Brendan Marcelo

CYSE200

Describing the CIA Triad and Dissecting Authentication vs Authorization with Real World Examples

Introduction:

The CIA triad is an underlying concept in information technology and cybersecurity that consists of three core principles: Confidentiality, Integrity, and Availability. Confidentiality dates to 1976 in a U.S. air force study. Integrity was first seen in 1987 in a paper that recognized that commercial computing had specific needs around accounting records that needed a focus on data accuracy. Availability was first seen in 1988 when the Morris worm shut down a significant portion of the embryonic internet. The CIA triad established a foundational concept in 1998. When all concepts are met, the security profile of an organization is much stronger and fully equipped to handle threat incidents.

Confidentiality:

Confidentiality involves limiting access to information to authorized users only and ensuring data privacy. Information must be controlled to prevent the unauthorized sharing of data. Examples of this principle include authentication processes such as biometrics or cryptographic keys. Authorization is utilized to determine who has the access to specific data. For example, some specific files are only accessible by their creators or admins of that organization. In business, it is used to control financial spreadsheets, bank accounts,

and sensitive information related to an organization's finances. On the contrary, a loss of confidentiality is seen in big data breaches.

Integrity:

Integrity is maintaining the consistency, accuracy, and correctness of data throughout its life cycle, preventing unauthorized changes. Data must not be changed in transit and integrity sets the standard for ensuring the data cannot be altered by unauthorized people. IP or internet protocol uses a checksum to detect errors in the header of packets during network transmission. Cryptographic checksums are hash functions designed to provide a high level of security against accidental and intentional errors. Another way to ensure integrity is to use backup and recovery software. In business, integrity is seen as making sure your purchases are reflected in your account and allowing you to contact a representative if there are any issues.

Availability:

Availability ensures that information is consistently and readily accessible for authorized parties. This plays a factor in keeping systems, networks, and drives up to date with the latest software and antivirus protections. Fast and adaptive recovery within an organizations technical infrastructure is essential in this concept. The use of extra security equipment such as firewalls and proxy servers are also an example of availability.

Authentication and Authorization:

Authentication is a process that verifies that someone or something is who they say they are. It is essential in securing access to an application or its data. Examples of this are seen in establishing a username and password. There are a few different types of authentications such as passwords and security questions, USB security tokens, one time pin, and biometric authentication. Authorization is the process that determines user or services level of access. It gives users or services the permission to access certain data or perform a particular action. An access control list is used in authorization to determine which users or services can access a particular digital environment.

Authentication vs Authorization:

Although authentication and authorization may seem similar, each play a different role in securing systems and data. Authentication verifies identity, ensuring users are who they say they are, while authorization determines the level of access granted to authenticated users also specifying the data or actions accessible.

Conclusion:

The CIA triad stands as a foundation in cybersecurity and information technology, originating in significant moments in history and evolving into a practical concept by 1998. The trio of principles collectively strengthen the security profile of organizations. Confidentiality is exemplified by meticulous access control measures, while the loss of this principle is visible in the result of data breaches. Integrity is maintaining the correctness of data. It is ensured through checksums and backup systems, vital for business transactions. Availability, ensuring consistent access, demands a strong technical

infrastructure, illustrated by security equipment such as firewalls. Authentication and authorization collectively are the gatekeepers of success. While authentication validates user identity, authorization meticulously delineates access levels, providing a layered defense. Recognizing these differences and embracing these principles collectively prepares organizations with a formidable shield against threats.

WORKS CITED:

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

Fruhlinger, J. (2020, February 10). *The CIA triad: Definition, components and examples*. CSO Online. https://www.csoonline.com/article/568917/the-cia-triad-definition-components-and-examples.html

GeeksForGeeks. (2019, June 6). *Difference between Authentication and Authorization - GeeksforGeeks*. GeeksforGeeks. https://www.geeksforgeeks.org/difference-between-authentication-and-authorization/

Fasulo, P. (2021, September 1). *What is the CIA Triad? Definition, Importance, & Examples*. SecurityScorecard. https://securityscorecard.com/blog/what-is-the-cia-triad/

What is the CIA Triad_ Definition, Explanation, Examples - TechTarget.pdf. (n.d.). Google Docs. https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view