Sécurité informatique

Introduction

La sécurité informatique est une notion de plus en plus présente dans le monde actuel. Le concept de sécurité recouvre un ensemble de méthodes, techniques et outils chargés de protéger les ressources.

Nous partons de la simple définition jusqu'à proposer quelques méthodes et techniques capables de protéger l‘information et d‘assurer la sécurité des données.

Définition de la sécurité

La sécurité informatique c'est l'ensemble des moyens, techniques, outils et ressources mis en œuvre pour minimiser la vulnérabilité d'un système ou, si cela est possible, de le protéger contre des menaces accidentelles ou intentionnelles.

En anglais, il existe deux termes différents:

- ***Sécurité = "Safety"***

Cette notion recouvre la protection des systèmes informatiques contre les accidents dus à l'environnement, aux défauts du système.

- ***Sécurité = "Security"***

C‘est la protection des systèmes informatiques contre des actions malveillantes intentionnelles.

Les objectifs de la sécurité

Les objectifs doivent être satisfaits selon une stratégie appelée *politique de sécurité*. Parfois on doit même déterminer la priorité de chaque objectif par rapport aux autres ; ces objectifs sont :

La disponibilité

La disponibilité concerne les services (ordinateurs, réseaux, périphériques, applications, etc.) et les informations (données, fichiers, etc.) doivent être accessibles aux personnes autorisées quand elles en ont besoin : le système doit donc rester fonctionnel malgré la survenue d'erreurs, malicieuses ou accidentelles. De même, la disponibilité concerne les données qui ne doivent pas être supprimées ou devenir inaccessibles.

La disponibilité

Maintenant on va citer quelques risques qui portent atteinte à la disponibilité :

- La paralysie du système (considérée ensuite comme un exploit par les pirates qui l‘ont réalisée).
- La saturation d‘une ressource (serveur, imprimante, etc.).
- Les virus et vers informatiques.

La confidentialité

Les informations n‘appartiennent pas à tout le monde : seuls peuvent y accéder ceux qui en ont le droit, selon des conditions prédéfinies. Donc, le système ne doit pas divulguer des informations à une personne qui n‘a pas le droit d‘y avoir accès.

La confidentialité

Maintenant on va citer quelques risques qui portent atteinte à la confidentialité des informations :

- La récupération d'informations sensibles (mots de passe, articles avant publication, données personnelles, etc.).
- La fouille des messages, des données, des répertoires, des ressources réseaux, etc.
- L'usurpation d'identité.

L’intégrité

Les services et les informations (fichiers, messages, etc.) ne peuvent être modifiés que par les personnes autorisées (administrateurs, propriétaires…) ; donc, le système ne doit pas être modifié par une personne qui n‘en a pas les droits. C'est la propriété qui assure qu'une information n'est modifiée que dans des conditions prédéfinies (selon des contraintes précises).

L’intégrité

Selon la norme ISO 7498-2, l‘intégrité est la prévention d‘une modification non autorisée de l‘information.

Maintenant on va citer quelques risques qui portent atteinte à l‘intégrité du système :

- Le piégeage de systèmes (bombes logiques, chevaux de Troie, sniffers, etc.) afin de nuire à l‘entreprise ou de se donner les moyens d‘y accéder plus tard.

- La modification des informations afin de porter atteinte à l‘image du laboratoire (exemple : modification des pages web de L‘entreprise).
- L‘utilisation des ressources du site visé.
- Une intrusion en vue "d‘attaques par rebond ", c‘est-à-dire qu‘une autre cible est visée, le système actuel servant seulement de "point de passage". Le laboratoire est alors complice involontaire du piratage.

La non-répudiation

La non-répudiation est la propriété qui assure que l'auteur d'un acte ne peut ensuite dénier l'avoir commis.

Deux aspects spécifiques de la non-répudiation dans les transactions électroniques:

- **La preuve d'origine :** un message (une transaction) ne peut être déniée par son émetteur.
- **La preuve de réception :** un récepteur ne peut ultérieurement nier avoir reçu un ordre s'il ne lui a pas plu de l'exécuter alors qu'il le devait juridiquement.

Il y a différentes techniques pour assurer la non-répudiation qui sont la signature numérique et le certificat numérique.