8-2 Journal: Portfolio Reflection

Richard Backscheider

CS-405-H7070 Secure Coding 23EW2

12/17/2023

Southern New Hampshire University

Adopting a secure coding standard strengthens software systems against potential threats. Secure coding standards involve establishing guidelines, best practices, and coding conventions prioritizing security considerations across the development lifecycle. By integrating security into the coding standard, developers are encouraged to follow secure coding practices from the outset, reducing the likelihood of vulnerabilities and enhancing the codebase’s resilience to attacks. Noteworthy benefits include the early detection of vulnerabilities during development, prompt addressing of security issues, and the maintenance of consistent security practices throughout the codebase minimizing the risk of human error.

Before implementing security measures, conducting a comprehensive evaluation and risk assessment, accompanied by a cost-benefit analysis of mitigation strategies, is crucial. This strategic approach ensures optimal resource allocation, prioritizing mitigating the most critical and likely threats. It empowers decision-makers to make informed choices about resource investments, effectively balancing security needs with the overall cost of mitigation.

The Zero Trust security model, built on the assumption that no entity can be inherently trusted, establishes stringent identification verification for all attempting access to resources. This paradigm minimizes potential security breaches by restricting access and permissions to the minimum necessary for each user or system. Associated benefits include a significantly reduced attack surface, making it more challenging for attackers to exploit vulnerabilities and improved detection and response capabilities due to the model’s emphasis on scrutinizing unusual behavior.

The implementation and regular update of security policies provide a structured framework for defining, implementing, and enforcing security measures across an organization. Security policies cultivate a security-conscious culture within an organization by covering diverse areas such as access controls, data protection, and incident response. Benefits encompass the consistent application of security measures, reducing the risk of oversights, and ensuring compliance with industry regulations and standards, thus averting legal and financial repercussions.