8-2 Journal: Portfolio Reflection

CS-405

Michelle Fabry

April 22, 2021

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

By creating a secure coding standard, you can help ensure that you are following the same process for every project. Following a same consistent pattern for every project can help create a process that can incorporate security vulnerability checks as the code is being developed. Creating code that is readable and easy to understand and follows a code review process along with a robust unit testing format can produce an end product that has been thoroughly reviewed and tested to ensure that you have a safe secure product to deliver to production.

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

Once you begin the project process, taking the time to understand what the new process outcome should be and how it affects the users and the applications that are currently in use, you can then begin to break down and examine what the risks associated to the process will be. If you are introducing a new login process what risks are associated with this process and what are the costs if a secure process is not developed, if you are not able to avoid the risk, then understanding the risk level, you can then come up with some ideas that will help mitigate the risk and ensure that there are still some processes in place that can ensure a safe delivery to production. By being able to identify these risks at the beginning and having the ability to address these during the coding process, you can then be on alert when the product is delivered and may introduce some risks to production.

**Zero Trust**

Zero Trust policy is an effective practice to put in place that can help mitigate some of the risks that may be present within your system. By implementing the Principle of Least Privilege, you can create a system that only allows users the least amount of access to the system that they need to complete their functions within their roles. By not allowing full access to all users, this can help prevent hackers from gain full access to your data.

**Implementation and recommendation of security policies.**

Once a company is ready to implement a security policy it is best to start and identify your risks and where the highest level of risk exists at the moment and begin to build out policies from there. Once a security plan has been completed and is ready to put in place, you need to ensure that this policy is communicated throughout the company and that each user understands what their role plays in keeping and enforcing these policies are. Once the plan is place, you need to ensure that there are clear expectations and what the penalties would be for anyone that violates these policies and if a violation occurs enforcing these penalties will help create a culture that is on a path to creating a secure environment.