CIA Tirad

Stephen Saintcyr

Old Dominion University

Mr. Kirkpatrick

CYSE-200

1/29/2025

CIA Tirad

CIA Triad and the Differences Between Authentication & Authorization

The main concern for modern digital systems is cybersecurity. Information security is based on the CIA Triad, which includes Confidentiality, Integrity, and Availability. Each ensures that data is protected against unauthorized access, tampering, and disruptions. Understanding the difference between authentication and authorization will also be essential to secure systems and manage access controls effectively.

The CIA Triad

Confidentiality

Confidentiality means that information of concern is only available to those with authority. Cybersecurity involves encryption access control mechanisms and authentication methods to prevent unauthorized users from accessing protected data (Chai, 2022). Many organizations classify data based on sensitivity and apply measures to let the right people in, such as multi-factor authentication, role-based access control, and data masking.

Example

All online banking systems require customers to log in using passwords. They also incorporate a two-factor authentication procedure after customers try to access account details.

Integrity

Integrity ensures that data remains valid and trustworthy throughout its lifecycle; this prevents unauthorized or malicious changes and unintentional changes such as human error or system failure. Some ways to ensure data integrity are cryptographic hash functions, checksums, and digital signatures. Organizations also employ audit logs and other forms of access control to track and regulate changes.

Example:

Digital signatures verify the authenticity and tampering of e-mails and documents. An unmatched signature indicates that something with the file may have changed.

Availability

The system is accessible to users when required, and data and systems are accessible to authorized users. Organizations ensure redundancy, failover systems, and regular hardware and software maintenance to achieve availability (Chai, 2022). Firewalls, disaster recovery plans, and DoS attack prevention are part of the security measures taken to maintain availability.

Example:

Therefore, redundancy and backups are applied using cloud storage service systems like Google Drive so users can still get their files during the downtime of one of their servers.

Authentication vs. Authorization

While the CIA Triad concerns data protection, system access management is equally important. Authentication and authorization are related yet different concepts in security. Authentication is verifying users to give them access to a particular system. More precisely, it indicates "Who are you?" and is generally done with username and password pairs, biometric scans, and authentication apps.

Authorization defines what an authenticated user is allowed to do within the system. Authorization is straightforward: "What are you allowed to do?" The permissions one is granted provide a level of access upon successful authentication.

Example:

Similarly, a university online portal uses login credentials for authentication. However, regarding authorization, although all students may have permission to view course materials, the instructor can only edit and upload assignments.

Conclusion

The CIA Triad is the backbone of cybersecurity, where data should be kept confidential, accurate, and available. Authentication and authorization go hand in glove to regulate access so unauthorized users cannot manipulate systems. Strong security measures will help organizations protect sensitive information and maintain system integrity.

Reference

Chai, W. (2022, June 28). *What is the CIA triad? Definition, explanation, examples*. TechTarget. Retrieved from https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA