Security and Privacy Basics

Data Security and Privacy @ uninsubria

Roberto Vicario

2024/2025

Contents

1 Data Security

Data security is the practice of protecting digital information from unauthorized access, corruption, or theft throughout its entire lifecycle. It involves implementing measures to safeguard data from breaches, loss, or damage, ensuring that sensitive information remains confidential and secure.

1.1 CIA Triad

The *CIA triad* is a widely used model that guides organizations in their data security practices. It consists of three core principles:

- **Confidentiality:** Ensuring that sensitive information is accessed only by authorized individuals. This can be achieved through encryption, access controls, and authentication mechanisms.
- **Integrity:** Maintaining the accuracy and consistency of data over its lifecycle. This involves protecting data from unauthorized modifications and ensuring that it remains reliable and trustworthy.
- **Availability:** Ensuring that data is accessible to authorized users when needed. This includes implementing measures to prevent downtime, such as redundancy, backups, and disaster recovery plans.

1.2 Threats

Threat	Description
Physical Threats	Risks to data security that arise from physical damage or theft of hardware, such as servers, laptops, or storage devices.
Malware	Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems. Examples include viruses, worms, and ransomware.
Insider Threats	Employees or contractors who misuse their access to sensitive data for malicious purposes, either intentionally or unintentionally.
Denial of Service (DoS) Attacks	Attacks that aim to make a system or network unavailable by overwhelming it with traffic or requests, rendering it inaccessible to legitimate users.
Human Error	Mistakes made by individuals that can lead to data breaches or loss, such as accidentally sending sensitive information to the wrong recipient or misconfiguring security settings.

1.3 Measures

Measure	Description
Encryption	Secures data by converting it into a format readable only with a decryption key, protecting it during transfer and storage.
Access Controls	Restrict access to sensitive data using authentication and authorization methods like strong passwords and multi-factor authentication.
Firewalls	Devices that filter network traffic to block unauthorized access and attacks.

Measure	Description
Incident Response	Plans to identify, contain, notify, and prevent future data breaches or security incidents.
Backup and Recovery	Regular backups ensure data restoration in case of loss or corruption, minimizing downtime during incidents.

2 Data Privacy

Data privacy, also known as information privacy, refers to the proper handling, processing, storage, and usage of personal data. It involves ensuring that individuals have control over their personal information and that organizations respect their privacy rights.

2.1 Human Privacy

Human privacy is a fundamental human right that encompasses the right to control one's personal information and the right to be free from unwarranted intrusion into one's private life. It is essential for maintaining individual dignity, autonomy, and freedom.

2.2 Data Security vs. Data Privacy

Aspect	Data Security	Data Privacy
Definition	Protects data from unauthorized access, corruption, or theft.	Ensures proper handling and usage of personal data.
Scope	Involves technical measures and controls.	Involves policies, practices, and regulations.
Goal	Ensures confidentiality, integrity, and availability of data.	Ensures individuals' rights to control their personal information.
Focus	Emphasizes risk management and threat mitigation.	Emphasizes individual rights and consent.