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.

1.1.1 Security Controls

Control	Description
Physical Controls	Security measures that protect physical assets, such as access controls, surveillance cameras, and secure storage facilities.
Access Controls	Mechanisms that restrict access to sensitive data and systems, ensuring that only authorized users can view or modify information.
Procedural Controls	Policies and procedures that govern how data is handled, processed, and stored.
Technical Controls	Software and hardware solutions that protect data, such as firewalls, encryption, and intrusion detection systems.

Control	Description
Compliance Controls	Adherence to legal and regulatory requirements related to data security, such as GDPR, HIPAA, or PCI DSS.

1.2 Risk Management

Risk management is the process of identifying, assessing, and mitigating risks associated with data security. It involves evaluating potential threats and vulnerabilities, determining their impact on the organization, and implementing measures to reduce or eliminate those risks.

1.2.1 Types of Risks

Type	Description
Malware	Malicious software designed to disrupt, damage, or gain unauthorized access to computer systems.
Phishing	A social engineering attack that tricks individuals into revealing sensitive information, such as passwords or credit card numbers, by posing as a trustworthy entity.
Denial of Service (DoS) Attacks	DoS attacks overwhelm a target's resources, rendering it unavailable to users. This is often achieved by flooding the target with excessive traffic from multiple sources.
Social Engineering	Manipulating individuals into divulging confidential information or performing actions that compromise security. This can include tactics such as impersonation, pretexting, or baiting.

Type	Description
SQL Injection	A code injection technique that exploits vulnerabilities in web applications by inserting malicious SQL queries into input fields. This can lead to unauthorized access to databases and sensitive information.

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 Governance, Risk, and Compliance (GRC)

Governance, Risk, and Compliance (GRC) is a framework that helps organizations manage their data privacy practices. It involves establishing policies, procedures, and controls to ensure compliance with legal and regulatory requirements while effectively managing risks associated with data privacy.

2.2 Audit Management

Audit management is the process of planning, conducting, and reporting on audits related to data privacy and security. It involves evaluating the effectiveness of an organization's data protection practices, identifying areas for improvement, and ensuring compliance with relevant regulations.

2.2.1 Types of Audits

Type	Description
Internal Audit	Conducted by an organization's internal team to assess compliance with policies and procedures.

Type	Description
External Audit	Conducted by third-party auditors to evaluate compliance with legal and regulatory requirements.
Third-Party Audit	Evaluates the data protection practices of vendors or partners to ensure they meet the organization’s security and privacy standards.

2.3 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.