Jacob Steckel

CSC402

Article Review 5

Adopting a Software Security Improvement Program

In this article the main point that the author is trying to get across is the importance of adopting a software security improvement program and the benefits that could come with such an idea. Developing the improvement program is no easy task, any time a company attempts to change the culture or the way it goes about things adversity is surely going to arise.

The roadmap showcased in this article goes over five basic steps that a company should take to improve their software security. The first is to build a tailored plan. This means that you must look over the way your company goes about things and decide what is the best way to gradually adjust your tendencies over time to enhance software security. The next step is to roll out individual best- practice initiatives carefully, meaning that you need your best men to take a leadership role in attempting to spread the best software security practices throughout your company. Next is train your people. In order for developers and engineers to utilize the best security practices, they must be aware of them and be trained on how to implement them. Establishing a metrics program is another step in the improvement process. The metrics program will be used to monitor progress and analyze the success that is occurring in the software improvement program. Knowing how you are doing with the improvement process if crucial. The last step is to establish and sustain continuous improvement capability. This means that you should constantly be trying to improve your weak points at all times, at no point is your security software too good to improve.

The article then goes over six different phases that your program should undergo to improve your software security program. Phase one is stop the bleeding where you locate all the biggest issues and bugs within your program. Phase two is harvest the low hanging fruit, where you focus on finding quick wins regarding building your program. Phase three is establish a foundation, where the company creates a good foundation so they can provide a way to build upon it in the future. Phase four is craft core competencies, where the company adopts software security practices that tailor towards the organization’s strengths. Phase five is develop differentiators, where you highlight your company’s attributes and characteristics that are unique and are not simply duplicated by other organizations. The last phase is build out the “nice to haves”. This phase involves adopting capabilities that don’t always relate to productivity.

This article was an interesting read because seeing how companies go about improving their software security is quite fascinating to me.