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

CIA Triad stands for confidentiality, integrity and availability. It is a basic model for development of security systems. Each point has its focal points with that security team can address concerns in different ways. This model is used for finding vulnerabilities and methods for identifying solution.

**Confidentiality**- Protecting the data from unauthorized access, this can be done by giving necessary privileges of accessing data to people within an organization. It is archived through encryption, authorized base access and secure authentication.

**Integrity**- It ensures the data is reliable, confidential and protected from unauthorized changes.

**Availability**- It ensures users get accessed to information and system in timely and reliably whenever they need. This shows the redundancy, backup and disaster recovery for an organization.

1.Gmail

* Confidentiality- It uses TLS (Transport Layer Security) encryption for data transit to prevent eavesdropping, all mails stored in encrypted google servers, it uses MFA to provide access, whenever a new login attempts it sends alert to account.
* Integrity- Digital signature and hashing ensures content is not changed, spam and phishing detection prevents malicious messages, secure protocols like SMTP with STARTTLS, IMAP over SSL ensures message authenticity.
* Availability- Redundance data centres, balancing load and backup to prevent down time, disaster recovery and failover mechanisms for continues access.

2. Online Banking APP

* Confidentiality- End-to-end encryption for financial transitions, MFA for account access, session timeout to reduce risk if device is unattended.
* Integrity- Transaction validation, digital certificates to prevent MIMA attack, audit logs to track all account actions.
* Availability- 24/7 online service, DDoS protection to keep the app accessible, backup and recovery-management when sever failure.

3. Hospital Electronic Health Record System

* Confidentiality- Access privilege to authorized users based on role, encrypted data for storage and data transfer, HIPAA regulation compliance to protect patient privacy.
* Integrity- Digital signatures and checksums to ensure data is not altered, audit logs for every action, regular verification and validation of data entries by medical staff.
* Availability- High availability servers, emergency access mode, regular backups to recover server failures.

**How Linux file permission works:**

Linux has owner, group and others for every file and directory.

Owner- person who created file

Group- file permissions are shared between multiple users

Others- remaining users in the system

It has 3 types of permissions

r- read

w- write

x- execute

rwx: owner can read, write, execute

r-x: group can read and execute but cannot write

---: other have no access