An Truong
110313636

SECURITY PRINCIPLES

Introduction

CIA Triad principles and its application in information security are playing important roles as well as contributing to ensure the development of IT security in an organization. This report will demonstrate the tenet of security via CIA Triad principles, dig deeper in explaining three factors that formed CIA Triad principles and present their application in a specific case of business.

Background Information

To have an accurate approach to security principles and CIA Triad, it is essential to have an awareness of the definition of CIA Triad and the three principles.

What is CIA Triad?

Definition

CIA Triad is a venerable security model, designed as a guidelines policy for information security management that secures an organization's information system which encompasses both user computer system and data. It is important that each of the elements of a system is designed to achieve one or more of three CIA Triad principles, which makes CIA Triad a fundamental tenet of information security.

Purpose

CIA Triad is used as a core principle in any organization's security infrastructure to design a security plan by identifying problem areas and detect appropriate solutions in the arena of information security. In other words, CIA Triad is a standard principle to organizations apply to protect a network and the data within that network.

What are the three principles of the CIA Triad?

CIA Triad is an abbreviation of its three principles, namely Confidentiality, Integrity and Availability, which each will be explained its definition, how it is damaged and corresponding solutions in this section.

Confidentiality

Definition

Confidentiality is a principle designed to control the access permission to data within a system and prevent unauthorized individuals, processes, or devices disclosure. Confidentiality processes the authentication (validate the identity of data's requesting) and authorisation (limit data access to authorized users), to ensure the internal data will be accessible by authorized factors only while preventing unauthorized factors from obtaining access.

How will confidentiality be violated?

There are multiple actions that compromise Confidentiality whether be intentionally attacked by attackers or unintentionally violated by external factors.

Confidentiality violation involves accessing data or having damaging actions such as steal or tamper with the data of an organization. These attacks can happen in both logical and physical approaches, by computer trespassing or directly attacked by external factors (attackers) trying to compromise the system. A system can be attacked intentionally by designed direct attacks that allow unauthorized personnel to be able to access the system such as failing to encrypt a transmission, accessing malicious code, misconfigured security control or oversight in a security policy.

In addition, Confidentiality can also be jeopardized accidentally by human error and carelessness, oversight or inadequate security controls. This includes failure in protecting or encrypting passwords or data while in process, in transit, and in storage, issues in sharing the same user accounts, poor or lack of authentication systems and even stealing of physical equipment and storage devices.

What countermeasures can be employed to strengthen Confidentiality?

- Data classification
- Strong access controls
- Strong authentication mechanisms
- Cryptography
- Training of personnel with access to data
- Avoid the loss of physical devices and lessen human carelessness

Integrity

Definition

Integrity is the concept of maintaining the accuracy, correctness, authenticity, and reliability of data and protect data from unauthorized modifications or being inappropriately tampered with during transit, retrieval and at rest. With the concept of non-repudiation, Integrity is ensured by the process of preventing faking deny of action trading information between sender and recipients.

Perspectives of Integrity:

- Prevent unauthorized users from making modifications
- Prevent authorized users from making changes by mistakes
- Maintain consistency of data

How will Integrity be violated?

Similar to Confidentiality, multiple actions compromise Integrity directly by allowing unauthorized networks to access the system or data to launch a cyberattack, aka attack vector. This hazarding factor can be demonstrated in various methods in data system violation, such as modifying configuration files or changing system logs to evade detection.

However, Integrity is also jeopardized by unintentional factors which are human error, viruses, coding errors, malicious modifications, and backdoors. These similarities are a result of a strong dependency between Confidentiality and Integrity.

What countermeasures can be employed to strengthen Integrity?

- Encryption
- Hashing
- Input validation
- Intrusion detection systems
- Strong access controls

- Strong authentication mechanisms

Availability

Definition

Availability is the ability to uninterruptedly accessing the data and resources depending on the demand of the authorized entity that a system or organization should respond to and provide the requested information from authorized accesses. Availability depends on Confidentiality and Integrity and will be maintained by the existence of both of them.

