Portfolio Reflection

Nicolas W. DeFrancisco

Southern New Hampshire University

Adoption of a secure coding standard encourages programmers to conform to a set of rules and guidelines to ensure that security is engrained as soon as code is being designed and written. It unifies the source code under a common standard. The use of secure coding standards defines a set of requirements and rules against which the source code can be evaluated against. Enforcing standards also eliminates the introduction of known vulnerabilities.

A secure coding standard guides design and development as well as forms a unified basis for test cases. Secure coding standards are the guidelines that should be the overarching basis to which should be continuously referenced throughout the software development lifecycle. By implication, this means that security should not be left for implementation in the end. Security should be embedded throughout the development pipeline starting with assessment and planning.

Risk is the potential for exposure to danger. It is the sum of an enterprise’s assets, active threats, resident vulnerabilities, and potential organizational impact. To effectively evaluate risks, risks need to be tied back to the business requirements, essentially assessing these risks as business risks associated with the technology gateway that exposes these risks. Accepting or mitigating a business risk is essentially a cost-benefit exercise. Any vulnerability in a system that has the potential to be exploited is considered a risk to some component of the business. The likelihood that a vulnerability is exploited, the potential impact should the known vulnerability be exploited, and the cost of remediation determine how coding standards and rules are prioritized. This gives us a cost-benefit decision-making criteria for the business. Stakeholders should also be considered when evaluating and assessing risks. Identifying stakeholders and the proximity to the business can be accomplished with a stakeholder analysis to understand the true cost of mitigation or remediation of business risks and security vulnerabilities.

Zero trust is a security concept that focuses on treating all resources and users as external. When attempting to access a system, users must verify their credentials at each privileged access level using modern, secure authentication methods. Zero trust means to always verify credentials. This means that a strict authentication and authorization policy needs to be in place to ensure that the system always verifies a user’s credentials.

Security policies are implemented based on modern security frameworks and best practices. The security policy was developed based on defense-in-depth approach where multiple security strategies are implemented to maximize security coverage throughout all layers of a system. A defense-in-depth approach guides the security policy as an overarching theme including the core principles and secure coding standards. Then, security is built into the software development lifecycle by adopting a DevSecOps approach to ensure that security is addressed throughout the development lifecycle in both pre-production and production/deployment phases.