TASK 1: Exploring the CIA Triad in Real-world scenarios

CIA triad is expansion of Confidentiality, Integrity, and availability. It is also known as heart of information security. Which are the three core principles that guide the development and implementation of security measures. These principles are essential for protecting sensitive information and ensuring systems operate securely.

Here is the breakdown for CIA Triad :

Confidentiality: Confidentiality is the property that information is not made available to unauthorized individuals, entities, or processes. While similar to "privacy" the two words are not interchangeable. Rather, confidentiality is a component of privacy that implements to protect our data from unauthorized viewers.

Examples: confidentiality of electronic data being compromised include laptop theft, password theft, or sensitive emails being sent to the incorrect individuals.

Integrity: integrity is an information security principle that involves human/social, process, and commercial integrity, as well as data integrity. As such it touches on aspects such as credibility, consistency, truthfulness, completeness, accuracy, timeliness, and assurance.

Examples: It uses digital signatures to verify the source and authenticity of data, hashing to detect changes, and implementing access controls and audit trails to track data access and modifications.

Availability: Availability in the CIA Triad entails that the authorized users can utilize data, systems and services at the time they require without such delays and un-needed downtimes.

Examples: cloud storage service, Banking systems, E- commerce websites, hospital patients records, etc,.

1. WhatsApp

Confidentiality -End-iosse encryption such that the message is only available to sender and receiver, device-based authentication methods and biometric lockers (fingerprint/face unlock) can be applied to that end.

Integrity- message authentication codes (MAC) protect against modification of messages in transit and encryption of backups prevents malicious modification, and the safety notifications warn the user when the security code of a contact is changed.

Availability - The use of cloud-based infrastructure, a large number of regional servers, load balancing to control heavy traffic, and backup SMS-based verification to ensure communication availability.

1. Online Booking System of Airline.

Confidentiality: It is confidential in the sense that the information about payments is encrypted by PCI DSS standard, confirmation of bookings requires OTP (One-Time Password), it restricts access to the passenger information so that employees can have the data of the passengers.

Integrity: Integrity uses synchronized databases to ensure schedule accuracy and applies the concept of digital signatures to e-tickets and log the transactions, to prevent manipulation of bookings.

Availability: Supplements its booking servers, does not rely on single payment gateways and has a backup recovery plan in place to ensure its business keeps operating even when the peak season set in.

1. USMS- University Student Management System

Confidentiality: Role-based access allowing only authorized personnel to access or modify student records, encrypts personal and academic information during data storage and data transmission, and implements solid passwords policies.

Integrity: Versioned academic record, audit logging of grade or attendance changes, checksums of uploaded files.

Availability- High-availability cloud hosting, MS SQL database back-ups on a regular basis and failover servers to maintain portals up through the examination and registration periods.

**How Linux file permission works:**

In linux every directory has three types of permissions

1. Read (r)
2. write (w)
3. execute (x)

There are three types of users:

1. owner (u) – owns the file
2. group (g) – other users in the same group
3. others (o) – all other users

rw- 🡪 owner can read/write

r-- 🡪 group can only read

--- 🡪 others have no access