8-2 Journal: Portfolio Reflection

Michael P Clisbee

CS 405: Secure Coding

Southern New Hampshire University

* Adoption of a secure coding standard, and not leaving security to the end
* Evaluation and assessment of risk and cost benefit of mitigation
* Zero trust
* Implementation and recommendations of security policies

Adopting a secure coding standard ensures that all projects will go by the same standards for development and implementation, no matter who is assigned a specific branch of code. When it is pushed to the main project branch you can be assured that have adequate security protocols in place to avoid inside and outside threats. By “not leaving security to the end”, you are not putting off security measures development until the end of the software lifecycle but are instead planning ahead by anticipating what possible vulnerabilities might occur before they actually do. By waiting, the result could mean unreliable code, under tested or non-compatible with other branches of code submitted by other developers. By following this guideline, you are using a proactive approach to coding as opposed to a reactive one.

Evaluating and assessing risk is essential when categorizing different threat levels in order to be proactive and develop security policies and other defenses. Weighing the cost to mitigate these concerns as opposed to the cost of leaving possible vulnerabilities in place is crucial when evaluating if leaving an issue unresolved will cause greater harm than good (NIST, 2007). There is no such thing as 100% secure code but adopting secure coding practices removes common vulnerabilities. As well, priming your security policy at the start will reduce long term hazards and costs. Always remain vigilant in the assumption that all systems have implied threats and flaws to be identified. Continuous personnel training is essential in staying ahead of the issues that are ever evolving.

Zero Trust policies are used by most companies in the business world today, who understand the importance of maintaining a hypervigilance regarding insider and outsider threats. These companies ensure that enforcing minimal user access with multiple redundant authentication checkpoints will ensure the safety and security or their data. Zero Trust policies incorporate Triple-A policies of Authentication, Authorization, and Accounting. As well, it uses an approach known as Defense in Depth (DiD), which is a cybersecurity concept that involves constructing layers upon integrated layers of defensive mechanisms to protect sensitive data and information. All of these approach vectors will ensure a more secure network.

All security policies can contain gaps. The key is to identify all possible avenues of attack approach and use that as you baseline for security creation. Test defenses before the breaches occur and develop a plan to respond when security fails. Based on the principles and standards included in an efficient security policy, it can be determined all possible avenues of attack approach have been covered to create and maintain a secure and proficient program. A zero-trust policy will be implemented when it comes to internal and external data access throughout the company network, creating a situational awareness necessary to maintain security and privacy and to keep all sensitive information safe and secure.

References

NIST (Feb, 2007). *A Guide to …Developing a Cost-Effective Risk Mitigation Plan…*, Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/IR/nistir7390.pdf

Forcepoint (2022). *Defense-in-Depth Defined.* Retrieved from https://www.forcepoint.com/cyber-edu/defense-depth