Cody Faircloth

Olga Mill

CS 405

11 December 2023

8-2 Journal: Portfolio Reflection

It is important for development teams to adopt secure coding standards before a project is initiated. This will allow consistency within the team as the development process occurs. This will also promote early and frequent consideration of security. This ties into the principle of not leaving security to the end. If security is put off until the end of the development cycle, security issues will be overlooked. This can tarnish the reputation of your organization by releasing an unsecure product to your customers. Patches can be used to fix the issues but exposing customers to security risks that could have been prevented in development can leave an ugly stain on the organization's reputation.

The cost of mitigation prior to release comes in the form of time costs, monetary costs, additional expertise on the team, and additional complexity which may require training for users. However, this cost is insignificant compared to the benefits that come with early mitigation. You create a quality product with maximum security when mitigation occurs prior to release. You prevent losses in revenue and reputation which accompany a security breach. Additionally, you get the peace of mind that comes with knowing you considered security in all phases of development.

In complex systems and software, no one should be trusted automatically. It is important to limit the privileges given to trusted users to not allow nefarious use. Additionally, it is important to thoroughly authenticate users to ensure unauthorized use does not occur. Similarly, to letting people into your home, you should vet individuals you allow to use your system or software.

Finally, it is important as a development team to critically analyze your security risks and create action plans to address these risks. You should always assume a breach will occur and that users will misuse our system. You should plan for contingencies to mitigate the effects of misuse or attack. After understanding this, security policies should be drafted and presented to all members of the team to create consistency standards. Policies such as Triple-A, Defense in Depth, and Encryption at all phases should be implemented for maximum coverage.