A proactive approach to security

Preparing for attacks is an important job that the entire security team is responsible for.
Threat actors have many tools they can use depending on their target.
For example, attacking a small business can be different from attacking a public utility.
Each have different assets and specific defenses to keep them safe.
In all cases, anticipating attacks is the key to preparing for them.
In security, we do that by performing an activity known as threat modeling.
Threat modeling is a process of identifying assets, their vulnerabilities, and how each is exposed to threats.
We apply threat modeling to everything we protect. Entire systems, applications, or business processes all get examined from this security-related perspective.
Creating threat models is a lengthy and detailed activity.
They're normally performed by a collection of individuals with years of experience in the field.
Because of that, it's considered to be an advanced skill in security.
However, that doesn't mean you won't be involved.
There are several threat modeling frameworks used in the field.
Some are better suited for network security. Others are better for things like information security, or application development.
In general, there are six steps of a threat model.
The first is to define the scope of the model.
At this stage, the team determines what they're building by creating an inventory of assets and classifying them.
The second step is to identify threats.
Here, the team defines all potential threat actors.
A threat actor is any person or group who presents a security risk.
Threat actors are characterized as being internal or external.
For example, an internal threat actor could be an employee who intentionally expose an asset to harm.
An example of an external threat actor could be a malicious hacker, or a competing business.
After threat actors have been identified, the team puts together what's known as an attack tree.
An attack tree is a diagram that maps threats to assets.
The team tries to be as detailed as possible when constructing this diagram before moving on.
Step three of the threat modeling process is to characterize the environment.
Here, the team applies an attacker mindset to the business.
They consider how the customers and employees interact with the environment.
Other factors they consider are external partners and third party vendors.
At step four, their objective is to analyze threats.
Here, the team works together to examine existing protections and identify gaps.
They then rank threats according to their risk score that they assign.

During step five, the team decides how to mitigate risk.
At this point, the group creates their plan for defending against threats.
The choices here are to avoid risk, transfer it, reduce it, or accept it.
The sixth and final step is to evaluate findings.
At this stage, everything that was done during the exercise is documented, fixes are applied, and the team makes note of any successes they had.
They also record any lessons learned, so
they can inform how they approach future threat models.
That's an overview of the general threat modeling process.
What we've explored was just one of many methods that exist.

Revision #2
Created 27 August 2023 17:04:44 by naruzkurai
Updated 27 August 2023 18:32:26 by naruzkurai