What is the CIA Triad?

The CIA triad is a term widely used in the Information Technology industry and it stands for Confidentiality Integrity and Availability. It is a very important process model used in the Cyber security world to securely create, operate and foster a healthy digital footprint for your IT infrastructure. Authentication and Authorization are two major concepts utilized in the cybersecurity field and within the CIA triad for securing your infrastructure.

The CIA triad also known as the AIC triad (availability, Integrity and confidentiality) is a model created to steer policies within an organization to a more robust cyber posture. (Chai, 2022). Confidentiality is the privacy and sensitivity of the data within your system per your organizations classification. The integrity portion of the triad involves assuring that the data within the system has not been altered, sabotaged or misplaced during its lifecycle. Lastly, availability means that the system and its data should be readily available and accessible by all parties with proper authorization. This triad is very important in the cybersecurity and information assurance workforce.

Authentication is the process of validating a user and their identity (Okta, 2024). One layer of authentication is a simple username and or password. In today's modern world businesses are validating authentication through more advanced standards like two factor authentication (2FA). Examples of 2FA are third party authentication applications, one time passcodes sent to the users registered email address or hardware RSA tokens. An example of this would be the something you have and something you know process of gaining access to a system. A user would log on to the system with a username such as John Doe and be prompted with a password. Hopefully one with a character length of 16 or longer for added security. The password is the something you know portion. Once Authenticated on the first factor you should

be then required to utilize the second factor being for example a hardware RSA token. Once you enter the RSA token passcode on the system you are now fully authenticated through both factors.

Authorization gives the users that were previously authenticated into a system authorization to access a specific resource (Okta, 2024). Authorization can be used synonymously with access control. A common example of this would be elevated privileges for System Administrators on a server or desktop. Normal users and the System admins both need access to the resource but through authorization the System Admins have elevated privileges to make changes to files and or important data.

In conclusion the CIA triad in combination with proper Authentication and Authorization methods is a very effective and promising concept to utilize within any IT organization.

References

Okta. (2024, September) Authentication vs. Authorization. *Identity 101.* Retrieved February 08, 2025, from https://www.okta.com/identity-101/authentication-vs-authorization/

Chai, Wesley. “What is the CIA Triad? Definition, Explanation, Examples”. 28, June 2022