The CIA Triad

The CIA triad, also known as confidentiality, integrity, and availability, is a concept created to direct information security policies inside a company. This is one of the fundamental instruments used in the information security world.

Confidentiality

Confidentiality is the first letter in the CIA triad. “It is roughly referred as privacy” (Chai). Measures for maintaining confidentiality are intended to guard against unauthorized access to sensitive data. Data is frequently categorized based on the scope and nature of the harm that could result from it getting into the wrong hands (Chai). These categories can then be used to implement more or less strict measures.

Sometimes safeguarding data confidentiality involves special training for those privy to sensitive documents. Training can help familiarize authorized people with risk factors and how to guard against them (Chai). Further aspects of training may include strong passwords and password-related best practices and information about social engineering methods to prevent users from bending data-handling rules with good intentions and potentially disastrous results (Chai).

Integrity

Integrity is the upkeep of data throughout its full lifecycle in terms of consistency, accuracy, and dependability (Chai). Data cannot be changed while in transit, and measures must be taken to prevent unauthorized parties from changing the data (Chai). These safeguards include user access restrictions and file permissions (Chai). Version control can be used to stop authorized users from making mistakes or accidentally deleting things (Chai). Organizations must also provide some method for detecting any data changes that can happen from non-human events like an electromagnetic pulse, natural disaster, or server crash (Chai). Checksums, including cryptographic checksums, may be used in data to verify its integrity; redundancies or backups must also be accessible in order to restore the impacted data to its original state(Chai).

Availability

Information should always be regularly and easily available to authorized persons. This entails keeping up with the systems, hardware, and technical infrastructure that store and show the data (Chai). The best ways to do this are to keep all hardware under strict maintenance, fix any hardware issues as soon as they arise, and maintain a stable OS environment free of software conflicts (Chai). “Additionally, it's critical to stay up to date on all required system upgrades” (Chai). Equally crucial strategies include ensuring appropriate communication capacity and avoiding bottlenecks from occurring (Chai). “When hardware problems do arise, redundancy, failover, RAID, and even high-availability clusters can help to prevent major repercussions” (Chai).

Authentication v Authorization

Administrators employ authentication and authorization as two crucial information security processes to safeguard systems and data. A user's or service's identity is confirmed through

authentication, and their access privileges are established through authorization. Although the two phrases have a similar sound, they serve different but just as important functions in protecting applications and data. It's essential to comprehend the differences. They determine a system's security when taken together. Without adequately configured authentication and authorization, a solution cannot be considered secure.

Verifying that someone or anything is who they claim they are is done through the authentication procedure. To safeguard access to a program or its data, technology systems normally require some type of authentication. “For instance, you often need to enter your login and password in order to access a website or service online; Then, in the background, it checks your entered username and password to a record in its database” (Authentication). The system assumes you are a legitimate user and provides you access if the data you provided matches (Authentication).

The security procedure known as authorization establishes a user's or service's level of access (Authentication). In technology, authorization is used to grant users or services permission to access certain data or carry out specific tasks (Authentication). For example, take a manager of a restaurant and a regular employee. The manager is going to have authorization to access certain things that the regular employee will not such as paystubs or money drops.

Conclusion

The CIA triad is a very fundamental instrument when it comes to information security. It is a good first step in understanding the importance of maintaining and developing a security plan. Although it will not give you all the answers, it will put you on a path to figure them out.

Works Cited

"Authentication vs. Authorization: What's the Difference?" *OneLogin*, https://www.onelogin.com/learn/authentication-vs-authorization#:~:text=Authentication%20verifies%20the%20identity%20of,the%20security%20of%20a%20system. Accessed 12 Feb 2023.

Chai, Wesley. "What is the CIA Triad? Definition, Explanation, Examples." 28 June 2022, https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view. Accessed 12 Feb 2023.