

Thomas Winterrowd

CYSE-200T

September 15th 2024

Analysis of the CIA triad and Authentication vs. Authorization

Introduction

This document will explain the functionality of the CIA triad and Authentication & Authorization. The CIA triad is an important model used to evaluate the security of an organization. Confidentiality, Integrity and Accessibility are all key factors that an organization must balance and manage correctly.

Confidentiality

Confidentiality is about the privacy and protection of information from unauthorized actors. Confidentiality can be used to measure how secure something is from unauthorized access attempts. The more sensitive a piece of data is, the more damage that is dealt from having it leaked or accessed wrongly, therefore needs higher confidentiality. Examples of sensitive information that require high confidentiality are credit card numbers, social security numbers and passwords. Methods like encryption and multi-factor authentication are used to ensure proper confidentiality.

Integrity

Integrity is about making sure that sensitive information is only changed by authorized actors, and the ability to identify that the information is valid. Having data remain unchanged by unwanted attacks is extremely important, especially when the data is in transit. Some measures for countering attacks against integrity are making back-ups, comparing data with message digests and encrypting data. Integrity can easily be the difference between a cyber attack that goes undetected and one that does not: An example could be proper integrity controls preventing an attacker from erasing important log files and being unable to cover their tracks.

Availability

Availability is about guaranteeing that information and services are accessible to the properly authorized users at all times, or as close to all times as possible. Availability heavily involves redundancy, in which access is guaranteed through means like frequent data backups and redundant servers. Availability serves to protect from non-human incidents like hard drive failure and hardware failure in a server, and it also serves to protect from attacks like DDoS's. Being able to properly access information when needed is imperative to the entire business, and improper management that leads to poor availability can easily lead to loss of profits by the organization not being able to function correctly.

Authentication

Authentication is the action of validating the identity of a user: Checking to see if they are who they say they are. In order to validate an identity, metrics like what they have, who they are and what they know can be used. Some examples of validating by what they know are security questions like "What was the name of your first pet?" and a password.

Authorization

Authorization is the action of granting a user privileges and permissions. In order to make sure that the user is not attempting to access permissions they do not have, their identity is validated through authentication beforehand. Permissions are the user's ability to read or write some piece of information, or the ability to access a certain system.

Authentication vs. Authorization

Authentication and Authorization work together to ensure that there is no misuse of permissions, and that permissions for valid users are granted correctly. Authentication and Authorization are separate actions, but they are both equally important to security and the function of an organization. Authentication validates the user's identity, and Authorization grants privileges and carries out actions based on the results of Authentication.

Conclusion

Confidentiality, Integrity and Availability are all critical aspects of cybersecurity, and Authentication and Authorization serve to strengthen the CIA triad. Different levels of attention and support are needed for each element of the CIA triad depending on what is being defended, but proper balance is necessary to prevent security incidents and waste of resources. As part of proper balance, it is possible that too much attention to one element of the CIA triad can detract from another: For example, too much focus to Availability can damage the Confidentiality of some information.

Works Cited

Hashemi-Pour, Cameron. "What Is the CIA Triad? Definition, Explanation and Examples." *TechTarget*, TechTarget, Feb. 2023,
www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA.

"Confidentiality, Integrity and Availability in Cyber Security." *Kobalt.io*, 5 Nov. 2021,
<https://www.kobalt.io/confidentiality-integrity-and-availability-in-cyber-security/>

"Authentication vs Authorization: What Is the Difference?" *Fortinet*,
www.fortinet.com/resources/cyberglossary/authentication-vs-authorization.