Bryan Chan

CS405

Prof. Nguyen

22 December 2024

Week Eight Journal

**Adoption of a secure coding standard, and not leaving security to the end**

Josh Ryther in the Medium article, “Don’t Leave Security to the End” (2022), explains this principle in the following quotation: “Security isn’t something to consider at the end but must be an integral part of the software development lifecycle from the beginning. Making design choices with security in mind allow for more secure coding practices and can decrease refactoring.” (Ryther, 2022). By pushing the security of the program towards the end of the SDLC, the program ends up being less secure.

**Evaluation and assessment of risk and cost benefit of mitigation**

Before implementing zero trust, the system administrator must be aware the risk and cost benefit. Beginning with the risk, According to the SentinelOne article, “Mitigation (Risk Management): Key Strategies & Principles” (2024), one of the risks presented by risk mitigation are resource constraints (SentinelOne, 2024). In other words, decisions on how resources will be used, must be made with intentionality. In addition to this, the previously mentioned SentinelOne article (2024) writes that one of the benefits of risk mitigation is increased security (SentinelOne, 2024). This will serve as a great positive to companies, as greater security will prevent security attacks and data breaches from occuring.

**Zero trust**

Toby Kueh in the ThreatPost article, "A Practical Guide to Zero-Trust Security", explains the security policy's impact on an application's security: "[...]this model considers all resources to be external and continuously verifies trust before granting only the required access." (Kueh, 2020). To put it another way, the security policy does not assume the best for each component. Each component must be tested, before it is utilized.

**Implementation and recommendations of security policies**

After discovering the zero trust security policy, and its risks and cost benefits, it is recommended for all companies to implement the security policy. To summarize the major reasons why it should be implemented, consider the fact that by requiring verification for every step in the application, security attacks towards the system are prevented from happening. One way that this could be implemented, is by requiring auditing for every action done by the user. This will allow the system administrator to analyze any suspicious activity that occurs. All of these actions will result in a secure system.

References

Kueh, T. (2020, January 15). *A practical guide to zero-trust security.* Threatpost. https://threatpost.com/practical-guide-zero-trust-security/151912/

Ryther, J. (2022, February 6). *Don’t leave security to the end*. Medium. https://medium.com/@jryther91/dont-leave-security-to-the-end-ca13b107d4

SentinelOne. (2024, September 16). *Mitigation (Risk management): Key strategies & principles.* <https://www.sentinelone.com/cybersecurity-101/cybersecurity/mitigation-risk-management-> strategies/