**8-1 Journal: Reflection**

Anthony Baratti

Southern New Hampshire University

CS-405 Secure Coding

Professor R. Kraya

April 27, 2025

**8-1 Journal: Reflection**

The 2016 State of DevOps Report research suggests that teams that integrate security into their daily requirements and early operations can save up to 50 percent less time addressing and fixing security issues (Dora, 2024). Rather than waiting for development and testing to be completed to address security concerns, they should be planned and implemented from design through production, and at every viable step in between. Creating a culture that aligns with security from the start helps developers thoughtfully and purposefully implement security measures that can save time, money, resources, and credibility. It can also help integrate layers of security and provide a more robust defense-in-depth scheme. Consistently addressing and utilizing security automation tools can help build a solid foundation for credibility and trust, which in turn can help deliver more efficient and cost-effective software.

Although software security practices can be expensive, not just financially but also computationally (such as frequent encryption and decryption), it is important to integrate them when necessary. This is where risk assessment enters the design plan. Appropriately evaluating the risks by determining the likelihood of vulnerabilities and the impact (or cost of remediation), as well as developing a prioritized management plan for implementing security protocols to proactively manage potential risks, is crucial to the success of reducing the risk. Proper planning doesn’t just stop at development, though. It is vitally important to continue to monitor and review code through logging and auditing to ensure the efficient and intended operation of the environments. This process is important for maintaining user trust and developer credibility (Cooper, 2023).

Now more than ever, with technology having left the computer desk, and networking now acting globally, it is important to verify all entry points into systems. Cloud computing offers incredible versatility for information technology, putting devices and data at our fingertips “on the go”. With this technological revolution, more security concepts must be adopted in order to provide safe and secure interactions across the planet. Zero-trust policies can be designed and put in place to aid in the mitigation of security breaches and threats. Ensuring that all appropriate users, data, devices, connections, and applications deliver exactly what is promised through proper verification (such as user authentication, network authentication, or application certification) is vital to the success of remotely accessible systems and their internal or external components (such as databases and 3rd party entities). Adapting quickly and creating an environment with full visibility can be key to keeping all of these crucial components safe (Kueh, 2020).

Security policies are not just a recommendation, they are a key principle to a secure system and environment. They define the security protocols of projects through the evaluation of risks. To ignore a security policy is to ignore ethical (and sometimes legal) responsibilities to the company and the end-users. Granted, not all security policies will be built the same, or address the same concerns, but when a security policy is implemented, it should be strictly adhered to and hold accountability to all developers participating in the project. The policies should be comprehensive, including prioritized and threat-assessed risks, their solutions, and proof of completion (such as testing or static code review) (Dunham, 2020). This “checklist” of recommendations and rules is a standard that keeps a system in operation, and even *with* it, security concerns will continue to arise. There is no exception to actively addressing security concerns in an accessible program.

**References:**

Cooper, C., (2023, November 27). What is a software security assessment? *SoftwareDevelopmentUK.* https://www.softwaredevelopment.co.uk/blog/what-is-a-software-security-assessment/

Dora, (2024). *Shifting left on security.* Dora.dev. <https://dora.dev/devops-capabilities/process/shifting-left-on-security/>

Dunham, R., (2020, May 5). Information security policies: Why they are important to your organization. *Lindford & Co*. https://linfordco.com/blog/information-security-policies/

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