Understand risks, threats, and vulnerabilities

When security events occur, you'll need to work in close coordination with others to address the problem. Doing so quickly requires clear communication between you and your team to get the job done.

Previously, you learned about three foundational security terms:

- **Risk**: Anything that can impact the confidentiality, integrity, or availability of an asset
- **Threat**: Any circumstance or event that can negatively impact assets
- **Vulnerability**: A weakness that can be exploited by a threat

These words tend to be used interchangeably in everyday life. But in security, they are used to describe very specific concepts when responding to and planning for security events. In this reading, you'll identify what each term represents and how they are related.

Security risk

Security plans are all about how an organization defines risk. However, this definition can vary widely by organization. As you may recall, a **risk** is anything that can impact the confidentiality, integrity, or availability of an asset. Since organizations have particular assets that they value, they tend to differ in how they interpret and approach risk.

One way to interpret risk is to consider the potential effects that negative events can have on a business. Another way to present this idea is with this calculation:

Likelihood x Impact = Risk

For example, you risk being late when you drive a car to work. This negative event is more likely to happen if you get a flat tire along the way. And the impact could be serious, like losing your job. All these factors influence how you approach commuting to work every day. The same is true for how businesses handle security risks.

In general, we calculate risk in this field to help:

- Prevent costly and disruptive events

- Identify improvements that can be made to systems and processes
- Determine which risks can be tolerated
- Prioritize the critical assets that require attention

The business impact of a negative event will always depend on the asset and the situation. Your primary focus as a security professional will be to focus on the likelihood side of the equation by dealing with certain factors that increase the odds of a problem.

Risk factors

As you'll discover throughout this course, there are two broad risk factors that you'll be concerned with in the field:

- Threats
- Vulnerabilities

The risk of an asset being harmed or damaged depends greatly on whether a threat takes advantage of vulnerabilities.

Let's apply this to the risk of being late to work. A threat would be a nail puncturing your tire, since tires are vulnerable to running over sharp objects. In terms of security planning, you would want to reduce the likelihood of this risk by driving on a clean road.

Categories of threat

Threats are circumstances or events that can negatively impact assets. There are many different types of threats. However, they are commonly categorized as two types: intentional and unintentional.

For example, an *intentional* threat might be a malicious hacker who gains access to sensitive information by targeting a misconfigured application. An *unintentional* threat might be an employee who holds the door open for an unknown person and grants them access to a restricted area. Either one can cause an event that must be responded to.

Categories of vulnerability

Vulnerabilities are weaknesses that can be exploited by threats. There's a wide range of vulnerabilities, but they can be grouped into two categories: technical and human.

For example, a *technical* vulnerability can be misconfigured software that might give an unauthorized person access to important data. A *human* vulnerability can be a forgetful employee who loses their access card in a parking lot. Either one can lead to risk.

Key takeaways

Risks, threats, and vulnerabilities have very specific meanings in security. Knowing the relationship between them can help you build a strong foundation as you grow essential skills and knowledge as a security analyst. This can help you gain credibility in the industry by demonstrating that you have working knowledge of the field. And it signals to your future colleagues that you’re a member of the global security community.

Revision #1
Created 17 July 2023 02:47:48 by naruzkurai
Updated 15 August 2023 18:44:09 by naruzkurai