Timothy Barrett
9/15/2024
CYSE 200T

The CIA Triad – Guidance for Information Security in an Organization

The CIA Triad is used to ensure security systems are developed in such a way that the systems and the information that they hold are protected, and vulnerabilities are easy to fix (Fortinet). Information should be secure, trustworthy, and as accessible as possible.

Confidentiality – Keep Information Safeguarded

Confidentiality is ensuring data is secure. Roadblocks are essential to preventing people without proper authority from accessing PII, Personally Identifiable Information (IBM). This information can be used to commit theft of identify, especially if the stolen information consists of a combination of driver's license numbers, government issued ID numbers, and biometric identification (IBM). For this reason, it is imperative to safeguard this data by ensuring that personnel in an organization are savvy to social engineering methods such as phishing attempts. The users of accounts can authenticate or verify their identity by using something like two-factor authentication or biometric verification (Chai 2022). If one cannot authenticate themselves as being an authorized user, they will not gain access to the information and the roadblock will be successful.

Integrity – Information Must be Trustworthy

The integrity branch of the CIA Triad revolves around ensuring data is trustable and tamper free (Fortinet). Integrity can be ensured by enabling user access controls over files and

version control to track who changes files and when those changes occur (Chai 2022). Hashing, encryption, and things like digital signatures are all things that can be used to keep files trustworthy and easy to be quickly identifiable if an unauthorized change is made (Fortinet).

Availability – The Data is Readily Obtainable

Data that is inaccessible is not useful data (Fortinet). Information should be regularly attainable for those who are authorized to view it (Chai 2022). This branch is best utilized by making sure proper system maintenance is scheduled consistently and completed as scheduled (Fortinet). Unpredictable events such as natural disasters can be mitigated by utilizing redundant servers or networks that come online when the primary system has been taken down (Fortinet). It is important that downtime is kept to a minimum to ensure critical information of an organization is as readily available as possible (Fortinet).

Conclusion

Proper safeguards must be in place and fully maintained. If any section of the CIA Triad is lacking, the information that is meant to be secure, available, and trustworthy, could very easily be tampered with, brought offline, or stolen in large quantities.

References

1. Chai, W. (2022). What is the CIA Triad? Definition, Explanation, Examples. Retrieved 9/15/2024 from https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?jr=on
2. Fortinet. (2024). What is the CIA Triad? Fortinet, Inc. Retrieved 9/15/2024 from https://www.fortinet.com/resources/cyberglossary/cia-triad
3. IBM. What is personally identifiable information (PII)? Retrieved 9/15/2024 from https://www.ibm.com/topics/pii#:~:text=Personally%20identifiable%20information%20(PII)%20is,email%20address%20or%20phone%20number.