**Journal: Consider the Motive for the Attack**

Justin Starr

Department of STEM

CS 405 – Secure Coding

Professor Mike Alesso

August 18, 2024

**Journal: Consider the Motive for the Attack**

I will apply the concept of considering the motive for the attack by first thinking about why a cyber-criminal would want to attack the organization in the first place, and what they could gain from it. Whether it be monetarily, such as in the case of a DoS attack where your services are held for ransom, or an attacker breaches your infrastructure and steals sensitive information, holding it for ransom, or even selling it to other criminals, it is important to consider what could an attacker want and how could they benefit from it. Reasons could extend to other areas of interest, such as ideological reasons, political reasons, and even simply prestige and curiosity (Hosburgh, 2017). By considering all possible motives of an attack, you are able to have a better understanding of what needs to be protected and to what lengths you should attempt to secure it. If an organization does not think about motives of attacks during development and deployment, the organization seriously risks exposing itself to any number of potential attacks, especially the larger the organization it is. That is not to say though that only large organizations are susceptible to attacks, small companies are also susceptible to attacks, as it relates more to the services a company provides rather than its size. Therefore, I will apply this concept of always considering what services I provide, thinking about who might want to attack these services, and for what purpose. This will aid me in understanding what needs to be protected and to what extent I should implement security measures to help safeguard the organization from potential threats.

The way I would explain this to a new developer is similar to how law enforcement agencies seek to understand motives for crimes that are committed. Law enforcement officers often seek to answer the question “What was the motive for the attack?” because it often points investigators in a more concrete direction that enables them to understand the “why”, which can aid in discovering more information and evidence that can help support a case and find criminals (Hosburgh, 2017). This is similar to how we as developers should be considering motives for potential attacks against an organization. Explaining this to a new developer in this way will help them better understand that by thinking about motives for attacks, they can begin to think about how they will need to incorporate security throughout their development process, and what services they must ensure are safeguarded. This could also help by bringing a sense to the new developer that security should be taken into account from the very beginning of the development process and applied as an industry standard and best practice.

An example of this concept would be financial institutions, and how they are targets of cyber-attacks primarily related to financial benefits. If financial institutions did not consider that they would be targeted by cyber-criminals seeking to find ways to steal money from these institutions, whether it be from the institution itself, or individual account holders, they would not be well suited to protect themselves and their customers from these types of attacks. Understanding what services your organization provides, and what assets require protection, will help developers ensure that they incorporate security into their designs, helping to reduce the likelihood of malicious attackers gaining access to the organization's assets, whatever they may be.

**References**

Hosburgh, M. (2017, November 13). *What are the motives behind cyber-attackers?* CGS.

<https://www.cgsinc.com/blog/what-are-motives-behind-cyber-attackers>