Module Eight Journal

As developers, we must be proactive when it comes to vulnerabilities, errors, and bugs, and should be securely coding software from the beginning. Adopting a secure coding standard and following the policy can remove commonly exploited vulnerabilities. Coding standards are guidelines, rules, and best practices a team should focus on to create high quality, secure code. These standards can also help by reducing development and maintenance costs, by reducing the number of vulnerabilities from the beginning, rather than later in development.

Through the development process, software is always at risk of being exposed to vulnerabilities, bugs, and errors. These risks can expose the software and data of the consumers and company. Not leaving security to the end is a best practice that every developer should follow. Malicious users are always finding new ways to crack into software, and always searching for a way in. Developing without security in mind leaves an “open door” which can let attackers in easily, and if a breach does occur, it may already be too late to protect the data that may be compromised.

While developing software, risk assessment should be performed to provide an overview of potential risks and vulnerabilities, along with the level of severity for each risk. These vulnerabilities can lead to financial loss from data breaches, downtime of systems, etc. Performing a risk assessment can help a team determine what the most important/dangerous vulnerabilities they may face in their development are, so they can prioritize mitigation to reduce the possible financial burden.

Zero Trust is a new, strategic approach to security which eliminates implicit trust, and requires validation during every stage of a digital interaction. With traditional approaches, trust is somewhat of a “castle”, where anything inside the “castle” is trusted, and anything outside is not trusted. This would mean that anything on the network, including threat actors and malicious users, are free to move around the network, pivoting from one application to another, to possibly access sensitive data. Zero trust requires all users to be authenticated, authorized, and continuously validated to access the network, remain on the network, and change what they have access to (such as moving from one application to another). This helps, especially in today’s modern work lifestyle; remote work and cloud-based environments.

Security policies can help protect the assets of an organization, and generally identify the assets, owners of the assets, and any threats towards the assets. Assets are both physical and digital, and can include computers, IT equipment, and sensitive data. Implementing a security policy is also used to provide guidance as to how to protect the assets. Since it is such a complex digital world, and hackers and threat actors are constantly evolving their methods of attack, we must be vigilant in preventing these threats from being successful.

A security policy should include things such as the purpose of the policy, coding standards, security principles, a risk assessment, summary, and any other necessary details a company requires the team to follow for guidance. This policy may also be updated with recommendations. These recommendations can be different principles, standards, etc., that a company should implement at some point in the future. Since technology is always changing, and new vulnerabilities are always developing, developers must be able to update their software to protect their assets.