CS405

Sheel Patel

August 21, 2024

Journal: Portfolio Reflection

As we have discussed throughout this term, security should not be left to the end. Adopting a secure coding standard is crucial to making sure that secure is embedded at every stage of the DevSecOps lifecycle. By adopting best practices for secure coding via set standards, which developers can use as guidelines on how to avoid common pitfalls that lead to vulnerabilities. By introducing developers to these standards early, they are less likely to develop bad habits that lead to vulnerabilities. In adopting a secure coding policy, a proactive approach is taken and the code produced is more secure. This in turn mitigates the time and monetary cost of having to correct any issues later and a better, more secure product.

Evaluating and managing threats is a costly process, in regards to both money and time. In attempting to correct all issues, the cost must be weighed against the benefit. However, being able to do so requires a strong knowledge of the likelihood a specific type of incident will occur and the severity of the incident. While layering all security measures may protect against all threats, there is a cost to utilizing a strategy like this. The more layers of defense are added, the greater the resource cost imposed upon the system. A balance must be struck between the cost to mitigate and the level of threat reduction it provides.

One strategy for mitigation is deploying a Zero Trust model. The Zero Trust model assumes that there may be threats which exist both on the inside and the outside of the network perimeter. As such the model works off of a "never trust, always verify" principle. Any request, inside or outside, is treated the same, as though they are a threat. Implementing a Zero Trust model can be difficult as it requires a different approach, deeper insight into actions taking place on the network, and a thorough authentication and authorization process so only the appropriate users have access to confidential and privileged resources.

Security policies provide guidelines for what should be done in order to protect the company and its assets. To properly deploy security policies, there must be training, mechanisms to enforce the policies, and clear communication. The policies should be designed specifically to address the needs and possible risks of the company. It's recommended that policies be updated on a regular basis to ensure the new threats are addressed.