

Shawn Ziegler

CYSE 200T

Write-Up

2/21/25

The CIA Triad

Introduction

The CIA stands for Confidentiality, integrity, and availability. The CIA triad is a model that allows organizations to guide policies for information security. These three principles are the most important components in information security. Availability entails that access to reliable information is a guarantee if authorized. Confidentiality is a set of restrictions that regulate access to information. Integrity declares that the information is accurate and true.

Importance of the CIA Triad

Each letter within the triad represents key components within cybersecurity. The triad is a useful tool to guide the development of new products and technologies for organizations. The organization can use the triad to evaluate the needs and how value is being provided in these components. A good example of confidentiality is banks requiring an account or routing number when accessing a bank account online. A good example of integrity is running backups to restore affected data back to its natural state. Great examples of availability are making sure all hardware is immediately repairable, also making sure system upgrades are made when needed. This will ensure a proper functioning operating system.

Authentication vs. Authorization

Authentication is used to verify a person's identity. On the other hand, authorization gives a person the right to access a system and its resources. The authentication process relies on credentials. A good example of this is when a person uses a username and password to log in to a computer or program. Another example is when a person needs to scan an I.D. or scan their fingerprint to enter a building. Authorization relies on gaining permission to access a specific network or program. A good example of this is a company's database; the person must be authorized to be able to access any files or navigate through the database (Kosinski, 2024).

Conclusion

The CIA triad is a very important tool to utilize within an organization, as it allows for companies to have a guide for information security. Companies can monitor what new products and implement technology advancements based on the company's needs. Authentication and authorization are both very important because they both provide security for an organization. Having a strong authentication system makes it more difficult for hackers to gain access to a person's credentials. Within the authorization process, this will limit the impact that the hackers may have on a person's account or the company's database (Kosinski, 2024).

Sources

Kosinski, M. (2024, December 2). *Authentication vs. authorization: What's the difference?* IBM.
<https://www.ibm.com/think/topics/authentication-vs-authorization>