Christopher Gaceta

8-2 Journal

Secure coding can span a wide range of topics and it’s important to begin by adopting a standard that can be used within the company. By not leaving security to the end, we can start implementing secure coding within the early stages of the development lifecycle. For example, having Secure Coding Practices such as the SEI CERT Coding Standards, we can always account for these security policies in our coding. Validating input, heeding compiler warnings, keep it simple, default deny and practice defense in depth to name a few help construct the security policies and adopt a secure coding standard.

When evaluating and assessing the risk and cost benefit of mitigation, we need to ask the developer how important the application or software can be and the financial implications if it were to be compromised. For me, I would not put a price budget on IT security as it can cost millions to attempt to fix as well as the bad PR the company would receive. By implementing secure coding into our practices, we can eliminate the potential of risk which will save money for the company in the long run.

When thinking of "No one is safe" and the zero trust policy, I believe this is a great mindset to take when developing security for a company. There are cases where the hacker is working externally, and there are cases where the intruder is internal and has access to the systems. If they are internal, they are able to take/steal data and information that makes it easier since they have the credentials to access the network. It's important to regulate access for all external and internal users.

As a user, I should only have access to what I need to do my job. If I am an entry-level engineer, with senior access or CEO access I can do a lot of harm even by accident. Workers who work remotely will need a secure environment to get into the network and complete work, as well as companies who use cloud systems to manage their data. Authentication and authorization play an important role as well for every single user in the company. Credentials will need to be provided for zero trust policy to work so entries can be logged and tracked.

When it comes to recommending and implementing security policies, it is essential to have a foundation and defense in place for possible intrusions. Defense in depth provides layers of security and slows down the hacker from getting into the data of the company network. There are many ways to test for security such as unit testing, code analysis and reverse engineering. B recommending and convincing developers to utilize secure coding and policies, there will be a uniform policy that everyone can use and follow to be on the same page.