Justin Lassalle

CYSE200T

Feb 03, 2024

The Principles of CIA Triad

The text under consideration discusses the CIA Triad, which is a set of three fundamental principles that are critical to ensuring the security of data. These principles are Confidentiality, Integrity, and Availability.

Confidentiality refers to the principle that only authorized personnel should have access to specific documents, files, or data. To implement this principle, clearance or authorization is provided to authorized personnel. For example, banks use confidentiality by assigning a unique account number to each customer. In this way, only the authorized person can access their account. However, confidentiality can be threatened by various factors such as weak passwords, man-in-the-middle attacks, electronic eavesdropping, etc. To ensure confidentiality, companies can use various security measures such as encryption, access control, and data loss prevention.

Integrity is another essential principle of the CIA Triad. It refers to maintaining the trustworthiness of data by ensuring that it is in the correct state and is immune to any improper modifications. This principle ensures that the data remains accurate, consistent, and reliable. It involves protecting data during transmission, such as sending emails, uploading documents, or downloading files. Integrity can be threatened by various factors,

such as changing system logs, modifying configuration files, or human errors. Various security measures, such as data validation, checksums, and file permissions, can be used to maintain data integrity.

Availability is the third principle of the CIA Triad. It refers to the principle that authorized personnel should be able to access data whenever required. This means that authorized users can access files, data, and applications whenever needed. However, availability can be threatened by various factors such as hardware failure, power failure, or human error. To ensure availability, companies can use various security measures such as redundancy, load balancing, and fault tolerance.

Authorization and authentication are two different concepts that are essential to ensure the security of data. Authentication is used to gain access to an account, file, data, or documents. It confirms the identity of the user. Authorization is used to verify that the person accessing the data is authorized to do so. For example, when someone goes to pick up a prescription, the pharmacy checks their files to make sure they are authorized to do so. They then ask for identification to verify their identity, which confirms that they are the authorized person to pick up the prescription.

In conclusion, the CIA Triad is a critical aspect of data security for businesses and organizations. Every company should have a well-defined security program that adheres to these principles. To ensure the security of data, companies can use various security measures such as encryption, access control, data loss prevention, data validation, checksums, file permissions, redundancy, load balancing, and fault tolerance. By

following the CIA Triad, businesses can ensure that their data is secure and protected both now and in the future.

Works Cited:

What is The CIA Triad? - Definition and Examples - Technology & IT Blog - siteskills

Authentication vs. Authorization: What's the Difference? (twilio.com)