Daniel Holcomb

10/22/2021

Module 8

Portfolio Reflection

**Adoption of a secure coding standard, and not leaving security to the end:** It is very important to adopt a secure coding standard that everyone must abide by especially in the software development field because if everyone is held to a certain standard in ensuring your project is safe and secure then everyone can be on the same page for security. Everyone will have a different opinion about security but by implementing these standards then everyone does not have to run back and forth trying to get an understanding of what they are expected when they are creating a function for the project. Software development teams already require great communication skills on the project itself, why make their lives harder by having to figure out how to handle a security issue when creating functions of the project? There is also the cost of the project will go up and you could miss deadlines by trying to fix security issues that you chose to ignore and put security at the end instead of during the development process.

**Evaluation and assessment of risk and cost benefit of mitigation:** You must evaluate if it is worth your time to mitigate your process from a local system to a cloud based or a hybrid. It is important that before moving anything over from one system to another that you run a security check to see if anything has been breached due to the fact that if someone breached the files locally and gave themselves a “back door” and it was limited then but a misconfiguration through the new system gives them access to everything would be catastrophic.

**Zero Trust:** By implementing zero trust, we can ensure that we are not giving anyone too much access or any program too much access that could cause an outside threat to gain access and cause issues. It also protects us from a disgruntled employee that may intend to do harm before either they quit, in the process of quitting, or before they are removed from the system and ultimately fired from the company.

**Implementation and recommendations of security policies:** These should always be updated and if there are updates, they should be sent out immediately to the teams to ensure everyone remains aware that security is an ongoing process. The cyber security teams or IT teams should remain vigilant on these and use them to determine how best to keep the company secure from the various threats or vulnerabilities that the company may have to deal with. This should not be something that is built and left alone, it should constantly be updated just as we update our applications and hardware.