8-2 Journal: Portfolio Reflection

Steven Wade

Southern New Hampshire University

8-2 Journal: Portfolio Reflection

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

Adopting a secure coding standard helps a company “towards minimizing the vulnerabilities in their code” (Morrow, 2021). This is important to protect the company and its users. A secure coding standard outlines best practices to take to avoid common secure concerns. These standards put security in the forefront of developers minds so that they are being proactive when it comes to security and not leaving security to the end. Standards will point out security points such as default deny which could impact decisions during the design phase of the DevSecOps.

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

Each risk must be weighed against the potential cost of mitigation. Costs can be financial or reputational. A vulnerability that becomes exploited can severely damage a company’s reputation and public trust. Some risks would require extra time and considerations to fix which would increase operational costs. New risks are being discovered all the time so constant evaluation of software and development practices can improve security of an application as well as improving the reputation of the company.

**Zero trust**

Zero trust isn’t about placing blame or not having faith, it’s an improvement of the phrase “trust but verify” to “never trust/, always verify” (Kueh, 2020). By doing this, every person (employees, customers, users, manager, administrators) are on a level playing field and no one is treated with more or less trust than the other. The practice of having zero trust is a defensive approach to programming that helps developers implement security practices from the start and only allow specific actions and permissions based on user role. The five pillars of the zero-trust model build up layers of security which support the Defense in Depth principle.

**Implementation and recommendations of security policies**

Each company should adopt and implement security policies. At my company, we have strict security policies on admin privileges on computers, password strength for work computers, the use of a password manager and requiring unique passwords for every account, two-factor authentication enabled on all apps that support it, and so forth. These practices give us a starting point as a company. As developers, we are required to follow certain practices too with rules and recommendations unique to each environment and language used within applications. Security policies should be broad but honed so that they can be applied to multiple situations. OWASP, Microsoft, and SEI CERT are some good examples of security policy starting points if looking for inspiration (Morrow, 2021). Examining existing security policies from well-known and trusted sources can help to establish a company’s policy.

References

Kueh, T. (2020, January 15). A practical guide to zero-trust security. Retrieved April 21, 2021, from https://threatpost.com/practical-guide-zero-trust-security/151912/

Morrow, S. (2021, January 21). What is secure coding and why is it important? Retrieved April 22, 2021, from https://vpnoverview.com/internet-safety/business/what-is-secure-coding/