Larry Arndt

CS-405

February 24, 2023

Journal: Portfolio Reflection

When I worked in the SysCon.. short for system command in Bosnia for the signal network that supplied the Lt. Colonel his briefings to give to the 1st Armored Division General whose tanks we provided direct communications for the password was “trustnoone”. This is the attitude you need to have with your security because truly “no one is safe” A secure coding standard is a must have. All your coders must be on the same page and avoid making silly programing errors that let hackers slip in. This defensive posture is a must have component of any would be secure network.

Evaluating which of the coding standards pose the highest risk is paramount as well. This lets you focus training at the highest risk areas so you get the highest cost benefit and most mitigation of vulnerabilities. Zero trust is also key, as you want to implement triple-A policies as recommended where you authenticate your users with at least two factor identification methods. You make sure that they only access what they are authorized to access and that you account for all activities done on your systems with logs that have a detailed trail of all past actions taken.

You data also needs to be protected at all times, most likely to with encryption. Also, with authorization; systems and people should not be able to access it when it is not appropriate for them to do so, and it should be encrypted while it is at rest, in flight and in use. Stored data is protected, moving data is protected, and data that is being created and edited is protected. These security policies and recommendations work together to protect a system.