Kathryn McNeil

CS 405 Secure Coding

Southern New Hampshire University

12/18/2022

It is important to adopt a secure coding standard to provide guidance to your systems security. Creating a system can take a long time and can include many different people throughout the development process. Due to this, if a secure coding standard is not adopted, people may end up doing things differently. This lack of cohesion in the system can lead to vulnerabilities and lower your systems security. If a coding standard is used throughout the process then this can be avoided. It is also important to consider security from the moment development begins. This is the idea of not leaving security to the end. As with the coding standard, development can be a long process. If security is not considered until the end then there can be months’ worth of work that needs to be combed through to improve security. This is not only time consuming, but also unnecessary because if security is considered from the beginning then it will not need to happen.

While considering security it is important to consider the evaluation and assessment of risks. Security can be quite costly and in certain circumstances the highest form of security may not be necessary. For example, a small startup creating a simple gaming app that is free to download and use and does not handle sensitive data such as credit cards does not need the same amount of security that a banking app from a large banking company does. In this situation, the small startup may actually hinder their growth by investing too much money into security that is not really necessary. Meanwhile, it could be detrimental to a large banking company to not invest in the highest form of security for their app. Looking at these two companies, the startup has little risk. They are small, not handling sensitive data, and cannot afford to spend a lot of money. The bank is very large and well known making them a target for hackers. They also handle sensitive information such as people’s names, addresses, savings accounts, and credit cards. This company can lose millions of dollars if they have a severe data breach so it is worth it for them to invest in more security.

Mitigation in security refers to limiting the impact attacks can have on your system through the use of various security strategies. This is so important as proper mitigation techniques can save companies millions of dollars. Because of how prevalent hackers are, when one is developing a system it should be assumed that an attack will happen. This is where mitigation comes in; assuming that the system will be attacked, what can be done to prevent the worst possible outcome? By asking these questions a system that is much more secure can be created. This will not only serve to protect the company and its users, but also save the company a significant amount of money in the long run.

Zero trust is the idea of assuming every user is malicious. With this in mind, users have to verify themselves whenever attempting a significant change. Looking at google, we can see they implement this technique. For instance, the password manager saves your passwords, however, they cannot be accessed without entering your google account password. One has to be logged into google to access this page, and then reverify oneself to view the information. Google also does this with credit card information. One must be logged in to autofill your card information, however, one has to enter their CVV security code before Google will do it. This is a great technique as it is adds another layer of security to your system.

When planning security for a system it is important to think about where security will be needed. Consider what the system will do as well as its various parts. Think about where throughout the system attackers may target. For instance, where can common attacks such as SQL Injection occur? Once this understood one can start to choose the security policies that are right for their system. Perhaps you want to utilize defense in depth to mitigate damages when an attack occurs. Maybe you also want to make your security a zero trust system to prevent hackers from making changes they should not be able to. The most important thing is for you to have a good understanding of your system so that you can make decisions in security that will most benefit it.

Resources

Defense in depth (computing). (2022, August 14). In *Wikipedia*. https://en.wikipedia.org/w/index.php?title=Defense\_in\_depth\_(computing)&oldid=1104320010

HYPR. (n.d.) *Mitigation*. <https://www.hypr.com/security-encyclopedia/mitigation#:~:text=Mitigation%2C%20or%20Attack%20Mitigation%2C%20is,activism%2C%20retribution%2C%20or%20mischief>.

Raina, K. (2022, October 17). *Zero trust security explained: Principles of the zero trust mode*. Crowd Strike. https://www.crowdstrike.com/cybersecurity-101/zero-trust-security/

Seacord, R. (2018, May 2). *Top 10 secure coding practices.* Carnegie Mellon University Software Engineering Institute. https://wiki.sei.cmu.edu/confluence/display/seccode/Top+10+Secure+Coding+Practices