Career Paper

08/01/2024

Omari Holloway

When it comes to cyber security and protecting important information systems, there are numerous for this goal to be achieved. When cyber professionals review cyber events, they strive to understand what caused the issue and resolve it so it doesn't happen again through research and analysis.

The principle of determinism is one of the key principles used when protecting people and technology. The way this is done is dependent on the organization and its needs. A new trend on the rise though is employing ethical hackers to test cybersecurity protections. Ethical hacking is defined as an "authorized attempt to gain unauthorized access to a computer system application or data using the strategies and actions of malicious hackers." Unlike malicious hackers, ethical hackers operate within the permission of the system owners to use the findings to improve security for customers. The work completed by ethical hackers is inherently technical. Relying heavily on social science research and principles when conducting these acts, to understand how human factors influence cyberspace (***SecurityScorecard)***. This paper will explore the intersection of social science and ethical hacking, and their importance to society.

One of the main factors common amongst ethical hackers are not just that their technical experts, but also expert social engineers. Utilizing deception and manipulation to get victims to divulge sensitive information, highlighting the importance of education. The reason ethical hackers are so successful is due to their understanding of psychology and social dynamics to uncover vulnerabilities in victims. Drawing upon social engineering techniques such as phishing

and baiting to simulate real world attacks and test an organization's defenses. Another common trait amongst ethical hackers is that their effective at communication. The goal of social engineering attacks isn't to force you but to persuade you or make you comfortable enough to divulge sensitive information. They spend time with their victim utilizing their knowledge of sociology and psychology to make their victims more susceptible to attacks. This information is vital for companies and ethical hackers to understand how to best develop countermeasures to cyberterrorists. The number of social engineering cases is undoubtedly going to increase as the number of internet users increase.

Social media has connected millions of people across the world, but this connection isn't always positive. People establish relationships with strangers on the internet without truly knowing the person their speaking too. Ethical hackers may use these relationships to identify potential targets for social engineering attacks. It's important to consider these factors when developing plans to protect workers from social engineering tactics since every organization is different. One of the benefits of being an employer is being able to hire diverse qualified candidates. With this benefit comes further tailoring of cybersecurity policies to ensure everyone understands it to abide by it and enforce it while being protected. Consider the concept of the human firewall. The implementation of cybersecurity policies is only as effective as the person enforcing them. Ethical hackers are one piece of a global network dedicated to protecting citizens and cyberspace. Moreover, ethical hackers must consider

Ethical hackers are just of one of many vital careers dedicated to reducing cyber victimization. Through not only using their technical skills to protect cyber systems but also through analyzing events through a social science lens. Technology and society will forever be

intermingled requiring for professionals to understand the systems and victims they're trying to protect but also the perpetrators they're trying to catch.

References

- Bowen, B. M., & Zapata, C. J. (2016). A Sociological Approach to Cybersecurity. *Sociology Compass*, *10*(12), 1107-1120.
- Shaw, E., Ruby, C., & Postma, J. (2005). The Insider Threat to Information Systems: The Psychology of the Dangerous Insider. *Security Awareness Bulletin*, 2.
- Hadnagy, C. (2018). *Social Engineering: The Science of Human Hacking*. John Wiley & Sons.

"What Is Ethical Hacking and How Does It Work?" *Synopsys*, www.synopsys.com/glossary/what-is-ethical-hacking.html. Accessed 1 Aug. 2024.

karley, kathleen m., et al. *Social Cyber-Security - Casos*, www.casos.cs.cmu.edu/projects/projects/social_cyber_security/Carley et al Social Cyber Security.pdf. Accessed 1 Aug. 2024.

Shaw, Eric, et al. *The Insider Threat to Information Systems*, homes.cerias.purdue.edu/~mkr/sab.pdf. Accessed 1 Aug. 2024.

"The Human Factor in Cybersecurity." *SecurityScorecard*, 16 Feb. 2024, securityscorecard.com/blog/the-human-factor-in-cybersecurity/#:~:text=Humans%20are%20susceptible%20to%20cognitive,to%20mitigate%20human%20error%20effectively.