SEPTEMBER 2023

Report

PRIVATE SECURITY ANALYSIS

ACCESS CONTROL

It is a method that allows ensuring that users are who they say they are. It's like when you have to show your identification document somewhere to verify that you indeed have that identity. Access control is extremely important so that all users have the appropriate access to data and system resources. Now, what does access control specifically consist of? Above all, it's a series of restrictions that are applied according to the data and/or resources you want to access. It is based on authentication and authorization processes.

When we talk about authentication, we refer to the entry of credentials or the use of one or more authentication methods. On the other hand, authorization is the subsequent step to authentication, which is granting access to a specific group of resources and data. RedesZone has made available a guide that details the differences between authentication and authorization. You can even learn about the most used methods for each case.

BASIC PRINCIPLES

The three basic principles that govern access control and security are identification, authentication, and authorization. Down below, we'll see what each of them entails.

1. Identification

The first step is the identification of the user or worker. There are various methods to identify a person, such as fingerprints, identification cards, or voice recognition, among many others.

2. Authentication

The next principle is authentication. Based on these systems, it is determined whether the person attempting access is in the database and has the necessary permissions. In other words, it involves verifying the user's identity.

3. Authorization

Once the system has identified and verified the user's identity, it proceeds (or not) to authorize their access to the facilities or computer systems. Authorization is often limited to specific resources or facilities. For example, in workplace access control, entry to the warehouse may be restricted to warehouse operators or carriers.

ACCESS CONTROL OBJECTIVES

- Restricting or allowing access to specific areas or departments in a facility.
- Restricting or allowing access to computer systems, databases and other information services.
- Protecting physical assets, equipment, or organization´s data from theft or unauthorized access by third parties.
- Detecting unauthorized access and implementing mechanisms to prevent it.
- Recording and reviewing critical events carried out by users in the systems.
- Easing company organization and employee control.

ACCESS CONTROL BENEFITS

They are a completely necessary measure in any company. This helps ensure the security and privacy of the company's information. These controls can restrict access to systems and data that can be very sensitive to unauthorized individuals, significantly reducing the risk of security breaches or leaks.

Some of them are:

Understanding security requirements: Knowing what the security requirements of the system are is the first step in designing an access control framework. This helps us establish the appropriate permissions. In this field, it includes identifying sensitive data, determining who will have access, and establishing different procedures to manage and protect all information.

Maintaining password security: Passwords are a very common form of authentication for various services. However, it is crucial to establish security rules for passwords, which may include a minimum number of characters, variety, or a frequency for changing them periodically.

Compliance with necessary standards: Nowadays, we have laws that directly address data handling and how it will be used. With such regulation in place, companies are obligated to take appropriate security measures to strictly meet all security requirements. In our case, both at the national and european level.

Remote access management: The growing trend of remote work has made necessary to carry out centralized management in this aspect. Therefore, it is always important to periodically review access to all systems and data that may be sensitive.

Monitoring and audits: Keeping systems under monitoring and conducting regular audits helps us stay prepared for almost any issues that may arise. Preventing problems is the best way to avoid them.