Tgen Hampsher
February 12, 2025
CYSE 200T
Professor Duvall

Breaking Down the CIA Triad

BLUF: CIA Triad stands for Confidentiality, Integrity, and Availability; and it represents the foundational goals of any cybersecurity infrastructure.

Confidentiality

Confidentiality is seen as the first layer of defense in cybersecurity, and it describes who has access to data (Hashemi-Pour, 2023). In other words, professionals in the field would say this refers to who is authorized to access certain data. As data becomes more sensitive, the number of users authorized to access that data will decrease to mitigate the threat of lower-level employees mishandling the data. For users with access to data, they can help ensure that unauthorized users don't break into the network by creating secure authentication methods. Setting strong passwords, using Two-factor authentication (2FA), and potentially even storing the most sensitive data on computers independent of the network are adequate methods to properly authenticate users and protect the confidentiality of data (Fruhlinger, 2024). Therefore, authorization is the process of deciding who has access to certain data, and authentication is the process of checking to make sure authorized users are the actual person accessing the data rather than an intruder.

Integrity

Integrity is the next layer of defense and is seen as the ability to protect data from being modified or damaged by those who have access to the data (Hashemi-Pour, 2023). Once data is accessed, implementing controls such as user access control lists and file permissions is a great way for companies to protect their data from being altered via users. For example, a company may allow for most authorized users to view filed within the network; however, the permissions for editing that file and/or moving the file across the network will likely be limited to higher management positions that are more experienced and trusted (Fruhlinger, 2024). Additionally, the integrity of data can be maintained by ensuring that

backups of important files are saved in the case of the original file being deleted or altered beyond repair, which allows for the backup to be transferred to the location of the original file.

Availability

Availability is the last layer of defense in cybersecurity, and it means that data should be quickly accessed by those who are authorized to have the data, to respond to the integrity of data being breached (Hashemi-Pour, 2023). Ensuring availability is a continuous and complex process for companies that involve multiple factors such as updating/upgrading hardware and software when necessary. For most companies, this process involves security equipment, firewalls, and proxy servers, all of which help to monitor and guide traffic in and out of the network. Additionally, companies should create a business continuity plan (BCP) and disaster recovery plan (DRP) to respond to incidents that occur within the network. These plans should be detailed and thoroughly understood by all users on the network.

Conclusion

In conclusion, confidentiality, integrity, and availability are the three most important concepts that a cybersecurity infrastructure must address. For major companies with many devices and users on the network, the CIA Triad must be kept in the thought process of always protecting the network to ensure that residual risk left to a company is as low as possible. The CIA triad should be a starting point for every company.

References

Fruhlinger, J. (2024, July 12). *The CIA triad: Definition, components and examples*. CSO Online. https://www.csoonline.com/article/568917/the-cia-triad-definition-components-and-examples.html

Hashemi-Pour, C. (2023, December). *What is the CIA Triad? Definition, Explanation and Examples*. TechTarget. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA