JOURNAL ENTRY 6

Before studying cybersecurity, I had several misconceptions because I wasn't technologically informed and wasn't aware of what the field fully entails. However, as I progressed through my coursework, I have realized that these preconceived notions were entirely incorrect. Initially, I thought this field was only associated with hacking and aimed solely at stopping the “bad guys” (hackers). I didn't know what their motives were or why they should be stopped. I wasn’t fully aware of online security and its essence; I used to think that the internet was safe. I thought having access to free public Wi-Fi was cool, I just had to connect and surf the internet freely, and no one would know I was connected. I believed that having a password that no one else knew was enough, and I didn't see the need to change it, fearing I might forget it.

I used to think installing security software like an antivirus was enough to keep my laptop safe online, I thought VPNs were just a cool way to trick certain movie websites to gain access. Lastly, because I only came across articles about large company cyberattacks, I used to think they were the only ones targeted because of their large turnovers.

With what I've learned so far my perspective has changed and my misconceptions have been proven wrong:

My initial belief that cybersecurity was solely centered around hacking was wrong. I discovered cybersecurity is more than just thwarting hackers, it involves ensuring information, systems, network or entities are well secured through proactive measures aimed to prevent cyber incidents. These measures include deploying and implementing strategies to strengthen security posture. Moreover, my perception that all hackers were bad was also wrong. I have now learned that there are ethical hackers who help ogranization strengthen

their security by highlighting vulnerabilities. Additionally, I have also learned that this field is interdisciplinary in nature, comprising diverse skills from various disciplines.

Regarding my initial thought on Public Wi-Fi and online safety being harmless. I have now realized that it is insecure, making it easy for hackers to eavesdrop on data transmission, steal sensitive information, or gain access into personal accounts. Individuals who use public wifi are susceptible to phishing attack, identity theft, remote access malware, and ransomware attack. I've also realized that VPN is more than just a tool for tricking a website to view content; it should be used to secure connections over a public network by encrypting data, making eavesdropping difficult.

My initial thought on password security and the need to regularly change password was wrong, as one vulnerability that hackers exploit is weak passwords. They use dictionary or brute-force attacks to crack them and gain access. This has now highlighted the need for frequent updates and implementing multiple layers of protection. My perception that antivirus software was sufficient was wrong. With various sophisticated attack vectors used by hackers, antivirus programs may be unable to detect their behavioral patterns. Implementing security measures at every layer is required for robust protection, such as firewalls and instruction detection systems for filtering packets and detecting malicious activities as well as two-factor authentication for access control.

My initial thought that only large companies were targeted was wrong. I have come to learn that companies of all sizes, if they have known vulnerabilities that can be exploited, will be targeted. Small and Medium-sized companies fall victim to cyberattack because they lack adequate funds allocated to cybersecurity, thereby having weak security defenses. Small companies' data breaches aren't publicsized because they're either not aware they've been hacked or are afraid of losing the client's trust. However, the most targeted sectors are healthcare and financial due to the sensitivity of data they manage.

In summary, I had a big misconception about the field of cyber security, believing that it was all about being a hacker, targeting big corporations, and exploiting rich people. Based on my limited understanding I believed that using public Wi-Fis and having what I think are unguessable passwords was enough security or that using VPNs was just to confuse streaming sites. Getting involved in the field, I am glad I was wrong; it has given me a clearer understanding of the common misconceptions of the field and the other above-stated things. I enjoy the multifaceted view of the field and the ability to learn new things, such as the importance of VPNs, rotating passwords, networking, and security systems. I now appreciate the importance of ethical hacking and enhancing security systems, especially for more critical systems such as finance and health.

References

- *Antivirus alone does not protect your business - here's why*. (2024, March 14). Eye Security. Retrieved June 19, 2024, from https://www.eye.security/blog/antivirus-alone-does-not-protect-your-business-here-is-why
- Burge, S. (2023, October 1). *What is Password Security & Why is it Important?* International Security Journal. Retrieved June 18, 2024, from https://internationalsecurityjournal.com/password-security/
- CBNC. (2015, April Tuesday). *Think only big companies get hacked? Wrong*. NBNC Newsletter. Retrieved June 19, 2024, from Think only big companies get hacked? Wrong
- *The Dangers of Using Public Wi-Fi (and How To Stay Safe)*. (n.d.). Aura. Retrieved June 18, 2024, from https://www.aura.com/learn/dangers-of-public-wi-fi
- *Why is Password Security Important?* (n.d.). FutureLearn. Retrieved June 18, 2024, from https://www.futurelearn.com/info/courses/teaching-cybersecurity/0/steps/57176
- Yacono, L. (2022, November 22). *4 Critical Proactive Cybersecurity Measures You Need in 2023*. Cimcor. Retrieved June 19, 2024, from https://www.cimcor.com/blog/proactive-cybersecurity-measures