Cybersécurité
Les contrôles d'accès

L'objectif est de contrôler qui peut accéder aux données, systèmes, ressources et ce qu'il peut en faire.

1 – Les contrôles d'accès physiques

L'objectif est d'empêcher des utilisateurs non autorisés d'accéder physiquement aux sites, aux équipements et aux autres ressources de l'entreprise. **Voir chapitre précédent.**

2 – Les contrôles d'accès logiques

Les contrôles d'accès logiques désignent les solutions matérielles et logicielles utilisées pour gérer l'accès aux ressources et aux systèmes.

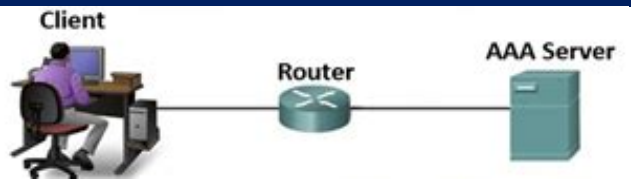
Exemples de contrôle d'accès logique :

- Le chiffrement, les cartes à puce, les mots de passe, la biométrie.
- Les listes de contrôle d'accès (ACL) définissent le type de trafic autorisé sur un réseau.
- Le pare-feu bloque le trafic indésirable.
- Les systèmes de détection d'intrusion (IDS) qui surveillent les activités suspectes sur un réseau.

3 - Les contrôles administratifs AAA

Le contrôle d'accès administratif (AAA) fait intervenir trois services de sécurité :

- **A**uthentification,
- **A**utorisation
- Traçabilité (**A**ccounting).



1 - Authentification = vérifier l'identité de l'utilisateur

L'authentification vérifie l'identité de chaque utilisateur, afin d'empêcher tout accès non autorisé. Les utilisateurs doivent vérifier leur identité en fournissant l'un des éléments suivants :

- Mot de passe - Carte RFID - Biométrie - MFA (double facteur)

2 – Autorisation = définir les droits

Les services d'autorisation déterminent les ressources auxquelles les utilisateurs peuvent accéder et les opérations qu'ils peuvent effectuer : accès aux fichiers, horaires, modifier, supprimer, etc.

3 - Traçabilité (Accounting) = enregistrer les actions

Consiste à suivre les activités des utilisateurs : log, connexions, etc.

Les modèles de contrôle d'accès

En cybersécurité, les modèles de contrôle d'accès déterminent comment les ressources et les informations sont accessibles par les utilisateurs ou les systèmes.

DAC : Contrôle d'accès discrétionnaire (le moins restrictif)

Le propriétaire des ressources a le contrôle total sur qui peut accéder à ses ressources. Les permissions sont définies par les utilisateurs eux-mêmes.

MAC : Contrôle d'accès obligatoire (le plus strict)

Il est généralement utilisé dans des applications essentielles ou militaires. Les permissions sont définies par une autorité centrale et non par les utilisateurs individuels.

RBAC : Contrôle d'accès basé sur les rôles ou contrôle d'accès non discrétionnaire (le plus utilisé)
Les permissions sont attribuées en fonction des rôles des utilisateurs (admin, employé, consultant, etc).

ABAC : Contrôle d'accès basé sur les attributs
Autorise l'accès en fonction des attributs des ressources auquel vous essayez d'accéder, de l'utilisateur qui accède aux ressources et de facteurs environnementaux (date, heure, emplacement géographique, etc).

Gestion des identités

Identité fédérée (OAuth)= un seul mot de passe pour tout **Cette méthode d'identification est à proscrire !**
Une identité fédérée relie l'identité électronique d'un utilisateur à des systèmes de gestion des identités distincts, ce qui lui permet par exemple d'accéder à plusieurs sites web à l'aide des mêmes identifiants de connexion aux réseaux sociaux (google, Facebook, …).

Solution d'authentification unique (SSO) permet à l'utilisateur d'utiliser un seul ensemble d'informations d'identification pour s'authentifier sur plusieurs applications. Ainsi, l'utilisateur n'a besoin de retenir qu'un seul mot de passe fort (ATRIUM, ...).

C**offre-fort de mots de passe** : il permet de protéger et stocker les informations d'identification de l'utilisateur avec un seul mot de passe fort requis pour y accéder.

Authentification basée sur les connaissances (KBA) pour réinitialiser le mot de passe si un utilisateur oublie son mot de passe. KBA repose sur des informations personnelles : ville de naissance, première voiture, etc.

Le hachage HMAC - Hash-based Message Authentication Code

Remarque
Une fonction de hachage est un algorithme qui prend en entrée des données (appelées message) et produit une sortie de longueur fixe, généralement une chaîne de caractères alphanumériques, qui est unique pour chaque ensemble unique de données d'entrée. Cette sortie est souvent appelée le "hash" ou la "valeur de hachage". Utilisez SHA-256 (le plus sécurisé) ou un algorithme plus puissant. Évitez SHA-1 et MD5.

Utilisations

- **Authentification** : Pour vérifier que les messages proviennent d'une source légitime.
- **Intégrité des Données** : Pour s'assurer que les données n'ont pas été modifiées pendant la transmission.

HMAC garanti que seules les parties autorisées peuvent vérifier l'intégrité et l'authenticité des messages.

Protocoles d'authentification

Protocole EAP (Extensible Authentification Protocol)
Un mot de passe du client est envoyé à l'aide d'un "hachage" (hash) au serveur d'authentification.

CHAP (Protocole d'authentification à échanges confirmés)
CHAP valide l'identité des clients distants à l'aide d'une fonction de hachage unidirectionnelle. CHAP vérifie t périodiquement l'identité du client pendant la transmission.

Kerberos = tickets sécurisés
Kerberos demande au client de prouver son identité au serveur puis au serveur de s'authentifier auprès du client. Le serveur Kerberos possède les ID utilisateur et les mots de passe hachés pour tous les utilisateurs. Il partage également des clés secrètes avec tous les serveurs auxquels il accorde des tickets d'accès. Les tickets sont utilisés en deux étapes avec le client. Le premier ticket est un ticket émis par le service d'authentification puis le client peut présenter ce ticket au serveur Kerberos avec une demande de ticket pour accéder à un serveur spécifique.