, leaving at almost the same time so the employee at the front desk would not suspect anything.

The last step is using the acquired knowledge. The attacker was able to fly under the radar and left backdoors open for them and a few of their hacker friends to exploit the company’s systems. They also left trick USB drives labeled ‘payroll’ or ‘risk

assessment 2019' which contained rootkits. Unsurprisingly, some employees plugged in the USB drives without a second thought. Finally, the attacker put a hook into a few machines, allowing them to still be obtaining information for a later date.

This was just one example; attacks can happen without the attacker even stepping foot into the place they are stealing information from. This next section will go into the various ways an attacker can obtain the victim's information, while still following the steps on the flowchart.

What Social Engineering Looks Like: Types and Examples

Previously, we went over one example in which the attacker went into the office physically. Of course, the attacker went in, fully knowing what they were trying to accomplish. However, there are many times where people with no malicious intent do a similar thing. This happens quite often at Saint Leo, specifically doors that need a keycard to get inside. Often times, one will open the door to their apartment building, and someone will ask them to hold the door, as they forgot their card. If the person holds the door, they just became the victim of a social engineering attack; this is because the other person, whether maliciously or not, exploited their trust allowing them to enter a building they may or may not have had access to. Of course, that is a less malicious example, however, the same can apply for any building, by people with malicious intent.

Another method is through the phone. Just like one can physically pretend to be someone, one can impersonate someone else via phone calls (Fruhlinger, 2019). An IT representative, law enforcement, auditor, etc. are all viable options that would make

most people feel the need to comply with their demands and, more importantly, feel the need to trust them.

The example from the previous section also used this method quite a bit in the information gathering phase. Social networking is making social engineering easier for attackers to commence their attacks on unknowing victims. Most of the time, people leave links to the rest of their social media as well. For example, on LinkedIn, one can also put their Facebook page, Instagram, Twitter, etc. as well. In other words, one the attacker finds one account, they can find the rest of them easily. With this, they can learn about the victim of choice, their likes and dislikes, their habits, and more. Attackers can also use online resources to find out and take advantage of news events, holidays, and the like. This is also like our previous example and the holiday event. Fake charities or shopping company scams are also fairly common when conducting these types of attacks (Fruhlinger, 2019). This also includes phishing attacks, posing as other well-known companies or people in order to gain the victim's trust. They can then send malware-laced attachments within those emails (Fruhlinger, 2019).

Famous Social Engineering Attacks

There are many social engineering attacks that have happened in the past decade or so. Some, however, have more serious repercussions than the rest. In this example, trust is being exploited but not as much as the victim's own greed is. The Nigerian 419 scam involves convincing the victim to help get "ill-gotten cash out of the country" and offering a portion of it in exchange (Fruhlinger, 2019). In 2007, the treasurer of a county in Michigan gave $1.2 million in public funds to a scammer in hopes of getting a payoff (Fruhlinger, 2019).

Another attack, one of Kevin Mitnick's early scams, involved him gaining access to Digital Equipment Corporation's OS development servers (Fruhlinger, 2019). He did this by calling the company and posing as one of their lead developers, claiming that he was having trouble logging in; immediately given a new login and password. This attack was done in 1979, but a similar attack was done in 2016, in which the hacker gained control of a U.S. Department of Justice email address.

Sometimes, all it takes is confidence to convince others to trust you. In 2015, employees at Ubiquiti Networks wired millions of dollars in company money to scam artists who were impersonating company executives (Fruhlinger, 2019). The scam artists used social engineering to not only impersonate higher ups but do it effectively enough to where people believed them enough to send them that quantity of money. This also entails phishing emails to a certain degree, as one can have confidence portrayed through how they write an email in a sophisticated and assured manner.

Social Engineering Techniques

Phishing and spear phishing are done by forging emails disguised as trustworthy entities to acquire information such as usernames, passwords, credit card information, etc. (KnowBe4). Water-Holing is another technique in which the attacker observes the target's most used websites and then uses vulnerabilities within the site to eventually infect the targeted group, thus gain access to their systems (KnowBe4).

Baiting is a technique as well, one used in our previous example; specifically involving the USB drives. The employee wanted the information on the drive, otherwise known as the bait, and the information ended up being a malicious file allowing the criminal to take the system over. The example from earlier also involved a quid pro quo

technique, simply meaning something for something. The attacker posed as a representative from Fortinet and was thought to have been there to assist another employee and received clearance to go into the main building. What the employee didn't know was that the attacker was there with malicious intent. Tailgating was also used, as the attacker, once inside, gained access to other areas of the building by following other employees inside, or asking to be let in because they forgot their keycard.

A honeytrap is a trick that is used with men, having them interact with a fictitious female online (KnowBe4). Men are known to be more trusting and vulnerable with a female, especially if they believe she is attractive; this is based on old spy tactics where a real female is used, thus this is a tried and true method (KnowBe4). Lastly, rogue is a form of malware that deceives users into paying for fake removal of malware (KnowBe4). This last one is more recent and is becoming a larger issue as it is popular and there is a plentitude of programs of this type.

Defense & Prevention Against Social Engineering

One cannot fully prevent social engineering, as mankind is born to trust others, starting with their mothers and continuing throughout their lives. However, with awareness of the many types and techniques used by hackers, one can get better at noticing these scams. In a company setting, training in security awareness is a must, and should be a regular training throughout the year (Fruhlinger, 2019). This training should also include real examples of past social engineering attacks to demonstrate how real these attacks are, and how easy it is to be tricked by them. Lastly, reviewing

and refining policies of the company, as well as going over exercises with all employees will allow them to learn and understand what attackers are doing currently.

Conclusion

In conclusion, social engineering is an attack that involves the manipulation of people and their trust which is, in most cases, too easily given, especially in the current state of the digital world. Devastating security breaches are happening on a regular basis and are not something of the past. Even worse, these attacks are not technical fixes, as this all relies on human nature and their errors. However, with regular training and awareness of these attacks, social engineering can be mitigated. Though, there will always be someone who, either out of innocence or mistake, will fall for one of the many social engineering techniques out there.

References

Cihodariu, M. (2019, Aug 29). *What is Social Engineering: The Tactics Used to Manipulate You.* Heimdal Security. https://heimdalsecurity.com/blog/what-is-social-engineering-tactics/

Fruhlinger, J. (2019, Sep 25). *Social engineering explained: How criminals exploit human behavior.* CSO. https://www.csoonline.com/article/2124681/what-is-social-engineering.html

Goodchild, Joan. (2009, Feb 4). *Social Engineering: Anatomy of a Hack.* CSO. https://www.csoonline.com/article/2123704/social-engineering--anatomy-of-a-hack.html

Nathaniel, S. (2018, May 24). *The History and Evolution of Social Engineering Attacks.* Commissum. https://commissum.com/blog-articles/the-history-and-evolution-of-social-engineering-attacks#

Social Engineering. KnowBe4. https://www.knowbe4.com/what-is-social-engineering/

What is Social Engineering? Examples & Prevention Tips. Webroot. https://www.webroot.com/us/en/resources/tips-articles/what-is-social-engineering