SEPTEMBRE 2023

3+ Report

ANALYSE DE LA SÉCURITÉ PRIVÉE

CONTRÔLE D'ACCÈS

Il s'agit d'une méthode qui permet de s'assurer que les utilisateurs sont bien ceux qu'ils prétendent être. C'est comme lorsque vous devez montrer votre document d'identité quelque part pour vérifier que vous avez bien cette identité. Le contrôle d'accès est extrêmement important pour que tous les utilisateurs aient un accès approprié aux données et aux ressources du système. En quoi consiste concrètement le contrôle d'accès ? Il s'agit avant tout d'une série de restrictions appliquées en fonction des données et/ou des ressources auxquelles vous souhaitez accéder. Il repose sur des processus d'authentification et d'autorisation.

Lorsque nous parlons d'authentification, nous nous référons à l'entrée d'informations d'identification ou à l'utilisation d'une ou plusieurs méthodes d'authentification. En revanche, l'autorisation est l'étape qui suit l'authentification et qui consiste à accorder l'accès à un groupe spécifique de ressources et de données. RedesZone a mis à disposition un guide qui détaille les différences entre l'authentification et l'autorisation. Vous pouvez même y découvrir les méthodes les plus utilisées dans chaque cas.

PRINCIPES FONDAMENTAUX

Les trois principes de base qui régissent le contrôle d'accès et la sécurité sont l'identification, l'authentification et l'autorisation. Nous verrons ci-dessous ce que chacun d'entre eux implique.

1. Identification

La première étape est l'identification de l'utilisateur ou du travailleur. Il existe différentes méthodes pour identifier une personne, telles que les empreintes digitales, les cartes d'identification ou la reconnaissance vocale, entre autres.

2. Authentification

Le principe suivant est l'authentification. Sur la base de ces systèmes, on détermine si la personne qui tente d'accéder à l'information figure dans la base de données et si elle dispose des autorisations nécessaires. En d'autres termes, il s'agit de vérifier l'identité de l'utilisateur.

3. Autorisation

Une fois que le système a identifié et vérifié l'identité de l'utilisateur, il procède (ou non) à l'autorisation de son accès aux installations ou aux systèmes informatiques. L'autorisation est souvent limitée à des ressources ou à des installations spécifiques. Par exemple, dans le cadre du contrôle d'accès sur le lieu de travail, l'accès à l'entrepôt peut être limité aux opérateurs de l'entrepôt ou aux transporteurs.

LES OBJECTIFS DU CONTRÔLE D'ACCÈS

- Restreindre ou autoriser l'accès à des zones ou à des départements spécifiques d'un établissement.
- Protéger les biens physiques, l'équipement ou les données de l'organisation contre le vol ou l'accès non autorisé par des tiers.
- L'enregistrement et l'examen des événements critiques effectués par les utilisateurs dans les systèmes.
- Restreindre ou autoriser l'accès aux systèmes informatiques, aux bases de données et à d'autres services d'information.
- Détecter les accès non autorisés et mettre en œuvre des mécanismes pour les empêcher.
- Faciliter l'organisation de l'entreprise et le contrôle des salariés.

LES AVANTAGES DU CONTRÔLE D'ACCÈS

Il s'agit d'une mesure tout à fait nécessaire dans toute entreprise. Elles permettent de garantir la sécurité et la confidentialité des informations de l'entreprise. Ces contrôles peuvent restreindre l'accès aux systèmes et aux données qui peuvent être très sensibles pour les personnes non autorisées, ce qui réduit considérablement le risque de failles de sécurité ou de fuites.

En voici quelques-unes :

- **Comprendre les exigences de sécurité :** Connaître les exigences de sécurité du système est la première étape de la conception d'un cadre de contrôle d'accès. Cela nous aide à établir les autorisations appropriées. Dans ce domaine, il s'agit d'identifier les données sensibles, de déterminer qui y aura accès et d'établir différentes procédures pour gérer et protéger toutes les informations.
- **Maintenir la sécurité des mots de passe :** Les mots de passe sont une forme très courante d'authentification pour divers services. Cependant, il est essentiel d'établir des règles de sécurité pour les mots de passe, qui peuvent inclure un nombre minimum de caractères, une variété ou une fréquence de changement périodique.
- **Respect des normes nécessaires :** Aujourd'hui, nous disposons de lois qui traitent directement du traitement des données et de la manière dont elles seront utilisées. Avec une telle réglementation en place, les entreprises sont obligées de prendre des mesures de sécurité appropriées pour répondre strictement à toutes les exigences en matière de sécurité. Dans notre cas, il s'agit d'exigences nationales et européennes.
- **Gestion de l'accès à distance :** La tendance croissante au travail à distance a rendu nécessaire une gestion centralisée de cet aspect. Par conséquent, il est toujours important de revoir périodiquement l'accès à tous les systèmes et à toutes les données qui peuvent être sensibles.
- **Contrôle et audits :** Le fait de surveiller les systèmes et d'effectuer des audits réguliers nous aide à rester prêts à faire face à presque tous les problèmes qui peuvent survenir. Prévenir les problèmes est le meilleur moyen de les éviter.