Security mechanisms

What are security mechanisms?

Security mechanisms are **technical tools and techniques that are used to implement security services**. A mechanism might operate by itself, or with others, to provide a particular service – IBM 27/01/2023

Examples of security mechanisms are:

* Authentication
* Authorisation
* Auditing
* Confidentiality
* Data integrity

# Authentication:

Authentication is the process of determining if someone or something is who or what they claim to be. Passwords are the default method of authentication and are used for almost everything, however they have multiple flaws. Due to them being so common most people repeat a pattern when deciding on a password or they use the same password entirely. Other more secure means of authentication are: Face ID, fingerprint scans, retina scans, access cards and voice recognition.

# Authorisation:

Authorisation is granting a system entity access to a system resource - CSRC. Different people within an organisation will have different levels of authority, therefore allowing them access to certain parts of the business. Without authorisation data will be very vulnerable to breaches and unauthorised access.

# Auditing:

A cyber security audit is **a comprehensive review of an organisation's IT infrastructure**. Audits ensure that appropriate policies and procedures have been implemented and are working effectively. The goal is to identify any vulnerabilities that could result in a data breach – IT governance 17/05/2022. A regular audit can expose new weaknesses in the infrastructure, once delt with breaches can be prevented keeping data secure.

# Confidentiality: The term 'confidentiality' means **preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information** – CSRC. Confidentiality is very important so data isn’t easily accessed. It reduces the chance of someone accidentally releasing information (social engineering) or being hacked.

# Data integrity:

Data integrity is the overall accuracy, completeness, and consistency of data. Data integrity also refers to the safety of data in regard to regulatory compliance and security – Talend. This is important to prevent a data leak or loss. Authorisation and Authentication play a big part in who can access and change what data. This is to minimise any errors when dealing with data which could lead to a data breach.