Victor Jarvis

CS 405

Journal: Consider the Motive for the Attack

Understanding the motive behind cyberattacks is crucial for anticipating them and hopefully preventing them completely. By focusing on why an attacker might target a system, an organization can better identify their vulnerabilities and implement more robust and effective defenses. For example, if an organization handles sensitive financial data, the motive would be financial gain, and by knowing this, they can prioritize securing payment gateways, customer information, and transaction records. Regularly updating threat models to include potential motives and aligning security measures accordingly can greatly enhance an organization’s cybersecurity posture.

When onboarding a newer developer, it’s crucial to explain that cybersecurity isn't just about the code necessarily. It’s also about understanding any potential attackers' motives. For example, if they're working on a project involving personal client data, you would say "Imagine someone wanted to steal the client’s personal data. Why would they do that? To sell it or blackmail someone? Knowing this, we have to keep secure the parts of our application where personal data is stored or transmitted, using encryption and access controls." It helps to encourage them to always think from the perspective of an attacker: what would they gain, and how would they try to achieve it?

In a scenario where a company experienced a ransomware attack, initially the motive might seem purely financial if the attackers demand payment for data decryption. However, upon deeper investigation, it could also be discovered that the attackers stole sensitive corporate data. This dual motive (financial gain and corporate espionage) highlights the importance of considering multiple potential motives in cybersecurity strategies. Upon reflection, an organization might conclude that understanding the full scope of an attacker's motives could have led to a more comprehensive defense strategy, potentially preventing the data breach from happening in the first place.