Using the CIA and AAA Models to Explain Cybersecurity Activities

Livinus Obiora Nweke

Abstract

Cybersecurity is a broad field that is mainly concerned with protecting the confidentiality, integrity, and availability of computing devices and networks, hardware and software, and most importantly, data and information. Cybersecurity cannot be achieved through technology alone, it also involves the use of procedures, products and people. The goal of this article is to use the CIA model and AAA model to explain the activities of cybersecurity.

Keywords: Cybersecurity, CIA model, AAA models

Introduction

Cybersecurity refers to protecting the confidentiality, integrity, and availability of computing devices and networks, hardware and software, and most importantly, data and information. Cybersecurity involves times when data or information is in transit, being processed, and at rest. It is achieved through procedures, products and people. Also, it requires knowing who the attackers are, what their motivations are, where the vulnerabilities lie, and how protected the systems are. The security mindset involves thinking about how things can be made to fail. The following explains the CIA model, which refers to the three important goals of cybersecurity and the AAA model, which describes one of the methods through which the objectives of cybersecurity are achieved.

CIA Model

The CIA model describes the three important goals of cybersecurity. The C stands for confidentiality. Cybersecurity requires privacy in data and information. Certain people, devices, or processes should be permitted or restricted from seeing data, files, and items, like username, password combinations, medical records, etc. Confidentiality is concerned with viewing of data or information because if the wrong people see data or information they are not authorized, many problems could arise.

The I in the CIA model stands for integrity. Cybersecurity requires us to feel safe that data transmitted, processed, and stored has not been changed from its original form either accidentally or maliciously. For example, if one bit of a message is change, the whole message could change. Also, the whole message could be corrupted or unreadable.

For the last letter A, it stands for availability. Availability guarantees that with all the cybersecurity measures in place for dealing with hardware, software, people, processes and more, users who are authorized to do their job should be able to do so. It requires that authorized users should be able to access the resources they need to do their job with easy while ensuring that the system have full tolerance and load balancing in the event of cybersecurity incident or disaster.

AAA Model

The objectives of cybersecurity are realized using the AAA or triple-A model. The first A refers to Authentication, which is the process of proving that you are who you say you are. When you claim to be someone, that is called identification; but when you prove it, that is authentication. Authentication requires proof in one of three possible forms: something you know, like a password; something you have, like a key; something you are, like fingerprint. The combination of more than one of these categories is called multifactor authentication. Multifactor authentication makes it hard to authenticate as someone else.

The second A in the AAA model is Authorization. Authorization means providing correct level of access that a user should have based on their credentials. This is tied to the principle of least privilege, which state that users, devices, programs and processes should be granted enough permission to do their required functions and not a single drop more. Any authorization beyond the normal job function opens the door for either accidental or malicious violations of confidentiality, integrity and availability.

The last A in the AAA model is accounting, which is keeping track of what users do while they are logged into a system. Keeping track of users and their actions is very important. From a forensics perspective, tracing back to events leading up to a cybersecurity incident can prove very valuable to an investigation.

Conclusion

This article has defined the three important goals of cybersecurity referred to as the CIA model and the AAA model, which is one of the methods through which these objectives are achieved. The CIA model which stands for confidentiality, integrity and availability, describes the three important goals that must be met in cybersecurity. On the other hand, the AAA model which refers to Authentication, Authorization and Accounting, describes the methods through which the three important goals in cybersecurity can be realized.

References

Margaret Rouse (n.d). Authentication, Authorization, and Accounting (AAA). Retrieved from http://searchsecurity.techtarget.com/definition/authentication-authorization-and-accounting

Terry Chia (2010). Confidentiality, Integrity, Availability: The three components of the CIA Triad. Retrieved from http://security.blogoverflow.com/2012/08/confidentiality-integrity-availability-the-three-components-of-the-cia-triad/

About the Author

Livinus Obiora Nweke

Sapienza University
Rome, Italy

Livinus O. Nweke is currently pursuing his Master's degree in Computer Science at Sapienza University of Rome, Italy and a MicroMasters in Cybersecurity at EDx/RITx. Livinus holds a Bachelor's of Science degree in Computer Science from University of the People, Pasadena, CA, USA and a Higher National Diploma in Electrical Electronics Engineering from Institute of Management and Technology, Enugu, Nigeria. During five years of professional experience, Livinus has held titles such as Computer Consultant, Senior Technologist, IT Officer, and Customer Care/IT Support Officer.

Livinus may be contacted at nweke.1735405@studenti.uniroma1.it