Greg MacPhelemy

CS 405

Portfolio Reflection

April 25, 2021

The adoption of a secure coding standard should be an aspect of development all software teams should implement. Developing software while maintaining secure code reduces the risk of the software have vulnerabilities which open the software, and potentially a network, to attacks and breaches. This course has shown me the importance of not leaving the security aspect of a project to the end as security should be an integral part of the development process.

A security policy should take into consideration the type of software and data that is being utilized to determine the risk that is involved in the case of a breach. This evaluation and assessment weigh the risk versus the cost of security implementation. The policy pertaining to a piece of software that does not manage sensitive data would not have as strict or deep policy as software that manages such data as medical or financial information of its users.

A financial institution’s software may utilize a zero-trust policy, which defaults to not trusting anyone inside or outside of the network. This requires all users to have proper authentication and authorization before gaining access to the system. A zero-trust policy creates added layers of security in the case an outer layer of security is breached, the attacker will still not have access to the system beyond the point of entry, since even users inside the network are still not trusted to move around and access data within the network.

Security policies should be implemented in all software development teams and projects. The policies should be outlined and adhered to from day one of a project. Depending on the type of data being processed will dictate the depth of the policy. Certain security practices should be included in all policies, such as buffer overflow/underflow handling and memory management, whereas other policies such as encryption and even Triple-A implementation may not be necessary for all applications. Starting off any project with a security policy for the team to follow will lead to more secure code and potentially fewer attacks on the software.