Skylar Proctor

14 February 2025

Cyse 200t

Understanding the CIA Triad and the Differences Between Authentication & Authorization

BLUF

The CIA Triad stands for Confidentiality, Integrity, and Availability and it is a foundational cybersecurity framework that ensures data protection. Additionally, authentication and authorization serve distinct roles in securing systems.

Introduction

Cybersecurity is a critical aspect of modern technology, safeguarding sensitive data from breaches, unauthorized access, and cyber threats. The CIA Triad establishes the principles necessary for data protection. Additionally, authentication and authorization are essential mechanisms that regulate access to systems and data. By understanding these concepts, organizations can better defend against cyber threats and ensure that their information is secure.

The CIA Triad

The CIA Triad is a widely accepted model that underpins cybersecurity strategies. It consists of three principles, Confidentiality which protects sensitive data from unauthorized access, we see this in Encryption, strong passwords, and multi-factor authentication (MFA). Integrity ensures that information remains accurate and unaltered unless modified by an authorized entity. Integrity is maintained through cryptographic hashing, digital signatures, and version control systems to prevent unauthorized changes. Availability ensures that systems and data are accessible when needed is critical for business operations and user experience. Availability is supported by redundancy, failover systems, and protection against cyber threats. These three principles work together to create a strong cybersecurity framework, helping organizations manage risks and protect their information assets.

Authentication vs. Authorization

Authentication and authorization serve distinct functions in cybersecurity. Authentication is the process of verifying a user's identity. It answers the question, *“Who are you?”* Authentication methods include usernames and passwords, biometrics (such as fingerprints or facial

recognition). Authorization, on the other hand, determines what an authenticated user is allowed to do within a system. It answers the question, *"What are you allowed to access?"* Authorization is enforced through access control policies, which grants permissions based on a user's role.

Example

A real-world example of authentication and authorization can be seen in online banking. When a user logs into their bank account, they provide a username, password, and sometimes an additional authentication factor, verifying their identity. Once logged in, the user can access account balances and transaction history but cannot modify the bank's internal financial records. Only employees with the necessary authorization can perform administrative tasks.

Conclusion

The CIA Triad establishes the core principles of cybersecurity, ensuring that data remains protected, accurate, and accessible. Authentication and authorization perform distinct roles in securing information systems. Authentication verifies a user's identity, while authorization defines their access level. Understanding and implementing these principles are essential for organizations to safeguard their systems from cyber threats and unauthorized access.