Hannah Stivers

Professor Charlie Kirkpatrick

CYSE 200T 33861

January 25, 2023

The CIA Triad

The CIA Triad is an extremely important foundational principle of cybersecurity. The CIA Triad consists of confidentiality, integrity, and availability. It is important to know the difference between authorization and authentication when looking at the CIA Triad.

What is the CIA Triad?

The CIA triad is a foundation model designed to help guide policies for information security within an organization. This is done by breaking the policies into three sections: confidentiality, integrity, and availability. Confidentiality is what people are most familiar with, this regards the rules that make material or areas a specific security level. The more confidential the information is, the more it can hurt the organization and its customers if anything happened to it. Integrity deals with ensuring that the information within the system is trustworthy and accurate. This means that data is stored properly and only accessed by those with the authorization to do so. Availability is how reliable the system is. This means ensuring all systems are running properly and receive regular maintenance and updating, this is for hardware and software used.

What is Authentication?

Authentication verifies that a person is whom they say they are. The most common example of authorization is a person's username and password for an account. The purpose is to verify the individual and avoid fraudulent activity.

What is Authorization?

Authorization is the level of access a person is given. A common example of this is administrative users versus general users on a computer. The organization should not allow all employees access to the same data, authorization is used to separate this. Data with different levels of sensitivity will have different authorized personnel assigned.

Example of the difference between Authentication and Authorization

In an organization, authentication is used by individuals to log in to computers or get into specified areas; whereas authorization is what the organization permits this person to do. For example, authentication would be the person's username, password, key card, fingerprint, etc. that allows them access, but where they have access to is dependent on their level of authorization. Someone that is at an entry-level or intern level will not have access to as much sensitive data as someone from a more senior level, this is a difference in authorization access.

Conclusion

Confidentiality, integrity, and availability make up the fundamental principles of security in information systems. The triad relies on rules for access, accurate information, and reliable access for organizations to work properly and securely. Authentication verifies who a person is, and authorization determines what they can do.

Works Cited

Authentication vs. Authorization. (n.d.). Retrieved from onelogin : https://www.onelogin.com/learn/authentication-vs-authorization#:~:text=Authentication%20verifies%20the%20identity%20of,the%20security%20of%20a%20system.

Chai, W. (2022, June 28). *What is the CIA Triad? Definition, Explanation, Examples*. Retrieved from https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view