The CIA Triad

Name: Caitlene Baer

BLUF

The three pillars of cybersecurity are confidentiality, integrity, and availability, which form the essential elements of cyber defense. Organizations must implement both the CIA Triad framework and authentication and authorization measures because these components ensure protected sensitive data and maintain organization-wide security stability.

Introduction

Organizations use the fundamental CIA Triad model for guidance in developing their information security policies by merging confidentiality, integrity, and availability elements. CIA Triad serves as another term for the AIC Triad, which exists to distinguish between the security needs and the intelligence agency known as the Central Intelligence Agency. (NIST, 2024)

In this context:

- Confidentiality restricts access to sensitive information.
- Integrity ensures data is accurate and unaltered.
- Availability guarantees reliable access to authorized users.

The CIA Triad stands as a fundamental cybersecurity principle, but experts recommend redesigning it because changing threats make it less effective. The authentication process, which confirms identity, works hand in hand with authorization for robust cybersecurity because they manage user access permissions. (TechTarget, 2013)

The CIA Triad

The CIA Triad is essential for maintaining secure, accurate, and accessible data (NIST, 2021). It comprises three core elements:

Confidentiality

- Purpose: Prevents unauthorized access to sensitive information.
- Techniques: Encryption, access controls, and secure communication protocols (NIST, 2024).

Integrity

- Purpose: Ensures data remains accurate and unaltered.
- Techniques: Checksums, cryptographic hashing, and version control.
- Additional Measures:
    - File permissions and access controls prevent unauthorized modifications.
    - Version control systems protect against accidental deletions.
    - Detection mechanisms identify changes from non-human events like electromagnetic pulses (EMPs) or server crashes.
    - Cryptographic checksums verify data integrity.
    - Backups and redundancies Restore data to its correct state after corruption or loss.
    - Digital signatures provide nonrepudiation, ensuring actions like logins and messages cannot be denied.

Availability

- Purpose: Ensures authorized users can access information when needed.
- Techniques: Redundancy, failover mechanisms, and disaster recovery plans (NIST, 2021).

Why is the CIA Triad Important?

Information security exists at its core with the three principal concepts presented through the CIA Triad. Secure data protection develops when organizations implement security policies through proper steps to handle both confidentialities along with integrity and availability.

The examination of these principles through the triad model enables businesses to ask specific questions about value provision within their essential areas. The holistic strategy provides security direction by ensuring objective achievement and risk management before determining product and technological decisions. (TechTarget, 2013)

Authentication vs. Authorization

While authentication and authorization are both vital to cybersecurity, they serve different roles:

Authentication

- Definition: Verifies a user's identity before granting access.
- Methods: Passwords, biometrics, multi-factor authentication (MFA), and security tokens (NIST, 2021).

Authorization

- Definition: Determines the level of access a user has after authentication.
- Methods: Permissions based on roles, security policies, or access control lists (NIST, 2024).

Example

The online banking account requires users to enter their password for authentication purposes. Once the system has authenticated the input, it enables the account holder to perform only transfer operations on the funds. (NIST, 2021)

Multi-factor authentication (MFA) with fingerprint matching and one-time passcodes could be implemented in this case. The joint account holders receive different permission settings within their account that are limited to specific user authorization.

When suspicious activity occurs, such as an unknown device login, the system should adapt by restricting access to protect the confidentiality and integrity of database data. The system demonstrates how users can achieve authentication in conjunction with authorization for safeguarding sensitive information. (NIST, 2024)

Conclusion

Cybersecurity entails the CIA triad: confidentiality, integrity, and availability. Information security protection for sensitive data combined with accuracy assurance and user reliability access relies on the Triad framework as a complete framework. (NIST, 2024)

The authentication and authorization elements work alongside Triad to validate system users while controlling access permissions, thus creating another security measure against unauthorized activities. The combined forces of these security components enhance the resistant power of information systems that protect against developing security threats.

To obtain complete data protection, organizations need to deploy essential security measures that follow the CIA Triad principles. The CIA Triad serves three functions in security policy development while assisting technology choices and validating compliance requirements for a particular industry.

CIA Triad provides guidance to organizational security objectives and goals, which organizations employ for risk evaluation purposes of new products and technologies.

The complexity of CIA Triad practices increases as organizations continuously improve their practices and security strategies through the evolution of ACTS. Security systems with resilience to maintain operational protection can be built by organization members who master CIA Triad principles.

References

- National Institute of Standards and Technology (NIST). (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST CSWP 29
- National Institute of Standards and Technology (NIST). (2021). *Digital identity guidelines*. NIST SP 800-63-3
- Hashemi-Pour, C., & Chai, W. (2023, December 21). *What is the CIA triad (confidentiality, integrity, and availability)?* TechTarget