How will Availability be violated?

By many things, mostly by external factors (not technically jeopardize)

- Hardware or software or device failure
- Power failure
- Communication interruptions
- Environmental issues
- Human error

The most well-known attack that affects availability is Denial of Service (DoS) attack, which is described as overload steam of data flow, flooding the system making it inaccessible to its intended users.

What countermeasures can be employed to strengthen Availability?

- Monitoring of performance, network traffic and network bandwidth
- Maintaining and testing backup systems
- DoS protection systems
- Designing fault-tolerant systems
- Testing access control systems

Apply CIA Triad in Business: An online education provider

Three components of CIA Triad – Confidentiality, Integrity and Availability – each has a close association with each other and co-exist to cover all possible information security of a business. In this section, each principle in three tenets of CIA Triad will be applied in the specific business, therefore, the functionality of the system will be visualized more clearly.

An online education provider is a business that provides users with a variety of online courses that are only accessible by authorized users who already had an account in the system, along with other functions including accessing users account, reviewing learning history and course payment system. All of these functions are required protection for the database of users personal details and courses payment records.

As an online education provider, the business should take and store information of students and staff, data of all courses, payment records for each account and an academic record for each student (for courses with assessments and certificates). These functions of the system underlined the importance of authentication and authorization processes in verifying the identity of users (either students or staff) and prevent academic record modification or fraud payment of any unauthorized

factors. Therefore, Confidentiality is more important than the other goals as the value of the information depends on limiting access to it, followed by Integrity and finally, Availability.

Logging functions of users and their accessibility into user account are needed to apply Confidentiality to provide access into the system only for students and staff and distinguish the privileged access to the data between students and staff, as there are differences in the range of accessible data and the API for two types of users in this system. It is necessary to meet the requirements of Confidentiality to secure the process of storing users information and proceeding with the payment of courses.

In addition, as the purpose of providing appropriate information for the right subject while accessing the system, the business uses Confidentiality to validate who is authorized for accessing the data, to such an extent that whether this individual is allowed to make modifications or not. This also applies the Integrity principle to prevent unauthorized users from making modifications (eg. non-users or students are not allowed to change the grade, only able to view) and to prevent authorized users from making unauthorized changes by mistakes. This is a direct example of the closeness of association between Confidentiality and Integrity.

Last but not least, Availability is needed to be ensured to prevent the overload while at some points, amount number of students access the system at the same time, which might rarely happen.

.

References

UniSA 2021, *Tenets of Cybersecurity*, seminar slides, INFT 5115 Security Principles, University of South Australia, delivered 28 July 2021.

BMC (n.d.). *What Is the CIA Security Triad? Confidentiality, Integrity, Availability Explained*. [online] BMC Blogs. Available at: https://www.bmc.com/blogs/cia-security-triad/.

ForcePoint (2018). *What is the CIA Triad?* [online] Forcepoint. Available at: https://www.forcepoint.com/cyber-edu/cia-triad.

Henderson, A. (2017). *The CIA Triad: Confidentiality, Integrity, Availability - Panmore Institute*. [online] Panmore Institute. Available at: http://panmore.com/the-cia-triad-confidentiality-integrity-availability.

SecurityInfoWatch (n.d.). *StackPath*. [online] www.securityinfowatch.com. Available at: https://www.securityinfowatch.com/home/article/10538077/what-is-a-security-infrastructure [Accessed 12 Aug. 2021].

Upguard (n.d.). *What is an Attack Vector? Common Attack Vectors*. [online] www.upguard.com. Available at: https://www.upguard.com/blog/attack-vector.

Walkowski, D. (2019). *What Is The CIA Triad?* [online] F5 Labs. Available at: https://www.f5.com/labs/articles/education/what-is-the-cia-triad.

Weber, M. (2019). *The CIA Triad - Confidentiality, Integrity, and Availability | inversegravity.net*. [online] Maximilian Weber. Available at: https://inversegravity.net/2019/cia-triad/.

Table of Contents