

# Les trois principes de base de la sécurité - CID

Les trois principes de base de la sécurité des système d'information sont :

- la **confidentialité** des données,
- l'**intégrité** des données,
- la **disponibilité** des données.

Le sigle CID correspond à ces trois principes.

## La confidentialité des données

La confidentialité des données est assurée par le contrôle d'accès.

Le **contrôle d'accès** consiste à mettre en oeuvre les solutions matérielles et logicielles pour **interdire les accès non autorisés** à un ordinateur, un réseau, une base de données ou d'autres ressources dans le réseau d'une organisation.

La mise en oeuvre d'un contrôle d'accès recouvre trois service de sécurité désignés par les lettres **AAA** :

- l'**authentification** ((Authentication),
- l'**autorisation** (Authorization),
- la **journalisation** (Accounting).

### L'authentification

L'authentification permet de vérifier l'identité d'un utilisateur afin d'empêcher tout accès non autorisé.

Pour cela, un utilisateur doit :

- **prouver son identité** au moyen d'un nom d'utilisateur ou d'un identifiant unique,
- **confirmer leur identité** en fournissant l'un ou plusieurs des éléments suivants :
  - Un élément qu'ils connaissent (comme un mot de passe) : facteur de **connaissance**,
  - Une chose qu'ils possèdent (comme un jeton ou une carte) : facteur de **possession**,
  - Un élément qui les caractérise (comme une empreinte digitale) : facteur **d'inhérence**.

### L'autorisation

Une authentification réussie ne suffit pas pour accéder aux ressources de l'organisation.

Les **services d'autorisation** consistent :

- à **identifier** les ressources auxquelles les utilisateurs peuvent accéder,
- **définir** les opérations que les utilisateurs peuvent effectuer.

Les autorisations (ou privilèges) correspondent en général à une **liste de contrôle d'accès ou ACL** (Access Control List). Les autorisations d'accès peuvent aussi contrôler les périodes au cours desquelles un utilisateur peut accéder à une ressource spécifique.

### La journalisation

La journalisation permet de garder une trace et donc de suivre les actions des utilisateurs :

- les ressources auxquels ils accèdent,
- le temps d'accès aux ressources,
- les modifications effectuées.

## L'intégrité des données

L'intégrité représente l'exactitude, la cohérence et la fiabilité des données pendant tout leur cycle de vie.

Durant leur cycle de vie, les données font l'objet de nombreuses opérations :

- la création ou la capture de données,
- le stockage,

- l'utilisation,
- la mise à jour
- le transfert. Cependant, elles ne doivent, à aucun moment, être altérées par des entités non autorisées.

Les méthodes utilisées pour assurer l'intégrité des données comprennent le calcul de hashes, les contrôles de validité des données et les contrôles d'accès. Les systèmes d'intégrité des données peuvent inclure une ou plusieurs des méthodes répertoriées ci-dessus.

From:

/ - **Les cours du BTS SIO**

Permanent link:

</doku.php/bloc3s1/principesecuritecid?rev=1643057657>

Last update: **2022/01/24 21:54**

