Adeline Harris

Write-Up: The CIA Triad

THE CIA TRIAD

1. Confidentiality
2. Integrity
3. Availability

Refers to the three core principles of cybersecurity that helps organizations protect their information assets by ensuring data confidentiality, integrity, and availability for authorized individuals. It is a key component of ISO 27001, a global standard for information security management (Irwin, 2023)

CONFIDENTIALITY

Is a crucial aspect of information security that ensures sensitive data remains protected from unathorized users disclosure. Organizations implement various measures to safeguard information, preventing it from falling into wrong hands. Methods used to ensure confidentiality include data Encryption, identity proofing, and two-factor authentication. For example a healthcare organization that stores a patient's medical record containing sensitive information such as medical history, diagnosis and treatment. To maintain confidentiality, they implement strict access controls, encryption and regular audit. Only authorized healthcare professionals can access these records, maintaining patient trust by keeping their information private and secure.

INTEGRITY

Integrity in information security ensures data is accurate, consistent, and trustworthy to prevent unauthorized changes. Data modification may occur accidentally due to system malfunction or data entry errors, and intentionally through malicious actions like malware attacks. Maintaining data integrity builds user trust, and organizations employ measures such as checksums, hash function, encryption and access controls to protect and confirm data integrity. In a university database that stores student grades. To maintain data accuracy, the system uses checksums or hash functions to create unique values from the grades and related details. When a professor enters grades, the system computes a checksum for that data. If someone attempts to change a student's grades, the checksum for that record will change. The system, with the integrity checks, will identify the inconsistency and issue a warning. This prevents unauthorized changes to student grades, preserving the reliability of academic records. (*What Is the CIA Triad and Why Is It Important?*, n.d.) (Lodhia, n.d.)

AVAILABILITY

Refers to the accessibility and usability of data or resources when and where needed by authorized users. It ensures information and services are consistently available and reliable. Availability is significant in an organizations to maintain seamless operations and meet customer expectations. Downtime can lead to bad experiences and customer loss while continuous access to the IT system allows employee efficiency. Ensuring availability gives organizations a competitive edge by providing reliable services. It can be intentionally compromised by DDoS attacks, where networks are flooded with traffic to overwhelm and disrupt services. And unintentionally if natural disasters like floods occur physically damage infrastructure, leading to service interruptions. To address these organizations implement measures like backup systems, data recovery plans and redundancy to maintain smooth operation and meet customers expectations. (*What Is the CIA Triad and Why Is It Important?*, n.d.)

Difference between Authentication & Authorization

Authentication verifies the identity of users or devices attempting to access resources. This process involves verifying credentials like biometrics, password or multi-factor authentication methods. It is accomplished when a user inputs the correct credentials stored in the system, which verify identity and enable access.

On the other hand, authorization occurs after authentication. After the user's identity has been confirmed, authorization decides what resources can be accessed. This step is essential for defining what users are permitted to do in the system. For example in the banking environment, authorization is important for ensuring secure access to sensitive information and operations. In online transactions, users need to verify their identity by providing their usernames,passwords, and extra security steps like two-factor authentication. Account holders and bank staff have different levels of permission. Account holders need authorization to check balance, transfer funds and pay bills. While bank staff have broader authorization to process significant transactions or manage accounts.

(*3 Types of Authentication Methods*, n.d.) (*Authentication Vs. Authorization - Authentication Vs. Authorization*, 2023)

References

Authentication vs. Authorization - Authentication vs. Authorization. (2023, February 14). Okta. Retrieved February 5, 2024, from https://www.okta.com/identity-101/authentication-vs-authorization/

Irwin, L. (2023, February 14). *What Is the CIA Triad and Why Is It Important?* IT Governance. Retrieved February 2, 2024, from https://www.itgovernance.co.uk/blog/what-is-the-cia-triad-and-why-is-it-important

Lodhia, R. (n.d.). *Checksum to Ensure Data Integrity*. Eagle Eye Networks. Retrieved February 3, 2024, from https://www.een.com/blog/checksum-ensure-data-integrity/

3 Types of Authentication Methods. (n.d.). Optimal IdM. Retrieved February 4, 2024, from https://optimalidm.com/resources/blog/types-of-authentication-methods/

What is the CIA Triad and Why is it important? (n.d.). Fortinet. Retrieved February 3, 2024, from https://www.fortinet.com/resources/cyberglossary/cia-triad