Michael Shunk

SNHU CS 405

December 17, 2022

Module Eight Journal

When examining the security of a system, there are a number of factors to consider:

* Adoption of a secure coding standard

A coding standard will give developers a framework to help them create secure code. The entire organization will be on the same page as far as best practices, providing consistency throughout the code. I believe the biggest advantage of this is that it helps embed security in the design of a system from its inception. When security is considered in the design and coding stages, it provides a secure foundation for the rest of the development process.

* Not leaving security to the end

Security should not be thought of as an afterthought. Not only is it more work to implement after the fact, but it may also not be as effective. If the underlying system has security flaws that are inherent in its design, no amount of retroactive security measures can fix that. By utilizing secure coding standards, security will be considered from the start. Using practices like DevSecOps can also help ensure that security is engrained in every step, from planning, development, testing, deployment, operation, and maintenance.

* Evaluation and assessment of risk and cost benefit of mitigation

There are a number of things to consider when evaluating the risks a system may face. First, one must consider the motivations of hackers when it comes to your system. What kind of data might they want to steal? Or would they want to simply interrupt your system’s operation? Honest consideration of these questions could help inform future security policies. The risk of attacks also needs to be evaluated against the cost of doing nothing. Attacks can have huge financial impacts, which need to be weighed against the cost of mitigating potential attacks. Aside from financial impacts, organizations could also suffer reputational damage, the cost of which can be harder to compute, as it may become an ongoing liability. Government sanctions could also be a possibility if an organization is found to be negligent with their security.

* Zero trust

While having authentication in place to prevent hackers from accessing a system is a good start, many attacks begin with the hackers having valid credentials. Once inside, there may be few limits to what they can access. Zero trust policies ensure that all requests made in a system are continuously validated and can be so granular as to consider the user, the device they are using, their location, and other attributes. This can give us the upmost confidence that the person accessing a resource is who they say they are and that they are allowed to do so.

* Implementation and recommendations of security policies

By having security policies in place, everyone involved in the system, from developers, IT staff, and users, will be understand what can be done to create a system that is secure as possible. Developers will have guidance on creating secure code, IT will know what kind of network structure needs to be configured and users will learn best practices to prevent their credentials being abused and how to avoid attacks like phishing and social engineering. Having security policies in place can go a long way to prevent attacks, but just as the technology that these systems use constantly changes, so do they attacks they face. This necessitates regular reevaluation of policies to make sure we’re always a few steps ahead of hackers.