Brandon Lombard

8-2 Journal: Portfolio Reflection  
CS-405

4/24/2022

The adoption of secure coding standards is highly important to the security of an organization. These coding standards provide a template to follow to ensure there is an adequate level of security against hackers and other malicious attempts. It is especially important to implement these security measures early on in the development process. This allows for the development team to properly prepare for an attack before it is too late. Important coding standards include validating user input, default deny, practice defense in depth, and much more. Validating user input entails validating data passed into the program, which ensures this data is not corrupt. Default deny, on the other hand, automatically denies all permissions to a set of data except those who have direct access. Finally, practicing defense in depth means creating a large layer of protective measures which therefore protects important data.

Evaluating the possible risks is defining the level of risk for certain security risks when compared to others. Then, risk assessment allows developers to identify hazards and evaluate any risks within the organization, which measures will then be incorporated to protect the systems. Then, mitigation refers to attempting to reduce the impact of corrupt data or other hacking events. This limits the impact of threats and helps protect the organization’s data and money. Then, zero trust is a security concept which focuses on the company not automatically trusting anything inside or outside of the company’s systems. This means that there will be a constant verification process to protect the organization from hacking and malicious code. This is highly important and should always be used in secure coding practices.

To implement these security policies, the security policy and plan should be followed. In this process, many things have to be considered throughout the implementation process. This includes identifying all possible risks, learning from mistakes, confirming the policy to legal requirements, having a high level of security, constantly improving the systems, etc. In this process, there are also many recommendations that should be considered. This includes using antivirus software, having strong passwords, using secure internet connections, and backing up company data.