Nate Bennett

Olga Mill

Secure Coding

Southern New Hampshire University

28 April 2024

8-2 Journal: Portfolio Reflection

Adopting secure coding standards like “[Do not read uninitialized memory](https://wiki.sei.cmu.edu/confluence/display/cplusplus/EXP53-CPP.+Do+not+read+uninitialized+memory)” (SEI CERT C++ Coding Standard - SEI CERT C++ Coding Standard - Confluence, n.d.) can be important for reducing vulnerabilities from early stages of the software development lifecycle. Not leaving security to the end is a practice where developers consider security at many stages of development. By embedding security into many stages of the development process, organizations potentially prevent some security incidents before they occur, by resolving vulnerabilities early, and strengthening security.

Risk assessment could be an important component of cybersecurity, involving the identification, evaluation, and prioritization of risks followed by strategic efforts to minimize, monitor, and control the risk of potential incidents. The cost benefit of mitigation could involve assessing the economic effectiveness of implementing security measures against potential incidents. This could help organizations decide how much to invest in security, and which areas of a network to prioritize.

Implementing the zero trust policy could involve not trusting users by default, regardless if they are within the organization or not. This policy could involve regular authentication as users navigate throughout an application, and implementing the principle of least privilege, which could involve granting staff members the least amount of permissions required for their job. Also, having strong access controls, potentially like multifactor authentication, and adding sections to an application to potentially help with containment in the event of an incident, could also align with implementing a zero trust policy.

Security policies can be important as they can define how an organization identifies, reacts to, and mitigates potential cybersecurity risks. Effective security policies could be recommended based on the potential risks that an organization could be facing based on the motives of potential threat actors. They can cover aspects ranging from employee access controls to incident response plans. Also, regular security training could potentially help staff members with implementing security policies.

Works Cited

*SEI CERT C++ Coding Standard - SEI CERT C++ Coding Standard -*

*Confluence*. (n.d.). Wiki.sei.cmu.edu.

https://wiki.sei.cmu.edu/confluence/pages/viewpage.action?pageId=88046682