Ryan G. Cooper

Professor Conlan

CS-405 Module 2 Journal One

May 19th, 2024

**Defense in Depth**

Defense in depth is a critical cybersecurity strategy that employs multiple layers of defense to protect information and systems. The thought is if or when one layer fails, another will be there to provide the necessary security. As said in the Cyber security minute video, there is not just one security protocol that can do it all but having multiple security protocols that defend different areas will make the whole system more secure. With this being said, a balance needs to be found so the defense does not end up too deep. A too-deep defense can lead to diminishing returns as more layers get added on. The complexity of the overall system also increases which can make management and maintenance difficult. Lasty, multiple layers on top of one another can impact the overall performance of the system.

There are several tradeoffs to consider as defense is depth is being implemented. Security over usability becomes a problem because as each layer of security is introduced, more checkpoints and controls are put on the user which can slow down legitimate access and operations. This can lead to frustration among users and can affect productivity. Then there is the higher costs for marginal increases in security. While adding more layers can increase security, each additional layer comes with associated costs, including purchasing, implementation, and maintenance expenses. Organizations must evaluate whether the increased security is worth the additional costs. When it comes to reputation, an organization’s brand and public image is most important. So having a robust security can enhance trust among clients and partners. Organizations known for strong security measures are likely to be trusted more by customers and partners, leading to better business relationships.

Not all organizations and companies are the same, thus not all defense in depth methods will be the same. A smaller business might prioritize cost-effective, simpler solutions, while larger enterprises might afford more complex and robust layers. The scale and scope of operations influence the depth of security needed. Certain industries like healthcare and finance may require specialized defenses due to the nature of the data handled. Places that use legacy systems that were not built with future compatibility, like today’s systems, will need additional protective measures. Each organization must assess its unique situation to determine the most effective implementation of defense in depth. The focus should be to find a balance between security, cost, and operational efficiency.

**References**

YouTube. (2017, January 23). Cyber security minute: How does defense in depth work?. YouTube. <https://www.youtube.com/watch?v=lnIRqw0jutA>

Yendamury, G., & Mohankumar, N. (2021). Defense in Depth approach on AES Cryptographic Decryption core to Enhance Reliability. 2021 IEEE International IOT, Electronics and Mechatronics Conference (IEMTRONICS), IOT, Electronics and Mechatronics Conference (IEMTRONICS), 2021 IEEE International, 1–7. https://doi-org.ezproxy.snhu.edu/10.1109/IEMTRONICS52119.2021.9422567