Carter Wood

CIA Triad Write-Up

This write-up will contain all of the 3 separate parts of the CIA triad and how they work and it also explain the differences between the terms Authorization and Authentication.

Confidentiality

The “C” in the CIA triad stands for Confidentiality. What they do is ensure that information is accessible only to authorized individuals or systems. This means that data is protected from unauthorized exposure, interception, or misuse. For example, encryption can mix up data, making it unreadable to those without the correct decryption key. There are certain limits to who can view or modify specific information, and physical security measures protect hardware and data storage devices from unauthorized access. With these measures at hand, organizations can protect their property which ranges from financial data to personal information and even other valuable assets.

Integrity

The “I” in the CIA triad stands for Integrity. What they do is ensure that data has not been modified, corrupted, or tampered with in any way. For example, different ways of validation can verify the integrity of data by detecting any changes that may have occurred during communications or storage. Data validation rules can ensure that data is consistent and accurate. By maintaining integrity, organizations can prevent errors, fraud, and data loss, making sure that information remains reliable and trustworthy.

Availability

The “A” in the CIA triad stands for Availability. What they do is make sure that information is accessible to authorized users whenever they need it. Availability also ensures that systems and data are operational and accessible without interruption. For example, redundancy can provide backup systems to ensure continuous operation in case of failures. Some organizations have plans that can help them recover from an incident and restore all of their data. By maintaining availability, organizations can ensure that critical business processes are not disrupted and that users can access the information they need when they need it.

Authorization vs. Authentication

There is a big difference between these two terms. Authorization is the practice of the ability of a user to access certain information such as passwords, files, applications, etc. Authentication is the practice of confirming that a user is who they really say they are. The article posted by SailPoint gives a very clear and concise explanation of the differences between these two terms. One simple example of authentication is entering a username or email and then following it with a password to login to an online portal or application. One example of authorization is if someone owns a Google Doc worksheet that is shared with others, the owner can give certain permissions to the users that have access to it such as viewers, editors, or commenters.

Conclusion

The CIA triad is built of 3 different parts; Confidentiality, Integrity, and Availability. Confidentiality is the practice of letting only authorized users access certain information. Integrity is the practice of making sure that data has not been modified without the permission of the owner. Availability is the practice of letting users access whenever the owner needs it. There is a difference between authorization and authentication; authorization is the practice of letting a

user access certain types of information while authentication is the practice of making sure you are who you say you are.