Introduction à la sécurité informatique

DA2I

FST

Objectifs de la sécurité informatique

- Le système d'information de l'entreprise est défini par l'ensemble des données et des ressources matérielles et logicielles permettant de les stocker ou de les faire circuler.
- Le système d'information représente un patrimoine essentiel de l'entreprise, qu'il convient de protéger.
- 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.
- La sécurité informatique, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

Objectifs de la sécurité informatique

La sécurité informatique vise généralement 5 principaux objectifs :

- La **disponibilité**, permettant de maintenir le bon fonctionnement du système d'information en assurant que l'information sur le système soit disponible aux personnes autorisées.;
- L'**intégrité**, protéger les donnés contre la destruction ou la modification non autorisée. D'une autre manière s'assurer que l'information sur le système ne puisse être *modifiée que par les* personnes autorisées;

Objectifs de la sécurité informatique (suite)

- La **confidentialité**, consistant à assurer que seules les personnes autorisées aient accès aux ressources échangées (garder les donnés loin des yeux des 'autres');
- La non-répudiation de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.
- 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.

Approche

- 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.
- La sécurité doit prendre en compte les aspects suivants :
  - **La sensibilisation des utilisateurs aux problèmes de sécurité**
  - **La sécurité logique**, c'est-à-dire la sécurité au niveau des données, notamment les données de l'entreprise, les applications ou encore les systèmes d'exploitation.
  - **La sécurité des télécommunications :** technologies réseau, serveurs de l'entreprise, réseaux d'accès, etc.
  - **La sécurité physique**, soit la sécurité au niveau des infrastructures matérielles : salles sécurisées, lieux ouverts au public, espaces communs de l'entreprise, postes de travail des personnels, etc.

Mise en place d'une politique de sécurité

- La sécurité des systèmes informatiques se résume généralement à garantir les droits d'accès aux données et ressources d'un système en mettant en place des mécanismes d'authentification et de contrôle permettant d'assurer que les utilisateurs des dites ressources possèdent uniquement les droits qui leur ont été octroyés.
- Les mécanismes de sécurité mis en place peuvent néanmoins provoquer une gêne au niveau des utilisateurs et les consignes et règles deviennent de plus en plus compliquées au fur et à mesure que le réseau s'étend.
- Ainsi, la sécurité informatique doit être étudiée de telle manière à ne pas empêcher les utilisateurs de développer les usages qui leur sont nécessaires, et de faire en sorte qu'ils puissent utiliser le système d'information en toute confiance.

Mise en place d'une politique de sécurité (suite)

- Il est nécessaire de définir dans un premier temps une **politique de sécurité**, dont la mise en œuvre se fait selon les quatre étapes suivantes :
  - Identifier les besoins en terme de sécurité, les risques informatiques pesant sur l'entreprise et leurs éventuelles conséquences ;
  - Elaborer des règles et des procédures à mettre en œuvre dans les différents services de l'organisation pour les risques identifiés;
  - Surveiller et détecter les vulnérabilités du système d'information et se tenir informé des failles sur les applications et matériels utilisés ;
  - Définir les actions à entreprendre et les personnes à contacter en cas de détection d'une menace ;

Mise en place d'une politique de sécurité (suite)

- La sécurité informatique de l'entreprise repose sur une bonne connaissance des règles par les employés, grâce à des actions de formation et de sensibilisation auprès des utilisateurs, mais elle doit aller au-delà et notamment couvrir les champs suivants :
  - Un dispositif de sécurité physique et logique, adapté aux besoins de l'entreprise et aux usages des utilisateurs ;
  - Une procédure de management des mises à jour ;
  - Une stratégie de sauvegarde correctement planifiée ;
  - Un plan de reprise après incident;
  - Un système documenté à jour.

Rôle de l'administrateur informatique dans la mise en place d'une politique de sécurité

- La politique de sécurité est l'ensemble des orientations suivies par une organisation (à prendre au sens large) en terme de sécurité. A ce titre elle se doit d'être élaborée au niveau de la direction de l'organisation concernée, car elle concerne tous les utilisateurs du système.
- Il ne revient pas aux seuls administrateurs informatiques de définir les droits d'accès des utilisateurs mais aux ses responsables hiérarchiques.
- **Le rôle de l'administrateur informatique est de s'assurer que les ressources informatiques et les droits d'accès à celles-ci sont en cohérence avec la politique de sécurité définie par l'organisation.**
- De plus, étant donné qu'il est le seul à connaître parfaitement le système, il lui revient:
  - de faire remonter les informations concernant la sécurité à sa direction,
  - de conseiller les décideurs sur les stratégies à mettre en œuvre,
  - d'être le point d'entrée concernant la communication à destination des utilisateurs sur les problèmes et recommandations en terme de sécurité.

Les causes de l'insécurité

On distingue généralement deux types d'insécurités:

- **l'état actif d'insécurité**, c'est-à-dire la non connaissance par l'utilisateur des fonctionnalités du système, dont certaines pouvant lui être nuisibles (par exemple le fait de ne pas désactiver des services réseaux non nécessaires à l'utilisateur)
- **l'état passif d'insécurité**, c'est-à-dire la méconnaissance des moyens de sécurité mis en place, par exemple lorsque l'administrateur (ou l'utilisateur) d'un système ne connaît pas les dispositifs de sécurité dont il dispose