Première année

Cours 7: Contrôle d'accès et gestion des identités

Le recours aux technologies de l'information et des communications (TIC) semble **indispensable** de nos jours. – > *évolution croissante des besoins des clients et de la production de données volumineuses*.

Les risques ? – > **vulnérabilité et risques potentiels** – > informations exposées

- **Accès non autorisé**
- **Altération ou destruction de données**
- **Divulgation de l'information ou vol de données**
- **Augmentation du niveau de privilège**

La gestion des accès

– > **Basée sur les principes de privilège minimal et de séparation des tâches**

Elle répond à 4 questions:

1. Qui a accès a quelle information?
2. Qui a approuvé l'accès?
3. L'accès est-il adapté aux tâches à accomplir ?
4. L'accès et les opérations correspondantes sont-ils correctement surveillés, consignés et enregistrés ?

Contrôle d'accès ou gestion des accès – > **vérifie si une entité** (personne ou organisation) qui **demande l'accès à un objet** (fichier, BDD, programme) **possède les autorisations nécessaires**.

Processus de contrôle des accès – > **permet de créer, d'identifier, d'enregistrer et de gérer l'identité des utilisateurs et les droits d'accès à l'information que détient l'organisme.**

Privilèges ou droits d'accès – > désigne l'**opération recherché à l'égard d'un objet** (lire, écrire, modifier, supprimer, imprimer, créer, copier, transmettre)

Rôle – > définit l'**ensemble des privilèges nécessaires à l'utilisation des objets** (applications ou ressources).

Rôle applicatif – > définit l'**ensemble de droits d'accès propres à une seule tâche dans une**

application.

Habilitation – > regroupe **plusieurs rôles ou rôles applicatifs permettant de hiérarchiser l'utilisation des ressources.**

Matrice de profils d'accès général – > **grille associée à une entité contenant les rôles définis** pour ses utilisateurs ou groupes d'utilisateurs.

Matrice de profils d'accès applicatif – > **grille associée à un objet contenant les rôles applicatifs définis** pour ses utilisateurs ou groupes d'utilisateurs.

Mise en place de mesures de sécurité:

- **Gestion des droits et des privilèges d'accès** – > permet à l'organisme d'assurer l'équilibre entre la protection de l'information qu'il détient et l'attribution des privilèges aux utilisateurs

---

Le modèle IBAC (Identity-Based Access Control)

1971: premier modèle de contrôle d'accès

– > toujours **utilisé par les OS (Windows) et serveurs Linux**

– > repose sur une **matrice composée d'un ensemble fini d'entités, de ressources et de règles**

– > **établissement d'une liste exhaustive contenant les autorisations d'accès** (*ACL: Access Control List*)

– > les **habilitations sont directement affectés aux comptes utilisateurs**

L'arrivée d'une nouvel utilisateur ou d'une nouvelle ressource nécessite la mise à jour des habilitations.

Le modèle MAC (Mandatory Access Control)

1973: contrôle d'accès obligatoire

– > **fonctionne par niveau de sécurité**

– > un niveau définit le **niveau d'habilitation de l'utilisateur et de la ressource**

– > l'utilisateur a **accès à la ressource si son niveau d'habilitation est supérieur ou égal au niveau de classification de la ressource**

1986: version étendue du modèle MAC

– > **fonctionne toujours par niveau de sécurité** mais un intervalle de niveaux est attribué à toutes les ressources

– > offre une **plus grande flexibilité**

– > **modèle proche de celui utilisé actuellement par le SGBD Oracle**

Le modèle RBAC (Rule-Based Access Control)

1992: modèle de contrôle d'accès par rôle

– > **habilitations sont affectées à des rôles**

– > les rôles peuvent **représenter des métiers, des activités, des projets ou des personnes physiques**

– > les rôles **désignent le lien entre les utilisateurs et les ressources**

– > il n'existe **aucun modèle générique que l'on pourrait appliquer à différentes entreprises**

Il atteint rapidement ses **limites** dès lors que **les utilisateurs sont géographiquement différentiables ou dès lors que l'entreprise est composée de services indépendants**.

Le modèle ORBAC (Organization-Based Access Control)

2003: modèle de contrôle d'accès fondé sur l'organisation

– > correspond à tout **organisme nécessitant une grande logistique**

– > reprend les **concepts de rôle, d'activité, d'objets et d'organisation**