Andrew Kuhn

8-2 Journal: Portfolio Refection

Southern New Hampshire University

04/19/2021

Adoption of a secure coding standard and not leaving security to the end, are two very important concepts that should be adapted by every company. A secure coding standard creates a policy to be followed by developers to maintain secure code. Without secure code, you are leaving yourself open to several vulnerabilities and potential financial liabilities. By not leaving security to the end, you will help fill holes within your system. It is much easier to make sure code is more secure line by line, rather than extracting a jar file to look at security vulnerabilities. If a developer looks at every class, they create to make sure there are no vulnerabilities, it will be a much more secure product in the end.

When evaluating and assessing risk and cost benefit. It is definitely a difficult task. As a lower-level employee, my job is to make sure things are secure. Not to determine the risk and reward of different vulnerabilities. However, it is a very important task. When looking at the potential risks of a security breach, you must determine whether it is financially responsible to mitigate the risk. This goes without saying, a 50k fix is not worth a 5k issue. However, a 50k fix is more than reasonable for a 5-million-dollar issue. This is the type of breaches that make the headlines when a company gives up millions of user information and credit card information.

When evaluating security of a company, following a zero-trust policy is something that should be required everywhere. If a user clicks a link on an email, it could potentially allow access to your entire system. This is the most common way that a hacker will infiltrate and steal valuable information. If a user were to follow zero-trust, this would not be an issue. However, people do not tend to look to deeply into what they are clicking on.

To implement security policies, there is a lot of studying and framework knowledge of a company. It is much easier to implement in earlier stages of a company but can be done at later stages as well. When implementing these policies, it is important to make sure that there are reasonable strategies that everybody can rely on. It would not make sense to give only one user access to write to a system. With that being said, not every user needs to have write access either. This is something that can be implemented on a scale, where dedicated team leaders and management have write access, and other employees are only granted read access. This will help a second set of eyes before someone accidentally runs a delete query rather than select on accident.

This course has been very valuable to my knowledge and future career aspirations. I currently work in the electronic medical record tech field, and security is one of the most important features of our business. As my college classes come to an end, I look forward to continuing growing my knowledge in the tech world. With the world of technology changing on a daily basis, learning new things should be an everyday event.