Abby Ramatowski

Secure Coding

04/18/2022

Portfolio Reflection

Cyber attacks can cause great detriment to individuals and organizations. All software can be the target of a cyber attack and companies that create or utilize software should make attempts to prevent cyber attacks. There are many techniques for securing code and taking steps towards preventing cyber attacks. The first step when creating secure code, should be to adopt a secure coding standard. The secure coding standard should include a set of rules that will be followed when coding and programming. It creates a concrete and transparent guide to follow. It should be maintained regularly to continue to prevent threats that may occur in the future.

The secure coding standard may include an evaluation and assessment of the risks and cost benefits of mitigation. Each security risk has potential cost risks and following the standards has cost benefits. The following website includes various coding standards and can be used as a reference when developing a secure coding standard and for determining potential remediation costs: <https://wiki.sei.cmu.edu/confluence/>.

Zero trust involves requiring all users go through authorization and authentication steps before gaining any access to the system. Implementing zero trust improves security by reducing the risk of data breeches. Zero trust provides very strong authorization and authentication practices and provides additional layers of security.

There are many steps involved to implement a security policy. The first step is to identify risks. This should be done by studying the program and determining what a hacker could gain by attacking the program. Studying other systems that have been hacked and what was lost during that attack can help to identify risks. The potential loss should be identified for each risk to determine which is a higher priority. Standards or rules should be determined that will help to prevent those risks. Using current standards such as triple-A framework, defense in depth, user validation, and many others should be implemented into the secure coding standard. The secure coding standard should also be maintained and adjusted regularly as needed to continue to prevent future attacks.