Portfolio Reflection

Daniel DeGouveia

Southern New Hampshire University

CS-405

**Portfolio Reflection**

When reviewing everything that I have learned in this course I feel that I have a more in depth understanding of the importance of adopting a secure coding standard and not leaving security to the end. While it can be easy to write your code and plan on adding security at the end, this is not best practice and can result in higher costs and more bugs or vulnerabilities that are found in the system. By successfully adopting a secure coding standard and thinking about security during the development stage the code can be written to be sure to reduce chances of malicious attacks. It is also worth noting that a good reason to always be thinking about how to make your code secure is that attackers are always thinking of ways to find and exploit vulnerabilities in the system.

Reflecting on the evaluation and assessment of risk and cost benefit of mitigation it is clear that it is by far more cost effective to attempt to prevent an attack than it is to repair the damage. Risk assessment should be a systematic process where any weak or hazardous portions of the system can be identified. These risks should then be evaluated so the team can implement control measures in order to attempt to reduce or remove these risks. There are many ways that risks can be mitigated, but ultimately the best tactic is to always be thinking about security while building and maintaining your systems.

The concept of zero trust, which is a security concept that supports the belief that the company should not automatically trust anything. This includes items that are located inside and outside of its perimeters. When using zero trust everything and anything must be verified that is trying to connect prior to granting access to the system. While there are people who disagree with this approach I feel that it is a smart idea. When dealing with security you can never be too careful, and while it might create an extra step prior to being able to access something, this can prevent huge attacks and save a company a lot of money.

One important thing that should always be done is having an implementation of some type of security policy. I think that the first step would be to identify your risks and look at the type of data that users will need to access. It is a good idea to always deny access by default, while this is not as strict as zero trust, this can still be a very useful way to prevent a malicious attack. It is also important to regularly update security certificates and ensure there is working antivirus software and all software is up to date on patches. Another recommendation would be to require strong passwords and even two factor authentication on software that supports this to help mitigate risks.

While security might not always be the first thought when building a system or software, it should be. This course has helped me understand what secure coding is, and the importance of thinking about security first rather than leaving it for the end. There are threats and vulnerabilities everywhere and if you are a developer who keeps security at the forefront of your mind you can save yourself and your company a lot of trouble in the future.