Myrna E. Santiago

09/17/2023

CYSE 200T_17570

THE CIA TRIAD

The CIA triad is an information security model use by organizations to protect information. It provides a simple and complete check list for evaluating an organization security (Coursera, 2023). Authorization and Authentication are first line of defense to maintain CIA triad structure. This write-up addresses the CIA triad and their line of defense.

What is the CIA Triad?

The CIA triad refers to the concepts of Confidentiality, Integrity and Availability of information security.

- **Confidentiality** keeps information in an organization private. Examples are:

    - Medical records

    - Employee records

    - Financial assets

    - Intellectual Property, like copyrights and patents

    - Forms of inside communications

- **Integrity** maintains consistency, accuracy and trustworthiness of the data (Chai, 2022). Examples are:
    - Data from a purchase you made, matches your bank account statement
    - Changes made to a database is authorized and the same across all the database.
- **Availability** allows authorized users to access data from different devices and places.
    - You are able to access your bank account day or night, from a desktop, laptop or smart phone.
    - Employees can access their personal information on the secure part of their company website to update it, check available time off or 401k information.

The CIA triad has added tools thru time to adapt to new technologies and focus on the new market. Examples of tools used to maintain confidential information is the use of encryption and access control lists. Tools used for integrity are education of the user, as well as, backups and recovery software. Lastly, keeping system and applications up-to-date, as well as, backups, help availability of data at all times (ideally).

Differences between Authentication and Authorization

Authentication is the verification of someone's identity (SailPoint, 2023). Common authentication methods are:

- *What you know:* most common is the use of username and password

- *What you possess:* like a digital id card or a mobile phone to receive an alpha numerical code

- *What you are:* fingerprint or facial recognition

Authorization determines what areas or data a user can access. Two common techniques are:

- *Role-based access controls (RBAC):* which gives permission depending on the role the user has in the organization

- *Attribute-based access control (ABAC):* which gives permission depending on attributes, like user attributes (level of clearance), environment attributes (location of the data), or resource attributes (level of data sensitivity).

Conclusion

      The CIA triad provides a baseline that organizations can follow to secure and facilitate access of data. By using some of the tools mention before, as well as, asking the user to follow protocols, data can be protected and maintain for long periods of time. Today organizations need to keep up-to-date on technology and informed of the proper guidelines and laws to protect their assets and future.

References

1. Coursera. (2023, July 20). *What is the CIA triad?* Retrieved September 17, 2023,

   from https://www.coursera.org/articles/cia-triad

2. Chai, W. (2022, June 28). *What is the CIA Triad? Definition, Explanation,*

   Examples.

   https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8

   l/view

3. SailPoint. (2023, March 3). *What is the difference between authentication and*

   authorization? Retrieved September 17, 2023, from

   https://www.sailpoint.com/identity-library/difference-between-

   authentication-and-authorization/