**Cyber Security Threats**

Jose Flores

CSOL-501-01-SP22: Foundations of Cyber Security

Dr. Michelle Moore

January 17, 2022

Abstract

As we begin our journey in the cyber security world, we learn about new and recurring cyber threats. Some cyber threats are easily prevented by educating each other, and some are difficult to avoid. The following are the top ten cyber threats cooperation faces daily.

IP Hijacking & Cloud Hacking

An Internet Protocol (IP) address uses a unique numerical tag to identify internet-connected devices such as computers, smartphones, or similar devices. We have always seen our IP address on our devices when trying to troubleshoot our internet or connection. IP hijacking is when the hijacker overtakes the victim's IP address and is used for criminal activity. This critical security threat devalues internet-enabled cloud services' integrity and trust (Liu et al., 2014). Hackers access the account and what is stored when they take over a cloud account. Another way to attack the cloud account is by denial of service. When the denial of service attack is performed on the cloud, it prevents the cloud’s ability to perform its functions or services (Masdari & Jalali, 2016).

Man in the Middle & Denial of Service

I believe the man-in-the-middle attack technique is a cyber security threat organizations face today because the attacker has already compromised the company’s trusted system and is waiting to strike. Especially in a financial company, the attacker might be waiting to take advantage of an email regarding account fund transactions. Another type of man-in-the-middle attack technique is IP spoofing. The attacker modifies the IP address to disguise itself as the receiver (Sun et al., 2021). Victims who use public Wi-Fi are vulnerable to these attacks due to the unsecured network and the unknown location of the attacker. The denial-of-service attack is not intended to gain any assets or knowledge but is meant to cost time and money for the victim. The attack is made by overwhelming the receiver system with information triggering a temporary halt or crash. We may see this cyber attack throughout the holidays without realizing it. Due to the pandemic, online shopping is in high demand to reduce the spread of COVID-19. We, as buyers, might overwhelm the online services causing it to crash, or it may be a denial of service attack on the website.

Insider Threat & Lack of Knowledge

The insider threat is a major cyber security threat because the insider may have access to resources, networks, equipment, or systems that may cause significant damage to the organization. The insider threat may be intentional or unintentional by the actions they do. An unintentional action is sending sensitive information to the wrong recipient because of a misspelled name or word in the email address. Intentional action is releasing classified information to the public as revenge because of termination. Cooperation should take the time and effort to teach employees about cyber threats. Educating their employees on identifying cyber threats such as phishing emails and links can minimize the number of victims. Some incidents occur by accident because the worker is unaware of the actions they did. If the cooperation had a semi-annual cyber security awareness training course presented by a subject matter expert, it could help an employee understand the importance of a cyber threat and the damage that can be caused.

Software Management & Malware

Maintaining the software updates installed on your computer is as critical as having the software. Breaches can be prevented promptly if the software’s patch is installed (Raths, 2019). Large cooperation has many computers and systems to maintain; however, taking the time to organize a team to manage the patch releases will reduce cyber threats. Upgrading to the newest software rather than outdated software with no patch updates can prevent cyber attacks. Malware is defined as “malicious software” intended to harm a computer, network, or server by infecting it. The different types of malware that can infect the device are viruses, worms, spyware, trojans, adware, fileless malware, or ransomware. Malware has been the most common cyber attack used to expose the vulnerabilities of a system (Rhode, Burnap, & Wedgbury, 2021). Having a computer infected by malware can cost time and money to clean. Early detection of malware attacks helps recover information (Rhode, Burnap, & Wedgbury, 2021).

Phishing & Password Attacking

Phishing is a cyber attack that gathers sensitive information by contacting targets by email, links, or text messages posing as an institution or someone. The attacker lures their victims to take action by sending them a malicious link or an attachment through an email (Bossetta, 2018). A phishing email may send a link acting as a bank representative asking for banking information and a password to access the victim’s account. The information gathered may result in identity theft or financial loss for the victim. Having a user password gives access to the person’s account and identity. Hackers may act as victims to gain information, wealth, or creditability. It is seen on a hacked social media account, and they are asking for money through GoFundMe accounts.

Conclusion

Cyber threats will continue to evolve and penetrate through cyber defense cooperation put in place. Understanding how cyber threats are used and developed can help overcome this challenge. Although there are more cyber threats, planning for any cyber threat will help reduce the possibility of being attacked.

Reference

Bossetta, M. (2018). The Weaponization of Social Media: Spear Phishing and Cyber Attacks on

Democracy. Journal of International Affairs, *71*, 97–106.

E, M., & A, K. (2019). New Authentication Scheme to Secure against the Phishing Attack in the

Mobile Cloud Computing. Security & Communication Networks, 1–11. <https://doi->

org.sandiego.idm.oclc.org/10.1155/2019/5141395

Liu, Y., Peng, W., & Su, J. (2014). A study of IP prefix hijacking in cloud computing

networks. Security & Communication Networks, *7*(11), 2201–2210. <https://doi-org.sandiego.idm.oclc.org/10.1002/sec.738>

Masdari, M., & Jalali, M. (2016). A survey and taxonomy of DoS attacks in cloud

computing. Security & Communication Networks, *9*(16), 3724–3751. <https://doi-org.sandiego.idm.oclc.org/10.1002/sec.1539>

Raths, D. (2019). Patch Work: Patch Management Is a Cornerstone to Information Security in

Today’s Highly Digitized Environment. So, Why Is It Still Such a Vulnerability? Government Technology, *32*(7), 38–42.

Rhode, M., Burnap, P., & Wedgbury, A. (2021). Real-Time Malware Process Detection and

Automated Process Killing. Security and Communication Networks, *2021*(1).

Sun, Y., Wang, B., Wang, C., & Wei, Y. (2021). On Man-in-the-Middle Attack Risks of the

VPN Gate Relay System. Security & Communication Networks, 1–7. <https://doi-org.sandiego.idm.oclc.org/10.1155/2021/9091675>