Portfolio Reflection CS 405

Security is a vital component of a secure development process. It is not something that should only be done once and then forgotten about. When looking at the DevOps Cycle it is important to illustrate that security is at every step of the way. Keeping coding standards in mind when developing code leads to better code that has fewer vulnerabilities. The testing phase should include testing the program's defenses. Instituting a policy of tool automation to continuously check for known vulnerabilities helps cover more surfaces than one person. The cycle doesn’t end there. As technology evolves it is best to keep checking back on the code to ensure it remains up to standard. Defense in depth is also more than code. Ensuring protection against all points of attack will protect more data.

The benefits of mitigating the possibilities of data breaches and leaks outweigh its costs. The main cost of adding security such as tool automation, is the cost of implementing it. This can be costly both in human resources and money. On the other hand, a company may spend millions in lawsuits if a massive data leak comes to light. Including security in the company's policy helps foster an environment of protection and confidence. Mitigating points of attack is another step to increase security. The more places data can be reached the more likely it will be. The benefits of security are summarized by overall safer code for both the company and the users.

Zero trust is another concept that aligns with the policy of defense in depth. It is the process of maintaining security over the internet. It elaborates on the idea of multi-step authentication. It states that measures must be taken to prevent malicious users from impersonating someone and stealing data. The three main concepts are default deny, policy of least privilege, and trusting no one.

As mentioned before, there are various ways that a security policy can be implemented. The ultimate goal is to cover as many bases as possible. Implementing tool automation, the triple-A framework, and Zero trust, are a good place to start.