Joshua Perez

SNHU CS-405-Secure Coding

December 14, 2023

**8-2 Journal: Portfolio Reflection**

As I reflect on this course and compile my portfolio, I'm struck by the critical importance and interconnectivity of various cybersecurity concepts we've explored, particularly in the context of secure coding practices, risk assessment, Zero Trust security models, and the implementation of effective security policies.

**Adoption of a Secure Coding Standard:**

Secure coding is fundamental to software development, ensuring that applications are not only functional but also safe from security vulnerabilities. As emphasized in Adam Murray's "Secure Coding: A Practical Guide," this involves adhering to a set of coding practices that mitigate the risk of security threats. These standards include validating user inputs to prevent injection attacks, using secure data storage and transmission methods, and implementing error handling to avoid leaking sensitive information. The FTC's "Start with Security" guide reinforces this by advocating for the integration of security measures from the early stages of the software development lifecycle, thereby embedding security into the fabric of the application.

**Evaluation and Assessment of Risk and Cost-Benefit of Mitigation:**

This area involves understanding the risks associated with software development and the deployment of IT systems and balancing these risks against the costs and benefits of implementing security measures. Ray Dunham's work on information security policies illustrates the importance of this balance, as over-securing can be as detrimental as under-securing, both in terms of financial costs and user experience. An effective risk assessment strategy considers the likelihood of various security incidents and the potential impact they could have, both financially and in terms of reputational damage. This assessment then informs the decision-making process regarding which security measures to implement, ensuring that resources are allocated efficiently and effectively.

**Zero Trust:**

Zero Trust is a security model that operates on the principle that trust is never assumed, regardless of whether a user or system is inside or outside the network perimeter. The resources from Cisco Nederland, Okta, and Check Point Software Technologies, Ltd., along with Tony Kueh's article, demonstrate that Zero Trust is about continuous verification and validation of every attempt to access resources in a network. This model requires robust identity and access management, ensuring that users are authenticated and authorized appropriately and that their actions are constantly monitored and logged. Zero Trust is particularly relevant in modern distributed systems, where traditional perimeter-based security models are insufficient to address evolving cyber threats.

**Implementation and Recommendations of Security Policies:**

Implementing effective security policies is about creating guidelines and procedures that dictate how an organization's data and IT resources are managed and protected. Jaikumar Vijayan's article on DevSecOps best practices highlights the importance of integrating security into the DevOps process, ensuring that security is a continuous consideration throughout the software development and deployment lifecycle. Effective security policies should be clear, enforceable, and regularly updated to respond to new threats. They should also include guidelines for incident response, ensuring that the organization is prepared to respond effectively to any security breaches that do occur.

**References**

Cairns, C., & Somerfield, D. (n.d.). The Basics of Web Application Security. Martin Fowler. Retrieved from <https://martinfowler.com/articles/web-security-basics.html>

Cisco Nederland. (n.d.). How Zero Trust improves security and the user experience. YouTube. Retrieved from <https://www.youtube.com/watch?v=-Why_ZjJUhg>

Dunham, R. (2020, May 5). Information Security Policies: Why They Are Important To Your Organization. Retrieved from <https://linfordco.com/blog/information-security-policies/>

Federal Trade Commission. (n.d.). Start with Security: A Guide for Business. Retrieved from <https://www.ftc.gov/business-guidance/resources/start-security-guide-business>

Kueh, T. (n.d.). A Practical Guide to Zero-Trust Security. Threatpost. Retrieved from <https://threatpost.com/practical-guide-zero-trust-security/151912/>

Murray, A. (2020, June 13). Secure Coding: A Practical Guide. Mend.io. Retrieved from <https://www.mend.io/blog/secure-coding/>

Mylonas, L. (n.d.). What is AAA security? An introduction to authentication, authorisation and accounting. Codebots. Retrieved from <https://codebots.com/application-security/aaa-security-an-introduction-to-authentication-authorisation-accounting>

Okta. (n.d.). What is Zero Trust Security?. YouTube. Retrieved from <https://www.youtube.com/watch?v=d-Jk3GzjwlM>

Programming Algorithms. (n.d.). XOR Encryption. Retrieved from <https://www.programmingalgorithms.com/algorithm/xor-encryption/cpp/>

Vijayan, J. (n.d.). 6 DevSecOps best practices: Automate early and often. Techbeacon. Retrieved from <https://techbeacon.com/security/6-devsecops-best-practices-automate-early-often>

Check Point Software Technologies, Ltd. (n.d.). What is Zero Trust Security?. YouTube. Retrieved from <https://www.youtube.com/watch?v=1D5mg9an19o>