CS-405-10861-M01 Secure Coding 2024 C-3

7-1 Journal: Consider the Motive for the Attack

Computer Science Department

Southern New Hampshire University

Eric Farkas

6/23/2024

It is challenging to predict the motives for hacking a system. One strategy for predicting risk is considering which motives apply to your organization. Financial gain should always be considered. Organizations that do not have or transact large sums of money often overlook it because they believe the risk is low. Hackers have been known to seize control of company systems or assets and extort money from the company to regain control. Companies that hold patents, trade secrets, and formulas are often targeted. Proprietary information is valuable not only to the owner but also to their competitors. This type of motivation is considered espionage. Hackers often target companies with large amounts of computing power or networks. The motive is to gain control of the computing power or network and use it for the hacker’s purposes. Some motives have no indicators. Hackers simply looking for a challenge or recognition may target an organization simply because they have never been breached before.

The best defense is a holistic, multi-tier security approach. The company should implement firewalls, antivirus software, intrusion detection, and periodic security audits. These measures will result in a robust cybersecurity plan. Employees must be empowered and trained to do their part. All employees should attend regular education on phishing, social engineering, credential management, and safe online practices. Business systems should require strong passwords, multi-factor authentication, and encryption. All devices and software should have a frequent maintenance schedule to apply updates that patch vulnerabilities. A data backup and disaster recovery plan should be established to ensure business continuity should a successful attack occur. The cybersecurity practices of any off-site services like cloud platforms and software-as-a-service providers should be evaluated and documented. Be careful to include framework and application dependencies. These are often maintained and patched outside the organization but remain in scope for patch verification and response actions. A response plan procedure should be established to outline detection, containment, and recovery strategies.

New developers should review the company security plan during their onboarding process. They should be interviewed to ensure they understand all aspects of the plan and ask any questions they may have. If deficiencies are identified, training should be scheduled to improve the new developer’s competency. They should be asked to review the current security policy and acknowledge compliance. The new developer should be allowed to contribute to the security policy should they identify an area where they can help. A meeting should be arranged to introduce the new developer to the security stakeholders. This meeting should cover roles, responsibilities, areas of subject matter expertise, and escalation procedures.

Password management is a significant area of concern for system security. Working professionals require access to dozens of systems to perform job tasks. Password policies have increased the complexity and frequency of updates to the point where passwords are complex to recall from memory. Many users leverage weaker passwords with easily memorable patterns that are incremented when a change is requested. Single sign-on (SSO) is a strategy companies implement to overcome the need to log into each system. While this simplifies user logins, it introduces credentials that can simultaneously compromise many systems. Multi-factor authentication (MFA) verifies that those credentials are being entered by their owner but is often accomplished with an SMS code or push notification response. Using strategies like this requires additional device security. MFA is ineffective when the tablet or smartphone the system leverages for additional verification is compromised or in a hacker’s possession. I will use this type of example in my final reflection.