CS-405 Secure Coding 2024 C-3

Module Eight – Journal

Instructor: Joseph Conlan

Gregory Isajewicz

**Adoption of a secure coding standard, and not leaving security to the end.**

The adoption of a secure coding standard and a secure coding policy within an organization ensures that all developers within that organization have a clear understanding and well-defined measure of expectations to follow in the interest of maintaining security. A secure coding standard serves to enhance security through consistency and best practices throughout the coding process. This plays into the importance of not leaving security to the end. This practice simply means that the incorporation of security in a system or application should be included at every step in the software development lifecycle. By doing this, developers can proactively identify and mitigate potential security concerns early and before they become major threats or vulnerabilities. Through this method, security is built into the software by design, rather than through a series of patches pushed as an afterthought.

**Evaluation and assessment of risk and cost benefit of mitigation.**

Incorporating security throughout development is also the more long-term cost-effective option. The financial ramifications of a security breach after release can be substantial; consider not only the cost of patching the breach, but the loss of revenue and even lawsuits that may stem from compromised data. According to Ani Petrosyan at Statista (2024), the average cost of a data breach in the United States in 2023 was 9.48 million dollars. This is no small expense, nor one to be taken lightly. While the mitigation of risk through robust security policies, threat analysis, and carefully crafter secure coding standards can incur a larger up-front cost in the development of software, it is almost certainly the better financial investment for the sake of mitigating the risk of a data breach.

**Zero Trust**

Zero-trust security seems to me to be well suited to a defense in depth strategy, as well as a security policy which incorporates default deny and the principle of least privilege.  In a zero-trust policy, the focus is not simply on building a wall around data with metaphorical guards looking outward - the would-be guards are instead mingling around the data as well, remaining ever suspicious of anyone inside the wall, even if they have been authorized to enter the wall. Zero Trust also requires continuous authentication and monitoring of devices accessing the system. In the modern day, with the growing popularity of remote work, many employees are using their own devices and their own networks to interact with work outside of the trusted network - adding a new security complication since the firewalls, policies, and controls placed on a companies’ trusted network do not apply to outside untrusted networks. While zero-trust may somewhat complicate these types of outside access on the user end, it also makes them more secure (CertBros, 2023).

**Implementation and recommendations of security policies.**

In order to effectively implement and maintain security policies, an organization must conduct a thorough threat analysis, identify likely threats, a security baseline, and vulnerabilities that are likely to arise. Regular tests and challenges of the security policy will help to ensure that the policy is effective and is being adequately implemented and upheld by staff. Regular monitoring and early detection should also be in place to aid in assuring compliance with the security policy. A security policy can also incorporate any applicable regulatory requirements which also helps to protect the organization legally. The security policy should be a somewhat living document, growing, evolving, and expanding as the need arises. The threat landscape in technology is ever evolving and our security policies must evolve with it.

**Resources**

CertBros. (2023, October 17). Zero Trust Explained | Real World Example [Video]. YouTube.

<https://www.youtube.com/watch?v=Y3DjoTiOiOU>

Petrosyan, A. (2024) *Average cost per data breach in the United States 2006-2023.* Statista.

<https://www.statista.com/statistics/273575/us-average-cost-incurred-by-a-data-breach/>