Adam C. Haas
1/23/2024
CYSE 200T
26759

Understanding the CIA Security Triad

Introduction

Organizations that want information security for their operations should, at a minimum, ensure their system meets the CIA security triad by keeping their information confidential, establishing integrity, and being available when requested. One of the key ways to ensure this is completed correctly is by requiring authentication and authorization. Organizations that implement safeguards to their information boost consumer confidence and help make sure their systems are functioning as intended.

Confidentiality

Confidentiality is one part of the triad and is paramount to ensuring that sensitive information is only available to those that have been approved. It certifies that data is accessed by only those who are authorized to do so (Kim and Solomon 2018, pp. 14–128). Chai (n.d.), writing about the CIA Triad, lists some good examples of ways to keep information private: data encryption, user ids, passwords, two-factor authentication, biometric verification, and security tokens. Organizations need to know they can trust that their systems won't reveal private information that could have unintended consequences for their mission.

Integrity

Integrity is another part of the security triad that requires keeping data safe and unchanged. Like Kim and Solomon (2018, pp. 14–128) explain, it is ensuring that data is accurate and valid. Organizations need to be able to certify that their information hasn’t been tampered with. Chai (n.d.) gives some great examples of this including: checksums, identity verification, back-ups, and digital signatures as ways to ensure non-repudiation of their data. Organizations' reliance on accurate data is important to ensure honesty and truthfulness.

Availability

Availability is the final third of the triad ensuring information is attainable when needed. Users need to be able to access data confidently when there is a need. Kim and Solomon (2018, pp. 14–128) hold that availability is expressed when data and systems are accessible and achievable. According to Chai (n.d.), there are different ways to accomplish this. Some examples include maintaining hardware, keeping software free of issues, providing sufficient bandwidth, redundancy, and a robust disaster recovery plan. Having systems and data available is a core need for function and success of an organization. Most businesses rely heavily on digital operations for many of their functions. A break in availability could inhibit or halt productivity.

Authentication Versus Authorization

The CIA security triad is fortified by two key functions of an organization: authentication and authorization. These two functions are closely entwined to make sure only the correct people have access to information systems. Kim and Solomon (2018, pp. 14–128) share that authentication is proving a user is who they say they are and authorization is the operation of giving access to an organization’s data and systems. Examples of authentication are passwords, tokens, or biometric readings. Examples of authorization are access control lists, physical access control, connection and access policy filters, and network traffic filters. To keep information systems secure, users must be able to show they are authentically who they say they are and that they have been authorized by the organization for entry into their systems and data.

Conclusion

The CIA triad is the foundation of information security within an organization. This is represented through the protection of information by keeping data confidential, non-repudiated, and available. These three aspects of the security triad are the bases for forming a complete and functioning security policy and rely heavily on authorization and authentication to confirm users have been given permission and they are who they say they are. Digital information is one of the major drivers of our culture making data security a top concern.

References

Chai, W. (n.d.). *What is the CIA Triad? | Definition from TechTarget*. WhatIs. Retrieved January 23, 2024, from http://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA?

Kim, D., & Solomon, M. (2018). *Fundamentals of information systems security* (3rd ed., pp. 14–128). Jones & Bartlett Learning.