Dominic Drury

06/24/2024

CS-405

8-2 Journal: Portfolio Reflection

I think that adopting a secure coding standard is vital for any organization to maintain a well-protected system, regardless of the size of that system. Having a standard gives everyone a guide that can be followed that does not let the chaos of making a new program make developers lose sight of secure coding best practices. It also gives new developers a key to what the company wants from their security and gives old developers reminders of things they may have become lackadaisical toward. In line with any good coding standard is the mentality that security should be implimented at every stage of development and not saved until the end. This allows for things to be tested throughout the entire life cycle of the program, which means that things are less likely to be forgotten about, and it means that if something needs to be changed it can be altered as early in development as possible.

While there is always a cost/benefit to anything, and mitigation of cyber threats is no different, I think that it will always be better to be safe than sorry. Still evaluating and assessing the risks is still an important part of security. The risk an app has that just keeps track of a user’s self-inputted budget data on a local device is far different than an app that keeps track of a user’s budget on a cloud service or that allows multiple users to use the same system. Even though this is more or less the same data, how it is used and stored greatly changes the security needs of the system.

Zero Trust is the idea that instead of using the traditional mentality of a perimeter defense, that trusted any device or user that made its way through the perimeter and into the internals, instead no device or user was trusted, and all were verified. This is done through things like multi factor authentication and uses a reverse proxy that limits a user’s movement within a system. While this methodology does put some inconvenience on the user, when done right they should be more or less ignorant of the scope of the change and the system will be far more secure.

Implementing security policies can be a lot of work and can cost time and money that some might feel would be better spent elsewhere, but that mentality is not a safe one. The cost of repairing the damage of an attack can far outweigh the cost of implementation, and the damage to the company's reputation might be broken beyond repair. That being said, not every single security measure needs to be implemented in order to have a safe and secure system. Recommendations should fix vulnerabilities that would actually exist for the system, and there is no blanket solution that will fix every problem for every program. Each are unique and come with their own unique requirements.