

Xavier Lesane

09/19/2021

What is the CIA triad?

Much like the three branches of government, the world of cybersecurity is governed by what we call the CIA triad. The CIA triad consists of Confidentiality, Integrity, and Availability. Confidentiality involves who can access a system's data. Methods such as two-factor authentication, biometric fingerprints, or physical key cards help secure the confidentiality portion of the triad and ensure not just anyone can access company information. Integrity is all about who can modify a system's data. Though confidentiality stops someone from accessing information, it does not protect against those who may have access but also may have ill intent or accidentally stumble upon restricted information. Integrity means making sure someone without the right roles or privileges knows certain information even exists. Examples of integrity include requiring access before modifying a document or setting permissions that hides content from all except certain users such as administrators or moderators. The final component of the CIA triad, Availability, makes sure data is always available when an authorized person wants/needs to access it. With the threat of DoS attacks constantly present we must make sure there is a way to keep the data accessible. Availability involves preventing and recovering from malicious events. Examples of availability include keeping anti-virus, anti-malware, firewalls, etc up to date and keeping back-ups of data whether physical or digital readily accessible when needed.

Authentication vs Authorization

In the Confidentiality aspect of the CIA triad, there are the terms authentication and authorization. Authentication is simply verifying you are who you say you are. If an employee wants to access data they must first verify they are an employee, doing this may involve entering a username or password given by a company or inserting a keycard/id when accessing a building. This ensures the person is who they claim to be. Authorization involves making sure a person can only see the data their position allows them to see. This sounds a lot like the work of the integrity aspect because it is. Authorization can give permission to see, edit, or delete a document and can also be used to take away someone's said permissions. These two aspects work in tandem to secure the confidentiality of a person or company's data.

References

Authentication vs. authorization. Okta. (n.d.). Retrieved September 21, 2021, from <https://www.okta.com/identity-101/authentication-vs-authorization/#:~:text=What's%20the%20difference%20between%20authentication,permission%20to%20access%20a%20resource>.

Fruhlinger, J. (2020, February 10). *The CIA Triad: DEFINITION, components and examples*. CSO Online. Retrieved September 21, 2021, from <https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html>.