Student's Name

Instructor's Name

Course

Date

Secure Coding and Social Engineering

Software vulnerabilities are the leading cause of computer issues in terms of security. Tailor and Azadegan argue that as software development improves, organizations should build secure systems throughout their software development life cycle. In this article, the authors discuss a prototype plan to incorporate security into the computer information systems curriculum at Towson University. This integration includes threading security touchpoints and risk analysis into major courses and two upper-level courses from each major (Tailor and Azadegan 24). Although the author's plan is a work in progress, their article contains essential information that can be used to develop secure coding mantras to identify and mitigate risks.

Such countries as the United Kingdom use industrial control systems (ICS) in their national infrastructure to handle risks. However, they do not understand ICS technical vulnerability. In their article, Green and colleagues use a mean time-to-compromise (MTTC) metric to explore the security risks of ICS. MTTC takes a holistic approach to understanding the potential impact of social engineering in a small European utility company (Green et al. 25). Specifically, the author used MTTC to investigate the impact of a successful social attack on susceptible devices. Green et al.'s findings are critical in understanding the degree of access a social engineering attacker can gain and how MTTC can be improved to assess security controls across technical, social, and organizational viewpoints.

In another article, Nelson and colleagues argue that attackers leverage social engineering to access private social network accounts and steal critical information. Thus, they propose the use of intrusion detection systems to hinder attacks on the social networking sites of government agencies, corporations, and schools (Nelson et al., 1). The authors also highlight how intruders conduct social engineering attacks, including spear-phishing and exploiting Windows functionalities. This article will be critical for secure coding and social engineering projects in illustrating how social engineering attacks are conducted and designing ways to reduce such threats. Concepts of machine learning algorithms are essential for working on certain types of data to enable users to decide on what to share on social media.

Works Cited

Green, Benjamin et al. “The Impact of Social Engineering on Industrial Control System Security.” *Proceedings of the First ACM Workshop on Cyber-Physical Systems-Security and/or Privacy*, 2015, pp. 23-29. DOI:10.1145/2808705.2808717.

Nelson, Jennifer et al. “Social Engineering for Security Attacks.” *Proceedings of the 3rd Multidisciplinary International Social Networks Conference on Social Informatics*, no. 6, 2016, pp. 1-4. DOI:10.1145/2955129.2955158.

Tailor, Blair and Shiva Azadegan. “Threading Secure Coding Principles and Risk Analysis into the Undergraduate Computer Science and Information Systems Curriculum.” *Proceedings of the 3rd Annual Conference on Information Security Curriculum Development*, 2006, pp. 24-29. DOI:10.1145/1231047.1231053.