Helena Trent
CYSE 200T
Intro to Cybersecurity, Technology, and Society

The CIA Triad

The CIA Triad is a collection of foundational principles used in cybersecurity. Confidentiality, integrity, and availability are the most important aspects of information security. These principles rely on authorization and authentication. It is believed that these principles are the key to effective cybersecurity.

What is the CIA Triad ?

The CIA Triad is a set of foundational principles pertaining to information security. CIA stands for confidentiality, integrity, and availability. These principles are very important to cybersecurity. There is not a specific time when the triad was first founded. It has developed over the years with multiple contributors. The U.S Air Force is believed to have founded the first ideas in 1976 (Fruhlinger, 2020). CIA is used similar to a checklist. It is believed that as long as these requirements are met security should be effective and up to standard.

Confidentiality

Confidentiality is the privacy portion of the CIA Triad. It states that information should be kept private and confidential. Unauthorized users are not permitted to view information (*What Is the CIA Triad and Why Is It Important?*, n.d.). Authentication and Authorization measures are both examples of confidentiality (Fruhlinger, 2020). Confidentiality is not strictly a tech

problem. Human error can also break confidentiality. Sharing credentials, unsecure hard copies, and leaving devices unattended could all potentially cause information security problems (*What Is the CIA Triad and Why Is It Important?*, n.d.).

Integrity

Integrity is making sure that the information being presented is accurate and untampered with. In most situations it would take a breach of confidentiality to break integrity. Users should not be able to make unauthorized changes to information (Fruhlinger, 2020). An example of this would be changing business documents to influence decisions. Hashing, encryption, and certificates are all effective ways to uphold integrity (*What Is the CIA Triad and Why Is It Important?*, n.d.).

Availability

Availability means that information should be available when needed. The biggest threat to availability is denial of service attacks and intrusions. To avoid these conflicts it is recommended to have proper backup procedures. Updated equipment is also essential for minimizing risk. It is also important to update hardware and software as needed. Another aspect of availability is being able to recover from disasters. Inevitably, something will happen. It is important to be prepared and have a solid disaster response plan to get systems back up and running in times of crisis (*What Is the CIA Triad and Why Is It Important?*, n.d.).

Authentication & Authorization

Authentication and authorization is what holds the CIA Triad together. While these two terms are often used interchangeably they are two different concepts in cybersecurity. Authentication is the process of making sure someone is who they say they are. It always comes first between the two and is arguably the most important part of cybersecurity (*Authentication Vs. Authorization: What's the Difference?*, n.d.). Authentication operates by using something only the user would know or have possession of. For example, iPhones use facial recognition as their authentication process. If the person attempting to access the phones does not match the scan they are denied access. While this is a fairly simple process the concept remains the same in complex systems.

Authorization determines what the user has access to once they authenticate themselves. It is used to stop information from getting into the wrong hands. For example, when sharing a file you may want to give the person permission to view but not to edit. Giving them permission to edit could result in a conflict of integrity since they are only authorized to view. Another example would be not having the clearance to view certain documents so they are unavailable. Access Control Lists are used to determine who is authorized to do what. These lists are commonly managed by an administrator who is authorized to handle and change permissions (*Authentication Vs. Authorization: What's the Difference?*, n.d.).

References

Authentication vs. Authorization: What's the Difference? (n.d.). OneLogin. Retrieved January 25, 2023, from https://www.onelogin.com/learn/authentication-vs-authorization

Fruhlinger, J. (2020, February 10). *The CIA triad: Definition, components and examples*. CSO Online. Retrieved January 26, 2023, from https://www.csoonline.com/article/3519908/the-cia-triad-definition-components-and-examples.html

What is the CIA Triad and Why is it important? (n.d.). Fortinet. Retrieved January 25, 2023, from https://www.fortinet.com/resources/cyberglossary/cia-triad