Joseph Silva Jr.

SNHU

CS 405: 7-1 Journal: Consider Motive of Attack

12/12/2021

* **How will you apply this concept to your own practice?**

When it comes to a hacker’s attack, I would compare the attack to my experience with crimes on patrol. During my interviews and investigations on patrol, I always discovered the type of crime, frequency of the crime, and the number of victims by learning the motivation of the suspect. For example, theft from a vehicle usually occurred at nighttime and there were multiple victims in the neighborhood usually came from a criminal(s) who had the motivation to steal for money and opportunity. Learning this motivation, I was able to find suspects by looking at surrounding neighborhoods and areas to locate video footage to find vehicle information and suspect(s)’ descriptions. Comparing an in-field crime with a hacker’s attack, the motivation of hacker will be helpful to protect and recover from an attack. When it comes to creating security standards for future attacks, the policy would have to take all the different types of motivations for hackers instead of only focusing on one type of hacker. After an attack occurs, a motivation on the list will be able to be singled out in order to discover who has attacked the system. To discover a motivation, a security team will have to take multiple factors into consideration such as: the type of corporation / government, any current events, type of security policy, and personnel.

* **How would you explain this to a new developer on your team?**

The best way I would explain security against a hacker’s attack and recovery from an attack would be comparing the hack to real life security features. The explanation to developing code to protect a system from an attack would be compared to how locked / secured doors, walls, security signs, etc. are used to protect and also deteriorate someone from attacking a system. Next, I would explain how developing programs that can be tested and dissected by the security team will help to investigate by comparing these tests from an attack to be like using security cameras, fingerprints, etc. to discover a pathway to find the attacker by looking for areas of code where the attacker might have left “evidence” behind. The better a developer does in developing a program’s security features will either prevent attacks from happening and/or assist a cyber security team to follow the path in locating the attacker.

* **What is one example of this concept you can use in your final reflection in Module Eight?**

One example I would use would be combining real life events and digital security features together to update my security policy for a specific attack and to also discover the motivation of a hacker after an attack has occurred. Being up to date with current events, a developer and a security team can prep themselves for an oncoming attack. For example, a company receives a large government contract in developing a program to keep track of personal information on employees of the government agency. The company’s security policy should prepare for any possible attacks in regard to hackers motivated by cash, terrorism, other countries’ government, and/or infamy.

**CITATIONS:**

1. Khagram, A. (n.d.). *The motivations of a Hacker*. swcomms. Retrieved December 12, 2021, from https://www.swcomms.co.uk/blog/article/the-motivations-of-a-hacker.