**Security Concepts**

|  |  |
| --- | --- |
| **Security Triad** | **Description** |
| Availability | Refers to the property of being accessible and usable upon request by an authorized entity. |
| Authenticity | Refers to the property of being genuine and trustworthy. It ensures that data is not tampered with or altered. |
| Confidentiality | Refers to the property of being private and kept secret. It ensures that data is only accessible to authorized entities. |
| Non- repudiation | is a security concept that ensures that an individual or entity cannot deny having taken a particular action. In the context of digital communication, it means that the sender of a message cannot later deny having sent it, and the recipient of a message cannot deny having received it. |

# **Authentication**

Here we have some examples of common methods of authentication:

**Something you know**: Password or paraphrases (The most insercurity auth method)

**Something you have**: Tokens, memory cards, smart cards;

**Something you are**: Biometrics, measurable characteristics, fingerprints, voice, iris patterns;

# **Methods of Authentication**

Two types of authentication methods:

**Single-factor authentication (SFA)**: Single-factor authentication (SFA) is a security process that requires users to provide only one type of identification method to verify their identity.

**Multi-factor authentication (MFA)**: requires users to provide multiple forms of identification to verify their identity, adding an extra layer of security to the authentication process.

**Security Controls**

|  |  |  |
| --- | --- | --- |
| **Concept** | **Definition** | **Examples** |
| Physical Controls | Controls that are tangible and focus on securing physical assets and resources. | Security cameras, locks, fencing, biometric authentication, security guards |
| Administrative Controls | Controls that focus on policies, procedures, and regulations to protect assets and resources. | Security training, access control policies, security audits, incident response planning |
| Logical Controls | Controls that use software, data, and technology to protect assets and resources. | Firewalls, intrusion detection systems, encryption, antivirus software, network access control |

**Governance Elements**

|  |  |  |
| --- | --- | --- |
| **Governance Elements** | **Explanation** | **Examples** |
| Laws and Regulations | **Legal requirements** established by governments or regulatory bodies that organizations must comply with. | Traffic laws and regulations on the road, General Data Protection Regulation (GDPR), Health Insurance Portability and Accountability Act (HIPAA) |
| Standards | Industry-specific **guidelines and best practices** that organizations can use to improve their security posture. | Building codes for construction, e International Organization for Standardization (ISO), National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS) |
| Policies | High-level statements that **define the objectives and principles** of an organization's security program | Company code of conduct or employee handbook |
| Procedures | **Step-by-step instructions** for implementing security controls | Emergency response plans for natural disasters |

**Risk Management concepts**

|  |  |
| --- | --- |
| **Concept** | **Definition** |
| Assets | Resources that an organization needs to protect, such as data, hardware, software, and personnel. |
| Vulnerability | Weaknesses or flaws in the security systems, processes, or technology that can be exploited by threat actors. |
| Risk | The potential loss or damage that an organization could face due to a security incident. |
| Likelihood | The probability of a threat exploiting a vulnerability. |
| Impact | The magnitude of harm that a security incident could cause to an organization, including financial, reputational, and legal. |

# **Identify risk**

**Employees at all levels** of the organization are responsible for **identifying risk**. Identify risk to communicate it clearly.

Identify risk to protect against it.

# **Risk treatment**

|  |  |
| --- | --- |
| **Risk Treatment** | **Definition** |
| Avoidance | The organization decides not to engage in an activity that could result in a risk. |
| Acceptance | The organization acknowledges the risk but decides not to take any action to treat it. |
| Mitigation | The organization implements controls to reduce the likelihood or impact of the risk. |
| Transfer | The organization transfers the risk to another entity, typically through insurance or outsourcing. |