Brandon Lingenfelter

CS 405

6/25/2022

**Portfolio Reflection**

Adopting a secure coding standard can be beneficial for not only the project you are working on but can be a benefit for your career as a whole. Utilizing a standard of secure coding in your work will help you create more secure and resilient code. By using a standard that supports secure coding through out the development life cycle you can ensure that you are not leaving security for the end. Avoiding treating security as an afterthought and considering security throughout the entire development life cycle can save time and budget for the project. Planning the project with security in mind and following through with security as a consideration as you build the project prevents delays that leaving security considerations till the end could cause.

For the various types of projects we create we need to evaluate where the attack vectors could lie and assess how to best mitigate the risk the attack vectors pose. Every project has a chance to prevent new risk that we must take an assessment of and decide how to best mitigate those risks. Mitigating risk can have a cost benefit that could save budget on the project or help the bottom line once deployed. If we do not mitigate the risk on average we could loose four times what mitigation could cost.

Using a zero trust system can protect an organization from external as well as internal threats. By building systems that ask for authorization at every stage we can protect our users and the organization from unauthorized access. Using zero trust we will as user to provide proof that they are who they claim to be as well as to authorize their devices. This concept will provide a layer of protection to our security protocol for us and our users.

Implementing a security policy is not a copy and paste job. Every project and organization will present different attack vectors we must address to keep the project, organization and user safe from attack. We must first address where and how a project or organization could be attacked. From these assessments we can begin to develop a recommendation on what security policies should look like for the organization and project. After proofing the recommendations a security policy can be developed and provided for implementation.

Citations:

National Institute of Building Sciences. (n.d.). Retrieved June 25, 2022, from https://www.nibs.org/projects/pdx-report