**Security Control**

**A control** is a safeguard or countermeasure designed to preserve Confidentiality, Integrity and Availability of data.

# **Overview**

|  |  |
| --- | --- |
| **Concept** | **Description** |
| Subject | Refers to an agent or entity that can access resources |
| Object | Refers to the resource being protected |
| Rules | Are rules that specify how subjects can access objects and what they can do with them. Rules may be based on specific security policies and restrictions. |

**Reviewing**

We will talk about the types of acess controls: Physical, Logical and Administrative. So, let's review this concepts:

|  |  |  |
| --- | --- | --- |
| **Layer** | **Description** | **Real-world analogy** |
| Physical Controls | Refers to tangible security measures, such as gates, fences, security cameras, and locks. | A locked door or a fence around a property |
| Logical/Technical Controls | Refers to technical measures, such as firewalls, intrusion detection systems, and access controls. | A security system in a building |
| Administrative Controls | Refers to policies, procedures, and guidelines that define how security is managed and enforced. Examples include security training, background checks, and security audits. | The security policies and procedures of a company or organization. |

## **Physical Controls:**

**Badge Systems and Gate Entry Environmental Design Biometrics**

## **Logical/Technical Controls:**

**Passwords**

**Biometrics (implemented on a system, such as a smartphone or laptop) Badge/token readers connected to a system**

|  |  |  |
| --- | --- | --- |
| **Concept** | **Description** | **Example** |
| Discretionary Access Control (DAC) | A type of access control where the owner of a resource decides who is allowed  to access that resource. | An example of DAC in real life could be a person owning a private Instagram account and deciding who is allowed to follow them and see their posts. |
| Mandatory Access Control (MAC) | A type of access control where access to a resource is determined by the system rather than the owner. | An example of MAC in real life could be a government agency using a classified computer system where access is based on a set of rules that define who is allowed to access the system and the level of clearance they have. |
| Role-Based Access Control (RBAC) | A type of access control where access to resources is based  on the role a user plays within an organization. | An example of RBAC in real life could be a company using a system where access to certain files and data is restricted based on an employee's job title and responsibilities. For instance, a marketing employee may have access to the company's social media accounts, while a financial employee may have access to the accounting software. |

**Terms and definitions**

|  |  |
| --- | --- |
| **Definition** | **Terms** |
| Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures. NIST SP 1800-15B | Audit |
| An architectural approach to the design of buildings and spaces which emphasizes passive features to reduce the likelihood of criminal activity. | Crime Prevention through Environmental Design (CPTED) |
| Information security strategy integrating people, technology, and operations capabilities to establish variable barriers across multiple layers and missions of the organization. Source: NIST SP 800-53 Rev 4 | Defense in Depth |
| A certain amount of access control is left to the discretion of the object's owner, or anyone else who is authorized to control the object's access.  The owner can determine who should have access rights to an object and what those rights should be. NIST SP 800-192 | Discretionary Access Control (DAC) |
| To protect private information by putting it into a form that can only be read by people who have permission to do so. | Encrypt |
| Devices that enforce administrative security policies by filtering incoming traffic based on a set of rules. | Firewalls |
| An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. | Insider Threat |
| An operating system manufactured by Apple Inc. Used for mobile devices. | iOS |
| The use of multiple controls arranged in series to provide several consecutive controls to protect an asset; also called defense in depth. | Layered Defense |
| An operating system that is open source, making its source code legally available to end users. | Linux |
| A system irregularity that is identified when studying log entries which could represent events of interest for further surveillance. | Log Anomaly |
| Collecting and storing user activities in a log, which is a record of the events occurring within an organization's systems and networks. NIST SP 1800-25B. | logging |

|  |  |
| --- | --- |
| **Definition** | **Terms** |
| An automated system that controls an individual's ability to access one or more computer system resources, such as a workstation, network, application or database. A logical access control system requires the validation of an individual's identity through some mechanism, such as a PIN, card, biometric or other token. It has the capability to assign different access privileges to different individuals depending on their roles and responsibilities in an organization. | Logical Access Control Systems |
| Access control that requires the system itself to manage access controls in accordance with the organization's security policies. | Mandatory Access Control |
| An entrance to a building or an area that requires people to pass through two doors with only one door opened at a time. | Mantrap |
| Passive information system-related entity (e.g., devices, files, records, tables, processes, programs, domains) containing or receiving information. Access to an object (by a subject) implies access to the information it contains. | Object |
| Controls implemented through a tangible mechanism. Examples include walls, fences, guards, locks, etc. In modern organizations, many physical control systems are linked to technical/logical systems, such as badge readers connected to door locks. | Physical Access Controls |
| The principle that users and programs should have only the minimum privileges necessary to complete their tasks. | Principle of Least Privilege |
| An information system account with approved authorizations of a privileged user. | Privileged Account |
| A type of malicious software that locks the computer screen or files, thus preventing or limiting a user from accessing their system and data until money is paid. | Ransomware |
| An access control system that sets up user permissions based on roles. | Role-based access control (RBAC) |
| An instruction developed to allow or deny access to a system by comparing the validated identity of the subject to an access control list. | Rule |
| The practice of ensuring that an organizational process cannot be completed by a single person; forces collusion as a means to reduce insider threats. Also commonly known as Separation of Duties. | Segregation of Duties |
| Generally an individual, process or device causing information to flow among objects or change to the system state. | Subject |

|  |  |
| --- | --- |
| **Definition** | **Terms** |
| The security controls (i.e., safeguards or countermeasures) for an information system that are primarily implemented and executed by the information system through mechanisms contained in the hardware, software or firmware components of the system. | Technical Controls |
| A one-way spinning door or barrier that allows only one person at a time to enter a building or pass through an area. | Turnstile |
| An operating system used in software development. | Unix |
| The process of creating, maintaining and deactivating user identities on a system. | User Provisioning |