Evolving strategies for the Foundation of Cyber defense

Nehemia Araia

Department of Cybersecurity, Old Dominion University

CYSE200T: 31563

Dr. Charles E. Kirkpatrick

January 28th, 2024

After reading this article I have learned that the CIA Triad has remained the bedrock of information security. This article explores the possibilities of the CIA Triad and introduces approaches to fortify organizational defenses. I believe this is true as professionals advocate for a stronger approach to safeguard critical assets effectively.

Understanding the CIA Triad

The CIA Triad consists of Confidentiality, Integrity, and Availability, and is known for the fundamental framework guiding information security practices in organizations. Confidentiality ensures that sensitive data remains available only to authorized people, preventing unauthorized users access. Integrity focuses on maintaining the reliability of data throughout its lifecycle, safeguarding against unauthorized changes. Lastly, Availability guarantees that information is consistently and always accessible to authorized users. Combining these three principals form a comprehensive security strategy, providing a framework for protecting against unauthorized users and data breaches.

The roles of Authentication and Authorization

Authentication and authorization are two important components of information security, both playing their own separate role in controlling access and verifying identities. Authentication verifies the identity of users or entities attempting to access a system or resource, making sure that they are who they claim to be. Common authentication methods include passwords and two-factor authentication. For example, when logging into your school account on myODU, you must provide the correct credentials along with two-step authentication if applicable. Authorization determines what actions or resources a user is allowed to access or perform after they have been granted access. It specifies the permissions and privileges given to authenticated users based on their role. For example, when accessing an ODU employee site, after logging in with your credentials, the system will recognize you as a staff member or a student if access isn't granted. Access control lists and role based access control are commonly used for authorization, making sure that people can only access data that are provided for their roles.

Conclusion

In conclusion, The CIA Triad remains the backbone of information security, while guiding organizations and navigating the complexities of the digital surface. By understanding the principles of authentication and authorization, organizations can fortify their defense against unauthorized access and data breaches. The Confidentiality, integrity and availability of information is extremely crucial to the operation of a business (Taylor, 2017, p.1). As highlighted in the article, authentication verifies user identities, while authorization controls access to resources based on authenticated identities. By transcending the principals of the CIA Triad and adopting advanced technologies and practices, organizations can adapt to emerging threats and gain trust through our connected world.

References

Taylor, C. (2017). *What is the CIA triad and why is it important?*. Fortinet. https://www.fortinet.com/resources/cyberglossary/cia-triad

Hashemi-Pour, C., & Chai, W. (2023, December 21). *What is the CIA triad?: Definition from TechTarget*. WhatIs. https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA