Understanding the CIA Triad, Authentication, and Authorization

Antoinette Elam

CYSE200T

Mr. Charles E. Kirkpatrick

9/15/2024

The three key concepts that inform information security policy are Confidentiality, Integrity, and Availability (CIA trinity). It protects systems from unwanted access while collaborating with authentication and authorization procedures to guarantee that sensitive data is accurate, safe, and accessible to authorized users.

The CIA triad is a concept intended to direct information security policy inside a company. CIA stands for confidentiality, integrity, and availability. It is sometimes referred to as AIC due to there being a well know CIA already.

Confidentiality

The C stands for confidentiality; this makes sure that only people with permission can access certain information. This prevents unauthorized access and guarantees the privacy of sensitive material.

Integrity

The I stand for integrity; this ensures that data is correct, complete, and unable to be changed by unauthorized parties. It is meant to keep data accurate and reliable for the course of its existence.

Availability

The A stands for authorized; this guarantees that any information and resources are available to authorized users when they need it. Systems must be operating properly to ensure that even in the event of a cyberattack or system failure that users can still be able to access what they need.

Authentication

When it comes to authentication and authorization, they are different but connected. Authentication is the process of confirming the identity of a user or system. That is accomplished through methods such as usernames, passwords, multifactor authentication and more. An example of this is when you're logging into your computer, cell phone, email, school account, or anything that is only to be accessed specifically by you to protect your information.

Authorization

Authorization is a method to determine what a user or system is allowed to do. Once the identity of a user or system has been verified, they are granted permissions and levels of access. This establishes when actions are acceptable. An example of this would be like using a computer a public library. After logging in you can access basic features such as the internet and word. However, you may not have access to administrative settings that may change how the PC functions. This is authorization, this ensures that you are only allowed to do what you are permitted to do.

The backbone for modern information security is comprised on the CIA triad as well as the authorization and authentication procedures. These principles are essential for sustaining safe, dependable systems in both personal and corporate contexts because they guarantee that data is accurate, secure, and available to the appropriate parties at the appropriate times.