James Jones

Kaan Esendemir

CS-405

4/28/2024

Portfolio Reflection

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

Adopting a secure coding standard has a few benefits first there is consistency across the development team. If everyone is following the same standards this keeps the teams individual code consistent with other team members. Next is ensuring that current security trends are being accounted for the threat landscape is ever evolving, and needs to be tracked to ensure code being developed is protected against these threats. A secure coding standard also offers a great training point for new developers. Security should be considered throughout development ideally using Defense-in-Depth. Leaving security till the end means that it will either call for extensive rework to existing code or only limited security features will be added leaving the application vulnerable.

* Evaluation and assessment of risk and cost benefit of mitigation

Many known vulnerabilities include risk assessments included in their reports and can give a strong indication of how dangerous a potential vulnerability may be. However this can be subjective depending on the exact nature of the application that is being developed. The cost benefit of mitigation will nearly always be less than the cost associated with a security breach. First mitigation means limited rework while remediation after a breach may include extensive rework. There is also the cost of associated with a security breach in general such as stolen assets. Finally there is the loss of confidence from the user base which will ultimately create the largest financial strain in this specific case. Simply taking the necessary steps required to mitigate risk upfront will greatly reduce overall costs.

* Zero trust

Zero trust is the idea that “No one is safe”, anyone is a potential target. The motivations behind hackers/bad actors can range from financial gain to “hacktivism” and everything in between. This means that there is always the potential to be attacked regardless of the purpose of the application.

* Implementation and recommendations of security policies

Implementation of a security policy is something that can take some time as it could have large impacts on the development team as they work to adopt the principles and standards outline in the policy. However it will ultimately lead to a more secure development process and help build up your developers. Recommendations for a security policy should include taking into consideration the specific technologies being used and the intent of the application being developed. The industry will also impact recommendations as industries such as healthcare and finance have many of their own regulations that must be incorporated. This comes down to there is not simply one security policy that can be used across the board but instead every development team/company needs to create their own that will work best for them.