**Module Seven Journal**

Joseph Veneski

Department of Computer Science, Southern New Hampshire University

CS-405 Secure Coding

Professor Kaan Esendemir

April 21, 2024

**Module Seven Journal**

**Applying Concepts:** Applying security concepts regarding determining motives and preventing common attacks should involve several strategies such as threat modeling, code audits and reviews, security training and awareness, and incident response plans. In a DevSecOps pipeline it is common to see threat modeling in the planning and design stages to understand what potential risks the system may be subject to and what attackers may possibly gain (PureStorage, 2023). As development begins, code should be subject to auditing and reviews to ensure that standards are met, and teams can share knowledge and improve their abilities. Threat modeling alone is not enough, often other strategies in combination are used such as creating user stories specifically aimed at security cases and possible interactions a bad actor may take. Raising awareness and increasing security training will help teams understand common motives and attack vectors which can help them build more robust and secure code. Finally, having incident response plans in place can help ensure swift reactions as well as increase understanding of the motive for potential future attacks.

**Explaining Concepts:** To explain to a new developer on the team the importance of understanding motive, I would discuss some of the most common security risks and vulnerabilities such as buffer overflows, SQL injections, cross-site scripting attacks and how they disrupt the system. It is important that new developers understand why someone would use one of these vulnerabilities to attack the system for gain, whether it is reputation, financial, political, or just to spread chaos (IBM, 2024). One of the best methods for me was to look at case studies of security breaches to understand the motive behind attacks such as selling consumer information on the dark web or causing service interruptions.

**Example:** An extremely common example of malicious attack is through ransomware which according to the Data Breach Investigations Report by Verizon in 2023, was involved in 24% of all breaches (Kerner, 2024). Ransomware attacks seek to block access to systems until a sum of money is paid. In these types of attacks, it is also common for attackers to attempt to steal personal identifiable information (PID) to use or resell as well. There have been numerous ransomware attacks already in 2024 such as by LockBit Ransomware on Crinetics Pharmaceuticals in March in which the attackers demanded a sum of $4 million USD (Cyber Management Alliance, 2024). Luckily, the company actively monitors activity logging and was able to notice the suspicious activity right away and locked down the compromised employee account the attackers were using. No matter what software is being designed, developers need to understand what potential risks are involved and how attackers will try to disrupt and abuse what is being developed. Keeping security in mind and taking a preventative approach will help developers create more robust and secure systems.

**References**

Cyber Management Alliance. (2024). *Biggest Cyber Attacks, Data Breaches Ransomware Attacks: March 2024*. <https://www.cm-alliance.com/cybersecurity-blog/biggest-cyber-attacks-data-breaches-ransomware-attacks-march-2024>

IBM. (2024). *Why Do Cyberattacks Happen?* <https://www.ibm.com/topics/cyber-attack#:~:text=Threat%20actors%20start%20cyberattacks%20for,damage%20and%20even%20destroy%20businesses>.

Kerner, S. M. (2024). *Ransomware Trends, Statistics and Facts Heading Into 2024.* <https://www.techtarget.com/searchsecurity/feature/Ransomware-trends-statistics-and-facts>

PureStorage. (2023). *How to Implement Threat Modeling in Your DevSecOps Process*. <https://blog.purestorage.com/purely-technical/how-to-implement-threat-modeling-in-your-devsecops-process/#:~:text=Threat%20modeling%20is%20the%20process,can%20be%20exploited%20by%20attackers>.