It's important to

understand how to protect an organization's

data and assets because that will be part of your role as a security analyst. Fortunately, there

are principles and guidelines that can

be used, along with NIST frameworks and

the CIA triad, to help security teams

minimize threats and risks. In this video, we'll

explore some Open Web Application Security

Project, or OWASP,

security principles that are useful to know as an

entry-level analyst.

The first OWASP principle is to minimize the attack

surface area. An attack surface refers to all the potential

vulnerabilities that a threat actor

could exploit, like attack vectors,

which are pathways attackers use to penetrate

security defenses. Examples of common

attack vectors are phishing emails and

weak passwords. To minimize the attack surface and avoid incidents

from these types of vectors, security teams might

disable software features, restrict who can access

certain assets, or establish more complex

password requirements.

The principle of least privilege means making sure

that users have the least amount of access required to perform

their everyday tasks. The main reason for

limiting access to organizational

information and resources is to

reduce the amount of damage a security

breach could cause. For example, as an

entry-level analyst, you may have access to log data, but may not have access to

change user permissions. Therefore, if a threat actor compromises

your credentials, they'll only be able to gain limited access to digital

or physical assets, which may not be

enough for them to deploy their intended attack.

The next principle we'll discuss is defense in depth. Defense in depth means that

an organization should have multiple security controls that address risks and threats

in different ways. One example of a

security control is multi-factor

authentication, or MFA, which requires users to take an additional step beyond simply entering their username and password to gain access

to an application. Other controls

include firewalls, intrusion detection systems, and permission

settings that can be used to create multiple

points of defense, a threat actor must get through to breach an organization.

Another principle is separation of duties, which can be used to

prevent individuals from carrying out fraudulent

or illegal activities. This principle means that

no one should be given so many privileges that

they can misuse the system. For example, the person

in a company who signs the paychecks shouldn't also be the person who prepares them. Only two more principles to go! You're doing great.

Keep security simple is the next principle.

As the name suggests, when implementing security controls, unnecessarily complicated solutions should be avoided because they can become unmanageable. The more complex the security controls are, the harder it is for people to work collaboratively.

The last principle is to fix security issues correctly. Technology is a great tool, but can also present challenges. When a security incident occurs, security professionals are expected to identify the root cause quickly. From there, it's important to correct any identified vulnerabilities and conduct tests to ensure that repairs are successful. An example of an issue is a weak password to access an organization's wifi because it could lead to a breach. To fix this type of security issue, stricter password policies could be put in place.

I know we've covered a lot, but understanding these

principles increases your overall security knowledge and can help you stand out

as a security professional.

More about OWASP security principles

Previously, you learned that cybersecurity analysts help keep data safe and reduce risk for an organization by using a variety of security frameworks, controls, and security principles. In this reading, you will learn about more Open Web Application Security Project, recently renamed Open Worldwide Application Security Project® (OWASP), security principles and how entry-level analysts use them.

Security principles

In the workplace, security principles are embedded in your daily tasks. Whether you are analyzing logs, monitoring a security information and event management (SIEM) dashboard, or using a [vulnerability scanner](), you will use these principles in some way.

Previously, you were introduced to several OWASP security principles. These included:

- **Minimize attack surface area**: Attack surface refers to all the potential vulnerabilities a threat actor could exploit.
- **Principle of least privilege**: Users have the least amount of access required to perform their everyday tasks.
- **Defense in depth**: Organizations should have varying security controls that mitigate risks and threats.
- **Separation of duties**: Critical actions should rely on multiple people, each of whom follow the principle of least privilege.
- **Keep security simple**: Avoid unnecessarily complicated solutions. Complexity makes security difficult.
- **Fix security issues correctly**: When security incidents occur, identify the root cause, contain the impact, identify vulnerabilities, and conduct tests to ensure that remediation is successful.

Additional OWASP security principles

Next, you'll learn about four additional OWASP security principles that cybersecurity analysts and their teams use to keep organizational operations and people safe.

Establish secure defaults

This principle means that the optimal security state of an application is also its default state for users; it should take extra work to make the application insecure.

Fail securely

Fail securely means that when a control fails or stops, it should do so by defaulting to its most secure option. For example, when a firewall fails it should simply close all connections and block all new ones, rather than start accepting everything.

Don't trust services

Many organizations work with third-party partners. These outside partners often have different security policies than the organization does. And the organization shouldn't explicitly trust that their partners' systems are secure. For example, if a third-party vendor tracks reward points for airline customers, the airline should ensure that the balance is accurate before sharing that information with their customers.

Avoid security by obscurity

The security of key systems should not rely on keeping details hidden. Consider the following example from OWASP (2016):

The security of an application should not rely on keeping the source code secret. Its security should rely upon many other factors, including reasonable password policies, defense in depth, business transaction limits, solid network architecture, and fraud and audit controls.

Key takeaways

Cybersecurity professionals are constantly applying security principles to safeguard organizations and the people they serve. As an entry-level security analyst, you can use these security principles to promote safe development practices that reduce risks to companies and users alike.

Mark as completed
Like
Dislike