

# Introduction à la sécurité informatique

Avec le développement de l'utilisation d'internet, de plus en plus d'entreprises ouvrent leur système d'information à leurs partenaires ou leurs fournisseurs, il est donc essentiel de connaître les ressources de l'entreprise à protéger et de maîtriser le contrôle d'accès et les droits des utilisateurs du système d'information. Il en va de même lors de l'ouverture de l'accès de l'entreprise sur internet.

Par ailleurs, avec le nomadisme, consistant à permettre aux personnels de se connecter au système d'information à partir de n'importe quel endroit, les personnels sont amenés à « transporter » une partie du système d'information hors de l'infrastructure sécurisée de l'entreprise.

## Introduction à la sécurité

Le **risque** en terme de sécurité est généralement caractérisé par l'équation suivante :

$$\text{Risque} = \frac{\text{Menace} \times \text{Vulnérabilité}}{\text{Contre-mesure}}$$

La **menace** (en anglais « threat ») représente le type d'action susceptible de nuire dans l'absolu, tandis que la **vulnérabilité** (en anglais « *vulnerability* », appelée parfois *faille* ou *brèche*) représente le niveau d'exposition face à la menace dans un contexte particulier. Enfin la **contre-mesure** est l'ensemble des actions mises en oeuvre en prévention de la menace.

Les contre-mesures à mettre en oeuvre ne sont pas uniquement des solutions techniques mais également des mesures de formation et de sensibilisation à l'intention des utilisateurs, ainsi qu'un ensemble de règles clairement définies.

Afin de pouvoir sécuriser un système, il est nécessaire d'identifier les menaces potentielles, et donc de connaître et de prévoir la façon de procéder de l'ennemi. Le but de ce dossier est ainsi de donner un aperçu des motivations éventuelles des pirates, de catégoriser ces derniers, et enfin de donner une idée de leur façon de procéder afin de mieux comprendre comment il est possible de limiter les risques d'intrusions.

## Objectifs de la sécurité informatique

Le système d'information est généralement défini par l'ensemble des données et des ressources matérielles et logicielles de l'entreprise 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, d'une manière générale, consiste à assurer que les ressources matérielles ou logicielles d'une organisation sont uniquement utilisées dans le cadre prévu.

La sécurité informatique vise généralement cinq principaux objectifs :

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

## L'intégrité

Vérifier l'intégrité des données consiste à déterminer si les données n'ont pas été altérées durant la communication (de manière fortuite ou intentionnelle).

## La disponibilité

L'objectif de la disponibilité est de garantir l'accès à un service ou à des ressources.

## La non-répudiation

La **non-répudiation** de l'information est la garantie qu'aucun des correspondants ne pourra nier la transaction.

## L'authentification

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 (par exemple par le moyen d'un mot de passe qui devra être crypté) 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 :

- **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 cantonne 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.

C'est la raison pour laquelle il est nécessaire de définir dans un premier temps une **politique de sécurité**, dont la mise en oeuvre 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 oeuvre 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 ;

La politique de sécurité est donc 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.

A cet égard, il ne revient pas aux seuls administrateurs informatiques de définir les droits d'accès des utilisateurs mais aux responsables hiérarchiques de ces derniers. Le rôle de l'administrateur informatique est donc 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, éventuellement de conseiller les décideurs sur les stratégies à mettre en oeuvre, ainsi que d'être le point d'entrée concernant

la communication à destination des utilisateurs sur les problèmes et recommandations en terme de sécurité.

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 ;

## **Les causes de l'insécurité**

On distingue généralement deux types d'insécurité :

- **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.