Johnny Canal Segura

CD 405

October 27, 2024

Portfolio Reflection

Adopting a secure coding standard should be standard practice to prevent countless attackers from constantly looking to exploit any system they can. This process should be exercised at every stage of the development process and not be implemented only at the end. This will ensure that any vulnerabilities are discovered early on thus increasing the effectiveness of the layers of protection. Leaving security to the end has resulted in costly breaches in many companies’ systems. These breaches not only cost companies financially but they also risk their reputation.

Vulnerabilities that may result in costlier breaches are prioritized over vulnerabilities with a lower likelihood of exploitation. This will ensure that security is implemented with the least amount of resources to avoid delays or exceeding a predetermined budget. A blueprint on how many resources will be designated to what area of the development process at the beginning to ensure appropriate resources are utilized efficiently.

Adopting a zero-trust approach will help developers consider potential attackers they would otherwise disregard by assuming attackers will not target a specific vulnerability.

Implementation and recommendations will depend on the system being used and the sensitivity of the data being accessed. Security policies that are important to implement regardless of these factors are defense in depth. A layered approach to security will always decrease the likelihood of an attack. This approach can help to protect the data of various types of companies. The more layers of security a team adds to protect a system the more likely an attacker is to move on to a weaker target regardless of the sensitivity of the data.