Name: Hans Peterson

Date: 1/28/2024

The CIA Triad

The CIA (Confidentiality, Integrity, Availability) Triad is a guiding model used to keep information secure and available. Authentication verifies a user's identity, while authorization checks a user's permissions.

Confidentiality

Confidentiality means that information is protected from unauthorized users. Chai states that "confidentiality measures are designed to prevent sensitive information from unauthorized access attempts" (2022). For example, passwords prevent unauthorized people from accessing accounts. On a physical level, a gate or a locked door will prevent outsiders from entering restricted areas. If an intruder accesses unauthorized information, they have breached confidentiality.

Integrity

Integrity means that data is unaltered; if a person is authorized to alter data, then there is still integrity. It is about "maintaining the consistency, accuracy and trustworthiness of data over its entire lifecycle" (Chai, 2022). All other changes are breaches of integrity. Server crashes and EMPs can alter data, which is considered a breach. To maintain integrity, checksums, backups, and system redundancies are implemented. If unauthorized users alter backup drives or data, then integrity has been compromised.

Availability

Availability means information is accessible to authorized users. This is maintained through the implementation of RAID, clusters, and the maintenance of all hardware to ensure the proper functioning of systems. Disaster recovery plans and contingent plans can re-establish availability in the event of natural disasters and other destructive events. Like integrity, backups are used. If unauthorized users cannot readily access information, then data has been breached.

Authentication

Authentication is about validating a user's identity before giving them access to a system. This occurs before authorization. The user is commonly "identified with username, password, face recognition, retina scan, fingerprints, etc," (GeeksforGeeks, 2023). Many organizations use MFA (multi-factor authentication), which uses a combination of checks. SSOs (Single-Sign Ons) are also common authentication forms. These systems prevent impersonators from gaining access.

Authorization

Authorization is about giving privileges to users after authenticating them. They have only the privileges that they need. A few authorization techniques are Role-Based Access Controls (RBAC), SAML Authentication, and OAuth 2.0 Authorization (GeeksforGeeks, 2023). An example of a breach of authorization is giving a non-admin user administration rights or access.

Conclusion

The CIA triad is composed of three elements that guide policies on keeping information secure and available. Confidentiality is about restricting unauthorized users from accessing data.

Integrity is about ensuring data is unaltered. Availability is about ensuring information is readily available to authorized users. Authentication and authorization have differences. Authentication is about verifying a user's identity, and authorization is about checking a user's permissions.

References

Chai, W. (2022, June 28). *CIA triad (confidentiality, integrity and availability)*. WhatIs.

https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?jr=on

GeeksforGeeks. (2023, February 22). *Difference between Authentication and Authorization*.

https://www.geeksforgeeks.org/difference-between-authentication-and-authorization/