**Module Eight Journal**

**Reflection**

Joshua Eberharter

Southern New Hampshire University

CS405 Secure Coding

Professor Mike Prasad

10 December 2022

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

Security has to be a mindset adopted from the beginning of the software development lifecycle. When security is left to the end, vulnerability fixes cost more, development times increase, customers become unsatisfied, and the program contains more defects.

To combat this, it’s important to create a security policy all team members are familiar with and fully understand. This policy serves as a guideline for the rest of development to ensure developers are using best practices to create quality, robust code and security vulnerabilities are prevented.

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

The assessment of risk is critical for making informed, data-protecting decisions. Security threats are constantly changing and evolving with technology. Therefore, developers and managers need to constantly be evaluating security policies and performing risk assessments. Tools like automated unit testing penetration testing help teams prepare for potential threats and how to respond in case of a breach.

**Zero trust**

According to Kapil Raina, a writer from Crowd Strike, “Zero Trust is a security framework requiring all users, whether in or outside the organization’s network, to be authenticated, authorized, and continuously validated for security configuration and posture before being granted or keeping access to applications and data” (Raina, 2022). This continuous verification limits the impact of potential insider or external security beaches. This requires organizations to continuously monitor and track user privileges and attributes.

**Implementation and recommendations of security policies**

The security policy contains the core principles and standards of an organization’s software development lifecycle. At a minimum, projects should incorporate some form of defense in depth to obstruct malicious users on as many organizational layers as possible. User activity and major events should be tracked and monitored to help identify potential security vulnerabilities. Authentication and authorization techniques like principle of least privilege and a basic username-password combo should be utilized. Additionally, all staff should be trained in secured practices like identifying phishing emails, suspicious links, and remembering to log out of machines when they are finished with them.

**References**

Raina, K. (2022, November 10). *What is Zero trust security? principles of the zero trust model*. crowdstrike.com. Retrieved December 10, 2022, from https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/