Vincent Snow

Journal Module 7 – CS405

02/25/2024

There are many possible motives behind hacking and attacks on software and computer systems. Whether malicious, selfish, or for curiosity, understanding motives may help us predict attacks and vulnerabilities. Considering these attacks should be part of a developer’s mindset in a DevSecOps process, and they should be discussed in the planning phase. For example, if you know your application will hold financial information for customers, you know that people will want this data to make a profit for themselves. Data leaks for this reason are now something that can be planned for and focused on. You can prioritize protection against data leaks, come up with a solid encryption plan, and a response plan that protects customers from financial loss in case the security methods should fail.

To a new developer on the team, I would explain the different types of common hackers and reasons they may do what they do with a few examples from news articles. All developers on the team should be aware of where danger lies. If the company has rival competitors, this is another example of things to be aware of. We may need to be extra careful about authorization and physical security measures. In any case, knowing motivations helps us prioritize.

This concept can be discussed in module eight’s reflection for the topic of ‘Zero Trust’. Hackers can be anyone – a disgruntled employee, a stranger, a business rival, a political rival, a criminal, even someone who believes they are doing something good and trying to help you by bringing attention to a vulnerability and demonstrating it. Throughout this class and degree, we have studied security many times and read articles in the news about cases of cyber-crime from all colors of hats. In Discussion three, I talked about a hacker who decided to hack a Facebook executive’s page and post links to it after his bug reports were ignored. This is one example for zero trust – Facebook's security failed in the Authorization area of AAA because a vulnerability allowed an unauthorized user to access members’ pages and edit them.