Rajiv Dialani

CS 405

August 21, 2024

**Journal: Portfolio Reflection**

Adopting a secure coding standard from the beginning of a project is essential for mitigating risks and reducing vulnerabilities. One of the main principles is to ensure that security is incorporated throughout the development process, rather than as an afterthought. For example, practices like input validation and buffer overflow prevention need to be implemented early to avoid common vulnerabilities that attackers can exploit. The main benefits of implementing secure coding standards: “reduce vulnerabilities by avoid common code defects and following best practices,” “increase resilience against attacks by ‘building security in’ throughout the SDLC,” and “promote a culture of security among developers through awareness and training” (“The Importance of Secure Coding Standards”, n.d.). By integrating security into the Software Development Life Cycle (SDLC) from the design phase onward, organizations can reduce vulnerabilities while maintaining quality and performance.

In cybersecurity, not all risks are the same. Evaluating risks means understanding potential threats, assessing their impact, and judging how likely they are to happen. The goal is to prioritize risks and apply solutions that reduce the most harm for the least cost. This approach includes doing a risk assessment to rank threats by severity and then a cost-benefit analysis to decide which solutions are worth implementing. For example, an organization might see data breaches as a high-risk scenario. While the cost of implementing strong encryption and access controls may be high, the financial and reputational damage from a breach would be much worse. So, the investment in these protections is worth it.

The Zero Trust model is a security approach that requires strict verification for everyone and everything trying to access resources on a network, whether they are inside or outside the network. The main idea behind Zero Trust is "never trust, always verify." Unlike traditional security models that trust users inside the network, Zero Trust assumes threats can come from anywhere and treats internal systems as vulnerable as external ones. Zero Trust relies on continuous authentication, least privilege access, and micro-segmentation. Every access request is treated as if it comes from a potentially compromised network and requires strict validation. Technologies like multi-factor authentication (MFA), identity and access management (IAM), and endpoint detection and response (EDR) are often used to support a Zero Trust setup.

Implementing security policies is key to setting a standard for expected behavior and controls within an organization. These policies outline the guidelines, rules, and practices needed to protect information systems and data. They cover various areas like acceptable use, access control, automation, and data protection. The policies should also be reviewed and updated regularly to adapt to evolving threats and technological changes. Effective security policies should align with industry standards like ISO/IEC 27001 and NIST CSF, involve stakeholders from across the organization, and ensure continuous monitoring and enforcement through audits and automated systems. Additionally, these policies should include incident response procedures to address breaches quickly and minimize damage.

**References:**

Check Point Software. (2019, November 21). *What is Zero Trust Security?*. YouTube. <https://www.youtube.com/watch?v=1D5mg9an19o>

Dunham, R. (2020, May 5). *The importance of a company information security policy*. Linford & Company LLP. https://linfordco.com/blog/information-security-policies/

*The Importance of Secure Coding Standards*. Sec1. (n.d.). https://sec1.io/blog/the-importance-of-secure-coding-standards/#:~:text=The%20main%20benefits%20of%20implementing,developers%20through%20awareness%20and%20training

Kueh, T. (2020, January 15). *A practical guide to zero-trust security*. Threatpost English Global threatpostcom. <https://threatpost.com/practical-guide-zero-trust-security/151912/>