Danielle Caplinger - September 13th, 2024

The CIA Triad, Authentication & Authorization

The CIA triad acts as the building blocks for good cyber security practices while authentication and authorization are some of the processes used to keep data confidential.

Overview

The CIA triad is a model used by cybersecurity professionals as a guideline for creating good information security policies. The CIA triad is also sometimes known as the AIC triad to not be confused with the government agency of the same name (Chai, 2022). CIA stands for confidentiality, integrity, and availability. All three of these processes need to be included in cybersecurity procedures to keep systems secure and functional.

Confidentiality

Confidentiality refers to keeping information private. Confidential data should only be accessed by those authorized, or allowed to do so. This is especially important when personally identifiable information (PII), medical information, or financial information is being stored. There are many ways to keep data confidential from a technical standpoint. Some of these include:

- Data encryption at rest, in transit, and while processing;
- Unique user credentials;
- Multifactor authentication (MFA);
- And password policies (Chai, 2022).

The data being protected will determine what levels of access controls that need to be used. Some data might only require a username for auditing purposes, while others may require a username, complex password, and a unique pin found in a MFA app. Once the level of confidentiality is determined, it is important for data to be protected at that level at all times.

Authorization

Authorization is often considered a part of confidentiality since a user needs to be authorized to access confidential information. Authorization is the process of allowing a user to access a specific piece of information or resource. This includes individual user, file, and group permissions (Kosinski 2024). Least privilege should be used here. Least privilege means a user should only be able to access what is needed to perform their task or job. For example, if Kathy works in the HR department, she should be able to access employee information. She should not be authorized to access the blueprints for a new prototype.

Authentication

Authentication is also related to authorization and confidentiality. If someone has access to a specific resource, they need to then prove that they are the authorized individual. Authentication is verifying someone's identity (Kosinski 2024). For example, if Rob is authorized to go into the server room for his company, he must first authenticate himself at the door using a fingerprint scanner. The scan proves his identity and lets him in. The most common type of authentication is based on something the user knows like a password. Other types include something the user has like a physical security token or something the user is inherently like a biometric scan. Some examples of common authentication methods include:

- Pins and passwords;
- Fingerprint readers;
- Digital certificates;
- And a physical ID card (Kosinski 2024).

Integrity

Integrity is the second part of the CIA triad. If data has integrity, then it has not been tampered or changed; it can be trusted to be accurate. Data must keep its integrity when it is being stored, being transmitted, and being processed. If changes are made to this data, auditing can be used to make sure it was an authorized change. Version control would then allow data to be reverted to the correct version if needed. Hashes and checksums are good examples of integrity checks for digital data. They verify that data has not been altered since the first hash or checksum was generated (Chai, 2022).

Availability

Availability is the last part of the CIA triad. Availability means that information and systems are always accessible for those allowed to access it. To keep systems available, redundancies need to be in place. This means having multiple pieces of equipment in case one fails as well as load balancers across the network. Information should be backed up properly at regular intervals. In the event of data loss, these backups can be restored to maintain availability. Disaster recovery and incident response policies should also be in place to ensure availability if a natural disaster or cybersecurity incident takes place (Chai, 2022).

Conclusion

The CIA triad is the best model for organizations to ensure they are using cybersecurity best practices. Following the CIA triad ensures that information is kept private, data can be trusted, and systems are available to those who need it. Authorization and authentication are key processes in access control to make sure users are properly identified and are allowed access to the information they need.

References

Chai, Wesley (2022, June 28). *What is the CIA Triad? Definition, Explanation, Examples.* TechTarget. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?jr=on.

Kosinski, Mark. (2024, June 8). *Authentication vs. authorization: What's the difference?* IBM. https://www.ibm.com/blog/authentication-vs-authorization/.