WHAT IS SECURITY THREAT MODELING?

Due to the rapid advancement of technology, the increased risk of cyber-attacks and system breaches has become a day to day issue that constantly needs to be addressed. From running payment software to data collection to use of the cloud, every area of an organization needs to be aware of liabilities as well as put plans into place to protect against them. However, when it comes to IT and tech, many organizations see security as a complex problem that is so big and intimidating that they often become lost on how to start or where to focus vital resources.

And, to make the problem worse, understanding the actual threat model can be complex. The answer of most organizations is to seek help from cybersecurity specialists who immediately ask, "what is your threat model?"--a jarring question that in-and-of-itself is exceptionally difficult to answer. The truth is, "threat modeling" is obscure jargon that does not reference one thing specifically and has no agreed-upon standard within the tech security industry. Commonly thought of as the act of being prepared and prioritizing threats, if you do some research on the topic, you will quickly realize there are a variety of expert opinions, framework structures, and methodologies out there. Nevertheless, threat modeling is one of the most important parts of the day to day practice of security.

In the following article, we will take a look at what threat modeling is, undercover how to answer the above question with confidence, and why there are so many frameworks from which to choose.

What is Threat Modeling?

Intended to be used as a cost-effective tool to help software/IT teams implement features that protect systems, at its core threat modeling is very simple. According to Wikipedia, it is defined as "a process by which potential threats, such as structural vulnerabilities or the absence of appropriate safeguards, can be identified, enumerated, and mitigations can be prioritized. The purpose of threat modeling is to provide defenders with a systematic analysis of what controls or defenses need to be included, given the nature of the system, the probable attacker's profile, the most likely attack vectors, and the assets most desired by an attacker." It can technically be applied to any aspect of life, serving as the foundation of everything a security professional does.

With that, beyond the core of what threat modeling is, the complexity of answering "what is your threat model?" starts when addressing all the different technical aspects of your unique organization as well as keeping in mind how different causes combine to create new threats. In reality, there is an unlimited number of threats that could cause damage to the security of an organization. Daunting as it may sound, ultimately, the end result of a strong threat model is an overview of a system as well as profiles of attackers with goals, along with a full list of vulnerabilities, outside threats, and potential inside breaches.

What Most Threat Models Include

Due to the uniqueness in nature, most threat models do not look the same but generally include the following basics:

- A description of the threat
- A list of assumptions regarding the function of the software or organization that can be reviewed in the future
- Vulnerabilities
- Actions for each vulnerability
- How to review and verify the vulnerabilities are being watched and are secure

The Basics Of Uncovering Vulnerabilities

A four-step process that can be done at any stage of system development and implementation or lifespan of an organization, the sooner threat modeling takes place the better, even if it's simple at first then built on. To start, in the tech world most experts agree that identifying threat modeling vulnerabilities is the systematic and structured answering of the following four questions:

1. What are we building?
2. What can go wrong?
3. What are we going to do about that?
4. Did we do a good enough job?

In the business world and when looking at an entire organization, the four questions turn into:

1. What are the high-values assets within the organization?
2. What areas of the organization's environment are vulnerable?
3. What are the most relevant threats to the organization's security?
4. Is there an attack vector that might go unnoticed, did we look for everything?

All easy to remember questions that are designed to be helpful in identifying assets along with weaknesses, each can be applied to a variety of projects, including waterfall or agile builds. The wording and answers to the four questions might look different from one project to the next, but the four principles and approaches remain the same.

For example, beginning with question number one, this starting point is used to define and decompose the scope of the project and threat model. If this question cannot be answered then answering the rest of the questions will be difficult. Do not move on from number one until it is entirely answered.

Moving on to question number two, this is the research phase that should also involve a number of team members collaborating with different awarenesses. The goal here is to find and brainstorm the main threats that can happen. At this time is when one of the many expert methodologies/frameworks like STRIDE, DREAD, PASTA, or VAST, just to name a few, can be applied. These techniques will include data flows, checklists, diagrams, and classifications, with personal preferences as well as the purpose of the threat model guiding the decision-making.

In question number three, the focus is to identify actions and mitigations. It is a clear and detailed explanation of every possible countermeasure.

Lastly, in question number four, it is time to look back and address quality, ability to carry out, progress, and most importantly, rank the threats.

When all four questions have been addressed, the result is a working threat model and an answer to the above, previously daunting, question “what is your threat model?”. Having highly detailed answers and a structured approach to each of the questions makes the threat model stronger. Take time to dive deep and fully answer the questions.

Brief Best Practices

No matter what type of framework is used or the focus of the threat model, there are a few key things that will help the process run smoothly. First, always take threat modeling seriously, considering it a priority from the start. This will save a lot of time and effort for all teams across an organization. Second, remember to consider the entire system and its working parts as a whole, not just in isolation. Causes can combine and affect another cause, so can system and application parts. Third, think outside of the box. Vulnerabilities can come in many shapes and forms. Users and employees are often more of a threat than a hacker. Consider things like what happens if an employee takes a laptop home and works off of your secure network or when they don’t change a password often enough. Always use threat modeling as a tool to constantly update and record new concerns.

Taking the energy and resources to correctly identify and allocate efforts to ensure your organization’s safety and systems’ security is invaluable. As cloud computing grows and more business is moved digitally, security threats will only grow. Putting into place systematic identification of vulnerabilities will keep your organization ready and protected in the future.