Name: Ean N. Miller

Date: 1-29-2023

OLD DOMINION UNIVERSITY

CYSE-200 CYBERSECURITY TECHNOLOGY AND SOCIETY

WRITE-UP #1: The CIA Triad

Table of Contents

Contents

The CIA Triad is vital to secure data and technology and prevent many technological threats and data leaks in the community. The Chai article talks about the CIA Triad, its meaning, and why it is vital in data security and other facets of life. It goes further, talking in great detail about the Triad's three main parts: Confidentiality, Integrity, and Availability.

When first seeing or thinking about the word confidentiality and its meaning, many people think of something like patient-doctor privilege in terms of therapy or any other medical topic. While confidentiality typically means secrecy from other people who are not privy to sensitive information regarding a person, confidentiality within the cybersecurity field carries the same meaning. Confidentiality is vital in the CIA Triad, with cybersecurity and securing data. Generally, however, to safeguard sensitive data and info, there is some particular training that some people have to go through to protect data and various other pieces of information and be authorized to safeguard it. As the Chai Article says, "Training can help familiarize authorized people with risk factors and how to guard against them." Without some training to keep sensitive documents from getting leaked, without this training a lot of sensitive data could get leaked and lead to catastrophes and various issues within the community. Some of this training involves several methods and techniques to keep sensitive data secure and safe from data leaks. One such method involves strong passwords; another strategy to prevent data leaks would be encrypting the data and files. Encryption makes the data found within files unreadable to everyone except the person who did the encryption; however, much like everything else, encryptions can be broken and should not be the only safeguard when trying to secure data. Another technique that can be used, along with file and data encryption, would be managing data access. Simply put, only certain personnel are privy to sensitive data, and if this group of authorized individuals is relatively small, it can help reduce some confidentiality risks.

Integrity is the quality of your character or product; in cybersecurity, this is relevant because, with high-quality products or techniques, data security is more secure than it is, compared to higher-quality methods. Not only that, but as mentioned early, integrity relates to one's character; in the field of cybersecurity, it refers to permissions and various user access controls, among other methods that organizations may employ to verify someone and the integrity of the system or organization. One way organizations may verify data is, as stated in the article, "...checksums, even cryptographic checksums…" which is essentially encrypted data. Not only that but organizations may also employ other means that can detect data changes they are trying to protect in case of attacks such EMPs or server crashes. Not only that, but integrity also "...refers to the accuracy and completeness of data." as stated by another article, *Confidentiality, Integrity, & Availability: Basics of Information Security*. Essentially integrity, much like confidentiality, is a vital part of the CIA Triad and in the field of cybersecurity. Integrity allows organizations to ensure and secure a system and data from unauthorized tampering and the completeness of its data.

Availability outside the field of cybersecurity generally means the ability to be used or just be around when something does not go according to plan. However, availability in the field of cybersecurity has a similar meaning, but it also means systems need "...Fast and adaptive disaster recovery…" as stated in the *Chai Article*. Without a fast and adaptive system or hardware, once a cyber attack happens and cripples an organization's data and hardware, it may take a while to get back up and running, leading to possible data being lost or leaked. Some precautions can be taken to prevent or improve disaster recovery, such as firewalls that can help with DoS or Denial of Service attacks. Firewalls are not the only preventative measure for a cyber-attack; proxy servers are fantastic methods to ensure data security. Since cyber-attacks are not the only issue when trying to secure data, disasters can also come from natural disasters like fire and flooding. A straightforward way of securing data if one of these events were to occur is to make a backup on an off-site server or another location.

Authentication and authorization are two rather similar-sounding concepts when put together, although there are many vital differences when talking about these two. One is the process or the ability to check or verify if someone’s credentials are valid and if they are authorized to access sensitive data. Authorization, on the other hand, as briefly mentioned, is more about the who or who is not privy to sensitive data and if they have the credentials or prerequisites to access the data. The crucial difference between authentication and authorization is how they work; not only that but without the correct or valid clearance, a person can go through the process of authentication without being denied. Authentication is another added measure or precaution to ensure that people have the correct credentials or clearance to access vital data. Meanwhile, authorization is what you have to access said sensitive data; without these two concepts, people would be able to come and go as they please, taking data from various organizations and creating massive data leaks. Essentially in any organization, you can not have one without the other. Although they sound and seemingly act similar, they have that crucial difference that holds security together and helps an organization’s security properly work

In conclusion, I believe that the CIA Triad and the many precautions that come with it are vital to our society's infrastructure. Without the various methods of confidentiality, many data leakages could cause discord within a community. Without integrity, tampered or incomplete data would be far more common and cause issues. Without availability, many hardware and software would not be adequately maintained and updated, turning many of our devices obsolete and would cause many businesses and organizations to falter. Not only that, but the critical difference between authentication and authorization is that authentication generally are systems that can give people access to specific data if they have the proper credentials. Where authorization is more about getting or having those previously mentioned credentials to access sensitive data, you can not have one without the other.

Sources Cited:

https://drive.google.com/file/d/1898r4pGpKHN6bmKcwlxPdVZpCC6Moy8l/view

https://www1.udel.edu/security/data/confidentiality.html

https://getsmarteye.com/confidentiality-integrity-availability-basics-of-information-security/