Jorge Argueta

SNHU

CS 405: 8-2 Journal: Portfolio Reflection

August 19, 2023

**Adoption of a secure coding standard, and not leaving security to the end**

We ought to create a platform- and language-specific secure coding standard. All external data sources, including user-controlled files, network interfaces, and command-line arguments, must have their input verified. It ought to prevent access by design. Instead of by exclusion, software should be able to recognize circumstances in which access is granted. To enforce and put security policies into effect, we must design software. When compiling your code, use the compiler's strongest warning level. By changing the code, we can get rid of the warning. Use multilayer defenses and a variety of tactics. The subsequent layer of security needs to be able to stop a vulnerability if the first one is unable to. Verify that error handling and logging are active. Two of the most effective methods for reducing their effects are error handling and logging. Error handling makes an effort to find programming problems before they have a catastrophic failure. Errors are recorded so that developers can identify and fix their root causes. Threat modeling consists of the four processes of document, find, address, and validate. To write safely, you must inspect your software for weak spots that are more vulnerable to attack. Threat modeling is a multi-step approach that ought to be incorporated into the entire software lifecycle, starting with development and ending with production.

**Evaluation and assessment of risk and cost benefit of mitigation**

When determining the seriousness of a risk in relation to other hazards, you are performing a risk evaluation. The quantitative component of risk assessment is this. The systematic process of detecting risks and assessing any associated dangers within a business, followed by the implementation of practical control measures to eliminate or reduce them, is known as risk assessment.

Mitigation is the process of attempting to mitigate the effects of disasters in order to lessen the loss of life and property. According to recent research by the Multihazard Mitigation Council, every dollar invested on mitigation results in an average $4 savings.

**Zero trust**

The idea behind the security concept known as "Zero Trust" is that an organization shouldn't automatically trust anything within or outside of its perimeters and should instead thoroughly check every connection attempt before granting access.

**Implementation and recommendations of security policies**

* Recognize your hazards.
* Get advice from others
* Verify that the policy complies with all applicable laws.
* Risk level equals level of security
* Involve personnel in developing policies
* Educate your staff
* Have it put in writing.
* Establish explicit punishments and uphold them
* Refresh the workforce
* Install the necessary tools.