India Henry

CYSE 200 - 9:30

28 January 2024

The CIA Triad and the Importance of Security

This paper will define what the CIA Triad is and why each aspect of it is important for businesses to implement. The CIA Triad consists of confidentiality, integrity, and availability. Confidentiality is to "limit access to information", integrity to "assure information is trustworthy and accurate", and availability to "guarantee access to information for authorized people" (Chai, 2017). This paper will also define and compare authorization, checking user identity, and authentication, a person's authority when accessing resources, as it relates to availability.

The CIA Triad

The CIA Triad is an acronym to describe a model designed to guide the implementation of information security policies for businesses. CIA stands for confidentiality, integrity, and availability. These three principles are an integral concept for information security, making these principles important to implement for the security of an organization. Seeing the interconnectedness of the triad is important for implementation as organizations learn to understand the relationship between the three concepts rather than seeing them as independent variables.

Confidentiality

Confidentiality is defined as "a set of rules that limits access to information" (Chai, 2017). Confidentiality ensures that sensitive information is protected against unauthorized users. This includes helping to train *authorized* users about potential risk factors, such as social

engineering[1]. Sometimes data is “categorized according to the amount and type of damage that could be done if it fell into the wrong hands” (Chai, 2017). Some of the best tactics for implementing confidentiality are to handle privacy based on how confidential the data is and to keep a list of who is able to access and alter the data.

Some examples of confidentiality include user identification and passwords to access websites, in some cases two factor authentication is also a part of the login process. “Extra measures might be taken in the case of extremely sensitive documents, such as storing only on air-gapped computers, disconnected storage devices or, for highly sensitive information, hard-copy form only” (Chai, 2017). There are also cases where data can be encrypted to maintain confidentiality.

Integrity

Integrity is defined as “the assurance that the information is trustworthy and accurate” (Chai, 2017). This means having accurate, trustworthy, and consistent data, which would mean ensuring that data is not changed during transport or by unauthorized users. This can also mean having multiple copies of the same document to prevent human error or server crash, which would allow for data to be restored in the event it is lost. Some examples on how to implement integrity is to have digital signatures to show “evidence of logins, messages sent, electronic document viewing and sending” (Chai, 2017). Human error cannot always be eliminated, but organizations should do as much as possible to educate their employees about compliance to minimize human error.

Availability

Availability is defined as “a guarantee of reliable access to the information by *authorized* people” (Chai, 2017). This means that information should always be readily available to

[1] Social methods that are used to obtain personal or confidential information which can be used illicitly.

authorized users, so all hardware and software updates must be maintained to keep the documents readily available. This would also mean that the worst case scenario, and how to combat it, must be thought of before it happens to ensure that the information remains secure and accessible. For example, firewalls or proxy servers used to guard against DoS[2] attacks. Some examples on how to prevent this would be to use network or server monitoring systems, ensure a data recovery plan in case of data loss, and ensure systems and applications stay updated.

A factor that influences the availability of data is *authorization*, defined as a process that checks a user's authorities before allowing them access to resources. In other words, authorization checks the ability of users to make changes to a document. An example of this would be an access token. Authorization can be confused with *authentication*, which is defined as the process of checking the identity of users before providing them access to resources, so the ability of users to be able to look at, but not alter, documents. For example, an ID token.

Conclusion

In conclusion, the CIA triad is an important aspect for businesses and organizations to implement to ensure the security of their private information. The three main ideas to implement are confidentiality, limiting access to information, integrity, ensuring the information is reliable, and availability, allowing for authorized users to access the information and authenticated users to make changes as needed to the information.

[2] A cyber attack that aims to make a machine or network resource unavailable to its intended users.

References

Chai, W. (2017, November 9). *What is the CIA Triad? Definition, Explanation, Examples*. Tech Target. Retrieved January 25, 2024, from https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view

Jain, S. (2023, February 22). *Difference between Authentication and Authorization*. GeeksforGeeks. Retrieved January 25, 2024, from https://www.geeksforgeeks.org/difference-between-authentication-and-authorization/

Merriam-Webster. (2024, January 15). *Social engineering Definition & Meaning*. Merriam-Webster. Retrieved January 25, 2024, from https://www.merriam-webster.com/dictionary/social%20engineering