Vincent Garza

Portfolio Reflection

Southern New Hampshire University

April 18, 2023

The adoption of secure coding standards is important because it removes software vulnerabilities that are commonly exploited and prevents cyberattacks (Morrow, 2023b). Plus, adopting these standards will save money in the long run because it cost less to prevent a cyberattack than it does to correct the problem after an attack has occurred. It is also a good idea to not leave security until the end because and coding defect introduced early in the development process could lead to a glitch or serious security breach due to increasing frequency and sophistication of cyberattacks (Bellairs, 2019).

A security risk assessment identifies, assesses, and implements key security controls in applications, and prevents applications security defects and vulnerabilities (Synopsys, n.dl). Cost-benefit analysis of mitigation is a useful way to assess coding projects because it reduces complexity to a single price figure (Shackleton, 2023). This approach can make it difficult to sell the value of a robust security system. But one thing to keep in mind in mind though is that cost of preventative measures is very small compared to the cost of data breaches.

Based on my understanding of zero trust policy, it basically means to implement security measures as if you don’t trust other people within the network to handle sensitive information. One way this zero trust policy is implemented to create a system where users are verified every time they request access, even if they were authenticated earlier (Microsoft, n.d.).

When implementing security policies, one of things that must be done is to find a balance between business requirements and security needs (Brecht, 2021b). An overly restrictive policy could do more harm than good and prevent IT workers from being fully productive. When recommending security policies, it is a good idea to be able to explain the security policy in lay terms because a manager or administrator may not be a developer. Plus, if you are able to explain it, then you understand it.

Works Cited

Bellairs, R. (2019). What Is Secure Coding? *Perforce Software*. <https://www.perforce.com/blog/sca/what-secure-coding>

Brecht, D. (2021, November 24). *Best practices for implementing an IT/cybersecurity policy | Infosec Resources*. Infosec Resources. Retrieved April 19, 2023, from <https://resources.infosecinstitute.com/topic/best-practices-implementing-itcybersecurity-policy/>

Microsoft. (n.d.). *Zero Trust Model - Modern Security Architecture | Microsoft Security*. Retrieved April 19, 2023, from <https://www.microsoft.com/en-us/security/business/zero-trust#:~:text=Zero%20Trust%20is%20a%20high,if%20they%20were%20authenticated%20earlier>.

Morrow, S. (2023b). What is Secure Coding and Why is It Important? *VPNOverview.com*. <https://vpnoverview.com/internet-safety/business/what-is-secure-coding/>

Shackleton, T. (2023). A Cost-Benefit Analysis Approach to Cyber Security. *Six Degrees*. <https://www.6dg.co.uk/blog/cost-benefit-approach-to-cyber-security/>

Synopsys. (n.d.). *What is Security Risk Assessment and How Does It Work? | Synopsys*. Retrieved April 19, 2023, from <https://www.synopsys.com/glossary/what-is-security-risk-assessment.html>