CJ McDonald

September 14, 2023

What is the CIA Triad? Definition, Explanation, Examples

This article informs the reader on the three principles of cybersecurity, confidentiality, integrity, and availability.

Introduction: The CIA Triad

CIA stands for confidentiality, integrity, and availability. The CIA triad is designed to guide policies for an organization's information security. They're the three most foundational needs for cybersecurity and are used to find vulnerabilities and methods for creating solutions

Confidentiality

The first principle of the triad is confidentiality. Confidentiality is essentially the steps taken to keep information private. The Chai article describes it as a measure "designed to prevent sensitive information from unauthorized access attempts" (Chai, 2022). The data tends to be categorized according to the damage that can be caused if something were to happen. Maintaining confidentiality ensures privacy and helps avoid ransomware attacks. An example would be two-factor authentication, which is "a system that requires two separate, distinct forms of identification in order to access something"(Kenton, 2022).

Integrity

The second principle of the triad is integrity. Integrity in this context, means information is trustworthy and not altered or modified by an unauthorized person. "Data must not be changed

in transit" (Chai, 2022). Integrity can be protected by setting up secure channels when sharing data. One example of integrity is an e-signature or a digital signature as it provides "effective nonrepudiation measures"(Chai, 2022).

Availability

Availability, the final principle, means information is consistently accessible when needed. This is crucial to daily operations as, without access, things cease to work properly. Availability involves "properly maintaining hardware and technical infrastructure and systems that hold and dispute the information" (Chai, 2022). The best examples of availability would be maintaining all hardware and software.

Differences Between Authentication & Authorization

Authentication is the process of verifying someone's identity, verifying they are who they claim to be. An example would be some form of biometric data, like a fingerprint or facial recognition.

Authorization is the process of granting someone permission to access a resource. Their ability to access that resource depends on that person's level of access and after all authentication steps are completed. Permission is usually granted by a person or an automated system. An example of authorization is a role-based access control system.

The difference between authentication and authorization is that "authentication checks the identity of a user, followed by authorization which authorizes what apps, files, or data can the who had previously authenticated have access to" (Andrioaie, 2022)

Conclusion

The three foundational principles of cybersecurity are confidentiality, integrity, and availability. The purpose of the triad is to help guide the development of policies for organizations and corporations. All three components are important to a business and without one of them, the information security of an organization would be at serious risk.