Les principes de sécurité informatique

[sommaire]

1. **Objectif**

- Connaitre les principales caractéristiques de la sécurité informatique;

- **Présentation**

- La sécurité des systèmes d'information (SSI) ou plus simplement sécurité informatique, est l'ensemble des moyens techniques, organisationnels, juridiques et humains nécessaires à la mise en place de moyens visant à empêcher l'utilisation non-autorisée, le mauvais usage, la modification ou le détournement du système d'information.
- La sécurité informatique c'est l'ensemble des moyens mis en œuvre pour réduire la vulnérabilité d'un système contre les menaces accidentelles ou intentionnelles. Il convient d'identifier les exigences fondamentales en sécurité informatique.
- **La sécurité informatique vise généralement cinq principaux objectifs :**

1. La confidentialité, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées ;
2. L'intégrité, c'est-à-dire garantir que les données sont bien celles que l'on croit être ;
3. La disponibilité, permettant de maintenir le bon fonctionnement du système d'information ;
4. La non répudiation, permettant de garantir qu'une transaction ne peut être niée ;
5. L'authentification, consistant à assurer que seules les personnes autorisées aient accès aux ressources.

- **La confidentialité**

- La confidentialité consiste à rendre l'information inintelligible à d'autres personnes que les seuls acteurs de la transaction.
- Seules les personnes autorisées peuvent avoir accès aux informations qui leur sont destinées (notions de droits ou permissions). Tout accès indésirable doit être empêché.

- **L'intégrité**

apcpedagogie.com

- Vérifier l’intégrité des données consiste à déterminer si les données n’ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).
- Les données doivent être celles que l'on attend, et ne doivent pas être altérées de façon fortuite, illicite ou malveillante. En clair, les éléments considérés doivent être exacts et complets. Cet objectif utilise généralement des méthodes de calculs de checksum ou de hachage.
- Le critère d’intégrité est relatif au fait que des ressources, données, traitements, transactions ou services n’ont pas été modifiés, altérés ou détruits tant de façon intentionnelle qu’accidentelle.
- Il convient de se prémunir contre l’altération des données en ayant la certitude qu’elles n’ont pas été modifiées lors de leur stockage, de leur traitement ou de leur transfert.

La disponibilité

- L’objectif de la disponibilité est de garantir l’accès à un service ou à des ressources.
- L'accès aux ressources du système d'information doit être permanent et sans faille durant les plages d'utilisation prévues. Les services et ressources sont accessibles rapidement et régulièrement.

La non-répudiation

- La non-répudiation de l’information est la garantie qu’aucun des correspondants ne pourra nier la transaction.
- La non-répudiation est le fait de ne pouvoir nier ou rejeter qu’un événement (action, transaction) a eu lieu. À ce critère de sécurité sont associées les notions d’imputabilité, de traçabilité.
- L’imputabilité se définit par l’attribution d’une action (un événement) à une entité déterminée (ressource, personne). L’imputabilité est liée à la notion de responsabilité. Elle peut être réalisée par un ensemble de mesures garantissant l’enregistrement fiable d’informations pertinentes par rapport à une entité et à un événement.

L’authentification

- Les utilisateurs doivent prouver leur identité par l'usage de code d'accès. Il ne faut pas mélanger identification et authentification : dans le premier cas, l'utilisateur n'est reconnu que par son identifiant, tandis que dans le deuxième cas, il doit fournir un mot de passe ou un élément que lui-seul connaît. Cela permet de gérer les droits d'accès aux ressources concernées et maintenir la confiance dans les relations d'échange.

apcpedagogie.com

- L’authentification consiste à assurer l’identité d’un utilisateur, c’est-à-dire de garantir à chacun des correspondants que son partenaire est bien celui qu’il croit être. Un contrôle d’accès peut permettre l’accès à des ressources uniquement aux personnes autorisées.

Nécessité d’une approche globale

- La sécurité d’un système informatique fait souvent l’objet de métaphores. En effet, on la compare régulièrement à une chaîne en expliquant que le niveau de sécurité d’un système est caractérisé par le niveau de sécurité du maillon le plus faible. Ainsi, une porte blindée est inutile dans un bâtiment si les fenêtres sont ouvertes sur la rue.
- Cela signifie que la sécurité doit être abordée dans un contexte global et notamment prendre en compte les aspects suivants :

Les mots de passe

- Les logiciels et les sites web proposent souvent des services personnalisés. Par exemple le site web de votre banque vous montre seulement votre compte en banque et pas celui de votre voisin. Cette personnalisation de l'information implique d'identifier avec certitude l'utilisateur. Pour cela, on va lui demander de saisir deux informations : un identifiant et un mot de passe.
- Voici quelques conseils pour sécuriser vos mots de passe.
- Il faut classer les accès en 2 catégories selon leur degré de sensibilité :
  - **D'un coté, vos accès sensibles :** ils permettent d'obtenir des informations très importantes. Quelqu'un de malintentionné peut utiliser ces informations pour vous causer de graves problèmes. Cette catégorie contient entre autre :
    - les logiciels et sites de votre vie professionnelle car les informations qu'ils contiennent ont souvent de la valeur. Un fichier client peut valoir plusieurs dizaines de milliers d'euros.
    - le site de votre banque : pas besoin de vous expliquer
    - votre messagerie électronique car elle centralise de nombreuses informations. De plus, beaucoup de sites renvoient sur simple demande les mots de passe sur cette messagerie
    - les réseaux sociaux car quelqu'un de malintentionné peut ruiner votre réputation
    - les sites commerciaux sur lesquels vous avez enregistrée votre carte bleue
  - **De l'autre coté, les accès usuels comme**
    - les blogs que vous consultez régulièrement,
    - les forums sur lesquels vous vous êtes inscrits une seule fois pour poser une question,
    - les sites des marques sur lesquels vous n'achetez rien...

apcpedagogie.com

Cours le commerce électronique

Source : https://apcpedagogie.com/les-principes-de-securite-informatique · téléchargé le 03/11/2026 · © APC Pédagogie · apcpedagogie.com

apcpedagogie.com