Security Concepts

CIA Traid are three main goals

Confidentiality

- Confidentiality protects information from unauthorized disclosure.

Confidentiality_Concerns

1. Snooping
   - snooping gathering information that is left out in the open.
   - "Clean desk policies" protect against snooping.
2. Dumpster Diving
   - Dumpster diving is to dump data anywere or dustbin.
   - "Shedding" protects against dumpster diving.
3. Eavesdropping
   - listing sensitive information
   - "Rules about sensitive conversations" prevent eavesdropping
4. Wiretapping
   - Electronic evaesdropping - listing through wire(internet)
   - "Encryption" protects against Wiretapping
5. Social Engineering
   - The attacker uses psychological tricks to persuade an employee to give then sensitive information or access to internal systems.
   - Best defence is to "Educating users"

Integrity

- Integrity protects information from unauthorized changes. #### Integrity_Concerns

1. Unauthorized modification
   - Attacks make changes without permission.
   - "Least priviege" protects against integrity attacks
2. Impersonation
   - Attacks pretend to be someone else
   - "User education" protects against attacks
3. Man-in-the-middle (MITM)
   - Attacks place the attacker in the middle of a communications session.
   - "Encryption" protects against MITM attacks
4. Replay
   - Attacks eavesdrop on logins and reuse the captured credentials.
   - "Encryption" protects against Replay attacks

Availability

- Availability protects authorized access to systems and data. #### Availability_Concerns

1. Denial of service (DoS)
    - Unlimited request to a server
    - "Block unauthorized connections" to protect against denial of service attacks.
2. Power outages
    - Naturally or Man-made
    - "Redundant power and generators" protect against power outages.
3. Hardware failures
    - any component failures
    - "Redundant components" protect against hardware failure
4. Destruction
    - Naturally or Man-made
    - "Backup data centers" protect against destruction.
5. Service outages
    - Programing error and the failure of underlying equipment.
    - building systems that are resilient in the face of errors and hardware failures.

Authentication and authorization

The access control process consists of three steps that you must understand. These steps are identification, authentication and authorization.

1. Identification incolves making a claim of identity.
    - Electronic identification commonly uses usernames
2. Authentication requires proving a claim of identity.
    - Electronic autherntication commonly uses passwords.
3. Authorization ensures that an action is allowed.
    - Electronic authorization commonly uses access control lists.

Authentication and authorization process, access control systems also provide "Accounting" functionality that allows administrators to track user activity and reconstruct that activity from logs. This may include tracking user activity on systems and even logging user web browsing history.

Password security

Password mechanisms - Password length requirements set a minimum number of characters. - Password complexity requirements describe the types of characters that must be included. - Password expiration requirements force password changes. - Password requirements prevent password reuse.

Multifactor authentication

Multifactor authentication combines two different authentication factors.

Three different authentication factors. Something you know, something you are and something you have.

something you know

- Passwords, PIN's, Security questions. #### something you are
- Biometric security mechanisms. #### something you have
- Software and hardware tokens.

single sign-On (SSO) Shares authentiacated sessions across systems - In a single sign on approach, users log on to the first SSO enabled system that they encounter. And then that login session persists across other systems until it expires. If the organization sets the expiration period to be the length of a business day, that means that users will only need to log in once a day and their single sign on is then going to last the entire day.

Non-repudiation

Non-repudiation prevents someone from denying the truth.

Solved the issue with 1. Signed contracts 2. Digital signatures 3. Video surveillance

Privacy

Privacy Concerns 1. Protecting our own data. 2. Educating our users. 3. Protecing data collected by our organizations.

Private information may come in many forms. Two of the most common elements of private information are "Personally identifiable information" and "Protected health information". 1. Personally identifiable information, or PII, includes all information that can be tied back to a specific individual. 2. Protected health information, or PHI, includes healthcare records that are regulated under the Health Insurance Portability and Accountability Act. Otherwise known as HIPAA.