Threat to Information Assurance - Phishing

Nicholas Jacob

University of Advancing Technology

January 30, 2022

The world of information technology is ever changing and expanding. The industry is lucrative in both money and informational data. When an industry holds this much value there will always be those who wish to exploit it in non-ethical ways. These exploitations come in many forms and new intrusion techniques are being created and adapted every day. MITRE has created a matrix called ATT&CK in an effort to create a method for those in the cybersecurity field to use as a foundation for developing better security. In this matrix they breakdown the methods and steps used by those who would attempt to break or intrude in an enterprise's network with malicious intentions. Outlined are a few of the intrusions used, one of which being phishing. Phishing is one of the more popular intrusion techniques being used today. Many are more aware of this, and the method has a lower chance of success than in previous years but the fact that it is still employed in large quantities show that it is still working enough to make it a profitable means of intrusion. We will go over what phishing and some of its variations, the risk it poses to the enterprise networks, and what steps to take in an effort to detect and mitigate phishing attacks.

Phishing is a social engineering method that focuses on having a user let the perpetrator into the network by having the user open something such as a hyperlink or attachment most commonly sent by means of an email. The perpetrator can choose to target either a specific individual based on previous reconnaissance made or an entire group of individuals in an attempt at playing the numbers game. A common target in the modern day is the elderly as they are more trusting and less educated about the unethical techniques being used. Culprits will provide the target with a link to open which may be a download link for malware. This is a preferred method as opposed to attachments as most email providers have systems in place to inspect all attachments for malicious content. The link may not just be malware that you have given permission to download but may instead lead to a social engineering website. This website may be posed to look like a popular website you already use and ask you to log in using your username and password for the real site. Once you have “logged in” you have given them access to the information they need to get access to your account on the real website where they can steal further personal data or lock you out by changing your password to something new. The link may also instead send you to a website with a download button for an application you think you are going to be installing and instead its malicious code that you will then click okay and accept on assuming it is the application. The attachment phishing attempts will include attachments that are posed to look like documents, PDFs, or other files you may open on a regular basis. The email may also include instructions on how to open the attachment and further instructions that walk you through telling your device to allow the attachment despite possible security defenses already in place.

Phishing poses many risks to the enterprise. As already discussed, it is a viable way for a adversary to install ransomware, malware, and gain access to the network using real verified credentials. Another phishing attack may focus solely on the social engineering aspect and directly ask the targeted individual or individuals for the information they are looking for. What if an average office employee gets an email that looks like it is coming from an IT person they recognize and are asked to verify their log in information? It may not work on all, but it only needs to work once for that employee to hand over access to the network. Malware that gets installed usually has a purpose of allowing the perpetrator remote access where they can choose what to do from there or may be code with the purpose of seeking out information and sending it back to the perpetrator. If the data stolen is information of users it may violate privacy laws similar to HIPAA which are in place to protect the privacy of individuals. Not only will the enterprise have potentially lost the trust of those who's data was stolen but fines will be issued by the government. Ransomware has become more popular of late and is often used to encrypt all the data it can and asking for some monetary amount paid for the decryption code. This results in down time of production at minimum and possibly a ransom paid.

There will always be a risk of phishing, but systems can be put in place to detect and prevent success. Possibly the most effective method of prevention is simply a raise in awareness through training. If you remove the ignorance of it and teach employees the signs to identify a phishing scam then it limits the chances of it making past that vital step. After that antivirus and antimalware software on the network will scan for, detect, and quarantine all suspicious files automatically. Restricting access to employees and users to only files and parts of the network they need will prevent those who gain credentials from accessing more than select data. Restrict web-based content prevents network users from getting to known suspicious websites, and blocks downloads or attachments. Setting up multifactor authentication will also help prevent access to those who got log in information as they would still require an additional factor to gain access to the network itself.

Phishing is and will continue to be a popular intrusion technique for as long as there are those who continue to fall for the social engineering practices used. There are different types of phishing techniques, and each has its own purpose and goal. We risk the data of not just our users but possibly that of confidential company secrets. Ransomware and HIPAA fines are just a bit of the monetary risk involved. Training needs to be created and required to effectively mitigate risk. Systems need to be put in place in order to prevent breaches and protect the enterprise and its interests.

References

Centers for Disease Control and Prevention. (2018, September 14). *Health Insurance Portability and accountability act of 1996 (HIPAA)*. Centers for Disease Control and Prevention. Retrieved January 30, 2022, from https://www.cdc.gov/phlp/publications/topic/hipaa.html#:~:text=The%20Health%20Insurance%20Portability%20and,the%20patient's%20consent%20or%20knowledge.

KnowBe4. (n.d.). *What is phishing?* Phishing. Retrieved January 30, 2022, from https://www.phishing.org/what-is-phishing

Malware: What is malware & how to stay protected from malware attacks. Palo Alto Networks. (n.d.). Retrieved January 30, 2022, from https://www.paloaltonetworks.com/cyberpedia/what-is-malware#:~:text=Malware%20(short%20for%20%E2%80%9Cmalicious%20software,methods%20to%20infect%20computer%20systems.

Winther, P. (2021, October 18). *Phishing*. Phishing, Technique T1566 - Enterprise | MITRE ATT&CK®. Retrieved January 30, 2022, from https://attack.mitre.org/techniques/T1566/