8-2 Journal: Portfolio Reflection

Steve Edmund

CS-405

Southern New Hampshire University

We often think that including security throughout the entire software development lifecycle is impossible and instead leave it until the end. However, implementing security concepts and practices into everyday operations decreases security-related risks. It is essential to be proactive and adopt secure coding standards from the outset. Throughout coding principles and standards, security should be reviewed frequently prior to coding. As a result of implementing the preventative component of Defense in Depth from the outset, the associated security risk is drastically minimized.

Threats to security can originate from just about any area, whether internal or external. Any decision-making process must be driven by the risk involved with daily decisions. Constantly, we are reminded that the risks of today will not be the threats of tomorrow, and that ignoring any potential threat can have grave implications. The expense of resolving the issues is negligible in comparison to the cost of reducing the related risks. Implementing extremely simple coding strategies, testing early and frequently, and doing static code analysis after each code modification are required. Additionally, we have access to automated unit testing and penetration testing that must be performed consistently.

Traditional authentication methods are failing, and we must therefore assume zero trust at all times because technology is advancing at a rapid rate. Every person, device, network, and data access and application must be continuously validated. In addition to conventional user names and passwords, we have integrated biometrics and multifactor authentication. Using Single-Sign-On access verifications, applications are beginning to be upgraded.

Security policies provide a framework for ensuring that code and data stay secure. Creating, maintaining, reviewing, and adhering to security rules are important for all businesses. Security policies must incorporate fundamental ideas, coding standards, and best practices into every development project. This will enable consistent safety implementation when security policies are adhered to.

Since technology has begun to evolve rapidly, the FTC has learned a number of lessons. This has made it possible for proposals to address common weaknesses that have historically affected numerous businesses, a valuable lesson. Controlling user access to data, user authentication, and storing and delivering data securely are a few of these lessons. Other recommended practices ensure that software is always up-to-date and that users receive fixes promptly. Such requirements as passwords are mandatory.