Isaiah W. Simmons

2/1/2025

The CIA Triad

Description of the CIA Triad

The CIA Triad is a foundational model in the field of information security, encompassing three core principles: Confidentiality, Integrity, and Availability. Each component plays a crucial role in safeguarding data from unauthorized access, ensuring its accuracy, and guaranteeing that it remains accessible to authorized users when needed. Confidentiality refers to the protection of sensitive information from unauthorized disclosure. This is typically achieved through encryption and access controls that restrict data visibility to only those who are permitted to view it. Integrity involves maintaining the accuracy and consistency of data over its lifecycle; this means implementing measures to prevent unauthorized modifications that could compromise its reliability. Finally, Availability ensures that authorized users have timely access to information and resources whenever necessary. This can involve redundancy measures like backups and failover systems designed to maintain operations during disruptive events.

Difference between Authentication & Authorization

Authentication and authorization are two distinct yet interconnected processes within the realm of cybersecurity. Authentication is the process of verifying the identity of a user or device. It answers the question, “Who are you?” This can be achieved through various methods, including passwords or biometrics (fingerprints or facial recognition). Authentication ensures that the person attempting to access a system is indeed who they claim to be. It also serves as the first line of defense in verifying a user's identity before granting them access to systems or data. Common methods of authentication include traditional username/password combinations, biometric verification such as fingerprints or facial recognition technologies, and multi-factor authentication which requires multiple forms of verification for enhanced security. For example, when an employee logs into their company’s system using a password along with a one-time code sent to their mobile device, they are undergoing an authentication process

designed to confirm their identity. Authorization, on the other hand, takes place after authentication. It determines the permissions and access levels granted to an authenticated user. Authorization answers the question, “What can you do?” It involves policies and roles that dictate what resources or data a user is permitted to access, ensuring that sensitive information is protected from unauthorized misuse.

Conclusion

Understanding the difference between authentication and authorization is essential for establishing secure systems that enforce both proper identity verification and appropriate access control. In summary, CIA Triad principles ensure holistic security, while the distinction between authentication and authorization provides clarity in access management.

Citations

Fasulo, P., (2024). *What is the CIA Triad? Definition, Importance, & Examples.* Retrieved from https://securityscorecard.com/blog/what-is-the-cia-triad.

Hashemi-Pour, C., (2024). *What is the CIA triad (confidentiality, integrity and availability)?.* Retrieved from https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA.

Chai, W. (2018). *Authentication as CIA triad - Information Security Stack Exchange.* Retrieved from https://security.stackexchange.com/questions/177853/authentication-as-cia-triad.