Justin Saldivar

Charles E. Kirkpatrick

CYSE-200

1/29/2023

A writeup on the CIA triad

Basics on the CIA triad

The CIA triad is a security model meant to ensure data is properly secured, transported, and protected. The most common phrase that is used to describe the three values is availability. confidentiality, and integrity. Availability means a steady and secure source to pull information from, confidentiality meaning constant and enforced clearance for the access of information, and integrity meaning that all information accessed has not been tampered with and is original.

What does each one mean and what do they do?

In the context of the triad, each phrase has a special role in keeping data secure, starting with confidentiality. Which means the protection of vital information from unauthorized attempts to access them. For example, security questions, two-factor authentication, or a security token such as a biometric check all fall under confidentiality (Chai, 2022). Next is Integrity, which means untainted and secure information that can be accessed without any changes both before and during transit, examples include logs of accessed materials, certificates or signatures of validity, and periodic checksums for any tampering or corruption (Chai, 2022). Finally, Availability means a consistent and secure way of accessing materials in a timely manner. Examples include off site servers, redundant critical systems, and up to date software, firmware, and hardware (Chai, 2022).

Why is it important?

As the tenets of the triad typically represent important principles to running a secure system. They provide a foundation in which to build your security policy that can handle or prevent potential leaks, an example of the triad working together to defend against threats is insiding. As all types of insiding typically result from a failing in the triad. An example of this is the loss of data thanks to the disabling of a patch in a critical system due to the desire for easier access to another system, this is a violation of integrity and can result in data loss or corruption (Froehlich et al.).

Challenges against the triad

The main issue that rises when managing a system using the triad is simply how much there is to look after, in addition. Data redundancy and maintenance checks can stretch the budget if the size is large enough, in addition. The rising popularity of Internet Of Things systems can add another layer to consider when implementing security for the system (Chai, 2022).

Justin Saldivar

Charles E. Kirkpatrick

CYSE-200

1/29/2023

Conclusion

To summarize, the CIA Triad is a general tenet and guideline for information security; it stands for confidentiality, integrity, and availability. These mean security from unauthorized taps and breaches, security of original data from tampering by outside sources, and a consistent way of accessing said information in the system. It is critical to prevent major data breaches and loss of trust from clients. The main challenges include scaling from infrastructure and outside variables such as IOT systems.

References.

Chai, Wesley "*What is the CIA Triad? Definition, Explanation, Examples."* 28-06-2022

What is the CIA Triad_ Definition, Explanation, Examples - TechTarget.pdf

Froehlich, Andrew, et al. "What Is an Insider Threat?" Techtarget.Com, TechTarget, 22 July 2022, https://www.techtarget.com/searchsecurity/definition/insider-threat.