CIA Triad Write-Up

Stephen Giorgi

School of Cyber Security, Old Dominion University

CYSE 200T Introduction to Cyber Security

Professor Kirkpatrick

September 18, 2022

Introduction

The CIA or AIC triad is a core concept in cyber security that is made up of three basic concepts. These concepts are Integrity, confidentiality, and availability. I will briefly describe the concepts as well as the difference between authentication and authorization. I will be referencing the given article by Wesley Chai, a video by ittaster, and my experience and training regarding the subject.

Integrity

I want to start by describing integrity. Ittaster defines this as "ensuring that data is not changed by unauthorized individuals." Right away, we need to know what makes an individual authorized. To put this simply, it is who ever is allowed access to specific data or hardware on a case-by-case basis. Like with security clearance, a person that has high authority in an organization may not be authorized or have the "need to know," so this excludes anyone that isn't working with the data. How we can maintain integrity through multiple ways such as digital signatures. Digital signatures are self-explanatory enough, they are code attached to a file that specific originator, such as a sender of an email, that will cause the file to be lost if the file is tampered with (ittaster). It is important that back up and recovery software is used in the case that data is lost (Chai).

Confidentiality

However, while integrity is important, data doesn't need to be tampered with to be dangerous for an organization or its members. Confidentiality is preventing unauthorized individuals from interacting with the data in the first place. This can be done, again, in a few ways and depending on the information. In my experience, it is best having the data stored on a

physical drive that is watched closely and is pulled from a workstation when not intended on being used, I.E., over night or over the weekend. Another way is by using methods of authentication. Authentication is simply proving that you are who you say you are as put by one of my instructors. This can be with an encryption key, which changes when it is given to appropriate personnel, or more commonly two-factor authentication. If that sounds familiar, that is because most services are using this to protect user data and usually consists of typing in a password and a one-time code sent over text or email.

Availability

Of course, using all this effort to protect the data, it only useful if the data is made available. Now this doesn't just mean that the data, system, or service is simply useable, but that consistent access that is availability. Availability is a very broad concept, so there are far too many measures for it to list. To summarize the kind of measures taken, most of them are redundancy of some kind (having back up systems, files, etc.) or considering environmental risks (frequent storms, blackouts, inoperable temperature, etc.). This is so there is less down time when something goes awry because with larger organizations it may mean millions to billions of dollars or even possibly lives. All three concepts must be upheld for the health of the organization.

WORKS CITED