Daniel Coffey

7-1 Journal: Consider the Motive for the Attack

CS 405 Secure Coding

02/20/2022

Motives can vary from person to person, so it is beneficial to be conscious of all the possible motives so you can be prepared to prevent an attack. There are common types of cyber-crime that plague the internet and business such as phishing emails, malware attacks, and ransomware. It is important to understand what a hacker is motivated by. There are six different types of motivations, and they are cash, challenge, hacktivism, revenge, subversion, and infamy. A hacker that is motivated by cash is trying to get money from stealing your information or selling your data to competitors on the dark web. A hacker who wants a challenge is tempted to break a system that is heavily guarded, and this will breed competition and recognition from other hackers. Some hackers believe if they target large companies, they are performing their own form of activism. Some hackers are looking for revenge, they utilize their anger and skills to target a person, group, or corporation. Some hackers live subversion. They like to meddle in current and corporate affairs. Lastly, hackers are motivated by accomplishing their goals and being notorious, especially now that they have multiple platforms to brag on.

While these are motivations for a hacker to hack, there are also three different types of hacking. Black hat hackers are the worst type of hackers because they spread malware in hopes to make financial gain. White hat hackers are known as “ethical hackers” and businesses utilize them to check for security vulnerabilities. Grey hat hackers are somewhere in between black and white hat hacking. They don’t look for approval and will do what they want but they also will report any vulnerabilities found, for a price. If they aren’t compensated properly, they might exploit the vulnerabilities.

I would explain to a new developer that the best thing we can do is utilize defense in depth and create tests. Hacking incidents happen all the time and the best thing we can do is try to be prepared for all of the possible scenarios. We can utilize automated security testing tools to make sure systems are up to date. Utilizing defense in depth will allow us to have backups for any line of defense that has been penetrated.

An example of this concept that I can talk about in my final reflection is the project that I just completed. The project encompassed defense in depth, a threat matrix, the 10 principles and 10 standards, the encryption policies, the triple-a policies, unit testing and examples, automation for pre-production and production, and tools to be used. It also went over the risks and benefits of defense in depth. I think utilizing all of this will help any development team be prepared for a potential attack.

