Name: Huong Quach

Date: 06/01/25

The CIA Triad

BLUF

A fundamental component of information security is the CIA Triad: Availability, Integrity, and Confidentiality. Furthermore, establishing safe access controls in systems requires an awareness of the distinctions between authorization and authentication.

Components of the CIA Triad

Confidentiality, integrity, and availability are the three guiding principles of the CIA Triad, a foundational model in cybersecurity (Riley, 2024). Organizations use these elements as the cornerstone for creating and implementing security policies. Preventing unwanted access to private information is known as confidentiality. Techniques including two-factor authentication (2FA), biometric verification, access control lists, and data encryption are frequently employed to guarantee that only authorized personnel can view or interact with sensitive information (kaspersky, 2020). Keeping information accurate and reliable throughout its existence is the core goal of integrity. This involves making sure that data stays consistent and stopping unwanted modifications. Checksums, digital signatures, version control, and frequent backups are examples of common methods. Availability guarantees that authorized users can access data and services when they're needed. This is accomplished by the use of failover procedures, system

redundancy, routine maintenance, and defense against dangers including hardware malfunctions and denial-of-service (DoS) assaults (Palo Alto Networks, 2019).

The Difference between Authentication & Authorization

Understanding the CIA Triad is crucial, as is knowing the difference between authorization and authentication, two concepts that are sometimes used synonymously but have different meanings in cybersecurity (OneLogin, n.d.). The process of confirming a user's identification is called authentication. Security tokens, biometric information like fingerprints or facial recognition, and usernames and passwords are frequently used for this (What Is a Security Token?, n.d.). The resources or actions that a verified user is permitted to access or carry out within a system, however, are determined by authorization. For instance, users authenticate by providing their credentials when they connect into an online banking program. After authentication, the system verifies the user's permissions to examine their account balance, initiate a transfer, or access financial records, among other things. Depending on their roles or security levels, numerous users may have different rights even if they successfully authenticate.

Conclusion

To sum up, the CIA Triad provides a strong foundation for comprehending the three major objectives of cybersecurity: preserving data integrity, protecting data confidentiality, and guaranteeing service availability. At the same time, establishing appropriate access control requires understanding the difference between authorization and authentication. Authorization establishes what a user is allowed to do, whereas authentication confirms who they are. Together, these ideas assist the larger goal of information security by protecting systems and data against threats.

References

Kaspersky. (2020). What Is Biometrics? How Is It Used in security? Kaspersky.com. https://www.kaspersky.com/resource-center/definitions/biometrics

OneLogin. (n.d.). Authentication vs. authorization. OneLogin. https://www.onelogin.com/learn/authentication-vs-authorization

Palo Alto Networks. (2019). What is a denial of service attack (DoS) ? - Palo Alto Networks. Paloaltonetworks.com. https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos

Riley, S. (2024, August 12). Council Post: Reprioritizing The Confidentiality, Integrity And Availability (C.I.A.) Security Triad. Forbes. https://www.forbes.com/councils/forbestechcouncil/2023/04/06/reprioritizing-the-confidentiality-integrity-and-availability-cia-security-triad/

What is a security token? (n.d.). SearchSecurity. https://www.techtarget.com/searchsecurity/definition/security-token