OWASP security principles

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.

Revision #1
Created 2023-06-06 00:17:29 UTC by naruzkurai
Updated 2023-06-06 00:17:58 UTC by naruzkurai