The CIA Triad and What It Is About

            “Confidentiality, integrity, and availability, also known as the CIA triad, is a model designed to guide policies for information security within an organization.      “(Chai,2022). Within this business outline, there is confusion about the difference between authentication versus authentication. In the discussion, we will go over what the triad is and how authentication and authorization compare.

*What is the CIA Triad?*

            The CIA Triad is a user manual for how employees should treat information security within an organization or company. This framework was created as a simplistic way of how cybersecurity should try to ensure the best data security that they can provide to any organization they may be working for. The first letter within the plan stands for the confidentiality supplied in the framework.  “Confidentiality in information security assures that information is accessible only by authorized individuals.”(Prakash,2024). This quote helps to gain a basic understanding of what confidentiality is. Suppose confidentiality is needed to ensure that employees who have the correct authentication within the organization can access what they need. Or it can even be as simple as assuring the confidentiality between one employee and another is kept ensuring security is the best it can be. Without confidentiality integrity and availability would be almost useless. Integrity is the assurance that no data that comes through has not been compromised and that it can be trusted. This step helps to verify that the data being held is in the correct form and not prone to attack. While also making sure that the correct employee with prior authorization can access the data. Upkeeping this component helps to ensure that what data is being given and sent is trustworthy and up to code. Last in this plan is the availability framework. Availability is used to remind the employee how to ensure every network, system, and application within those are up to date and able to operate. If these things are not operational then there’s a good chance that the business could lose all customers and go bankrupt. Author Mrinal Prakash says “Multiple things can threaten availability, including hardware collapse or software issues, power failure, natural circumstances beyond one's control, and human error.” (Prakash,2024). This shows a faint glimpse of how many errors there are that could lead to a failure of availability in a business. This shows that making sure availability is being provided is very important for the success of an employee in a business.

*Authentication vs Authorization How are they Different?*

            Within business, these two ideas of someone needing authentication or authorization are often blurred. However, with basic understanding many will find it easy to understand the difference between the two. Author Arpana Dhaka states” Authentication is the process of verifying the identity of a user” (Dhaka,2023) helping gain a general idea of authentication. Authentication is used to ensure that when people log in to a certain place, they are who they claim to be. One of the best examples of authentication would be the still somewhat new implementation of two-factor authentication. Examples of this being used would be the login process with a Microsoft account. When a user enters their credentials into the login screen, they are asked to do a two-factor authentication. Most cases involve sending a could to the person's phone number through text or sending it to their email. This ensures that the user is who they claim to be which helps ward off potential scammers getting into their account and misusing it. Authorization on the other hand is the determination of what can and cannot be accessed by specified users. Most businesses have authorization for each employee they have at the office to ensure that what is being accessed is not being accessed by someone who has no reason to be viewing the current document. One example could be provided within the school setting between a teacher and a student. Students are given authorization for the assignments, the lectures, and the book that provides the material that the student must learn. The teacher has authorization to access the answers to said assignments and the authorization to create and publish the lectures needed for the class. If a student were to gain access to the teacher’s authorization it would ruin the whole idea of learning since they would just have access to all the answers to the assignments that help them learn. This example shows how important it is for the right people to get the right authorization.

*Conclusion*

            After being able to understand the differences in authentication and authorization understanding the inner workings of the CIA Triad becomes simple. As we move forward in cybersecurity jobs and the new technologies that come along with it. Having a basic understanding of the CIA triad is a must to ensure that employees do not ruin the future of the business they may find themselves in. Proving that confidentiality, integrity, and availability are always upkeep will ensure that every cybersecurity employee will have a successful future in whatever organization they may join.

*References*

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

Prakash, M. (2024, July 24). What is CIA triad? examples, components, importance & goals. What is CIA Triad? Examples, Components, Importance & Goals. https://www.knowledgehut.com/blog/security/cia-in-cyber-security#what-is-cia-triad%C2%A0in-cyber-security?

Dhaka, A. (2023, January 20). Authentication vs. Authorization - Whats the difference?. Authentication vs. authorization – what’s the difference? https://mojoauth.com/blog/authentication-vs-authorization/