Chapitre 1

Principes de sécurité

Ce chapitre présente :
- les principales caractéristiques de la sécurité informatique ;
- les champs d'application ainsi que les différents aspects de la sécurité informatique et des réseaux ;
- les différents types d'attaques *via* Internet, les modalités et les conditions de succès d'une attaque.

1.1 CRITÈRES DE SÉCURITÉ ET FONCTIONS ASSOCIÉES

Les solutions de sécurité qui seront mises en place doivent contribuer à satisfaire les critères suivant :
- la **disponibilité** ;
- l'**intégrité** ;
- la **confidentialité** (critères DIC).

À ces trois critères s'ajoutent ceux qui permettent de prouver l'identité des entités (notion d'**authentification**) et ceux qui indiquent que des actions ou événements ont bien eu lieu (notions de **non-répudiation**, d'**imputabilité** voire de **traçabilité**) (figure 1.1).

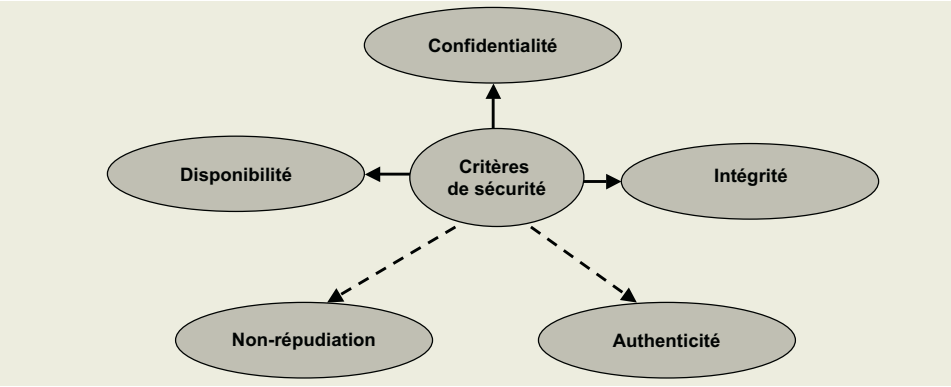

Figure 1.1 – Critères de sécurité.

1.1.1 Disponibilité

Pour un utilisateur, la **disponibilité** d'une ressource est la probabilité de pouvoir mener correctement à terme une session de travail.

La disponibilité d'une ressource est indissociable de son **accessibilité** : il ne suffit pas qu'elle soit disponible, elle doit être utilisable avec des temps de réponse acceptables.

Elle est mesurée sur la période de temps pendant laquelle le service offert est opérationnel. Le volume potentiel de travail susceptible d'être pris en charge durant la période de disponibilité d'un service, détermine la **capacité** d'une ressource (serveur ou réseau par exemple).

La disponibilité des services, systèmes et données est obtenue :

– par un **dimensionnement approprié** et une certaine redondance ;
– par une **gestion opérationnelle efficace** des infrastructures, ressources et services.

Dans le cas d'un réseau grande distance de topologie maillée par exemple, la disponibilité des ressources réseau sera réalisée à condition que l'ensemble des liaisons ait été correctement dimensionné et que les politiques de routage et de gestion soient satisfaisantes.

Dans un contexte de système d'information d'entreprise, des **tests** de montée en charge sont généralement effectués pour évaluer le comportement des systèmes sous certaines conditions extrêmes et contribuer ainsi à mieux définir leur dimensionnement.

Un service nominal doit être assuré avec le minimum d'interruption, il doit respecter les clauses de l'engagement de service établi sur des indicateurs dédiés à la mesure de la **continuité de service**.

Des pertes de données, donc une indisponibilité de celles-ci, sont possibles si les procédures d'enregistrement et les supports de mémorisation ne sont pas gérés correctement. Ce risque majeur est souvent mal connu des utilisateurs. Leur sensibi-

lisation à cet aspect de la sécurité est importante mais ne peut constituer un palliatif à une indispensable mise en place de procédures centralisées de sauvegarde effectuées par les services compétents en charge des systèmes d'information de l'entreprise.

De nombreux outils permettent de sauvegarder périodiquement et de façon automatisée les données, cependant, une définition correcte des procédures de restitution des données devra être établie afin que les utilisateurs sachent ce qu'ils ont à faire s'ils rencontrent un problème de perte de données.

Une **politique de sauvegarde** ainsi qu'un arbitrage entre le coût de la sauvegarde et celui du risque d'indisponibilité supportable par l'organisation seront établis afin que la mise en œuvre des mesures techniques soit efficace et pertinente.

1.1.2 Intégrité

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. Les critères de disponibilité et d'intégrité sont à satisfaire par des mesures appropriées afin de pouvoir atteindre un certain niveau de confiance dans le fonctionnement des infrastructures informatiques et télécoms et notamment dans l'application critique.

Si en télécommunication, l'intégrité des données relève essentiellement de problématiques liées au transfert de données, elle dépend également des aspects purement informatiques de traitement de l'information (logiciels, systèmes d'exploitation, environnements d'exécution, procédures de sauvegarde, de reprise et de restauration des données).

Rappelons que lors de leur transfert, les données ne devraient pas être altérées par les protocoles de communication qui les véhiculent. Ces derniers interviennent uniquement sur les données de contrôle du protocole et non directement sur les données à transférer : un protocole ne modifie pas le corps des données qu'il véhicule. Par contre, l'intégrité des données ne sera garantie que si elles sont protégées des **écoutes actives** qui peuvent modifier les données interceptées.

1.1.3 Confidentialité

La confidentialité est le maintien du secret des informations… (*Le Petit Robert*)

Transposée dans le contexte de l'informatique et des réseaux, la **confidentialité** peut être vue comme la « protection des données contre une divulgation non autorisée ».

Il existe deux actions complémentaires permettant d'assurer la confidentialité des données :

– limiter leur accès par un mécanisme de contrôle d'accès ;

– transformer les données par des procédures de chiffrement afin qu'elles deviennent inintelligibles aux personnes ne possédant pas les moyens de les déchiffrer.

> Le **chiffrement des données** (ou **cryptographie**)[1] contribue à en assurer la confidentialité des données et à en augmenter la sécurité des données lors de leur transmission ou de leur stockage. Bien qu'utilisées essentiellement lors de transactions financières et commerciales, les techniques de chiffrement sont relativement peu mises en œuvre par les internautes de manière courante.

1.1.4 Identification et authentification

Identifier l'auteur présumé d'un tableau signé est une chose, s'assurer que le tableau est authentique en est une autre. Il en est de même en informatique où des procédures d'**identification** et d'**authentification** peuvent être mises en œuvre pour contribuer à réaliser des procédures de contrôle d'accès et des mesures de sécurité assurant :

– la **confidentialité** et l'**intégrité des données** : seuls les ayants droit identifiés et authentifiés peuvent accéder aux ressources (contrôle d'accès[2]) et les modifier s'ils sont habilités à le faire ;
– la **non-répudiation** et l'**imputabilité** : seules les entités identifiées et authentifiées ont pu réaliser une certaine action (preuve de l'origine d'un message ou d'une transaction, preuve de la destination d'un message…).

Un nom associé à des caractéristiques identifie une entité : individu, ordinateur, programme, document, etc. L'identification est la reconnaissance de cette entité.

L'authentification permet de vérifier l'identité annoncée et de s'assurer de la non-usurpation de l'identité d'une entité. Pour cela, l'entité devra produire une information spécifique telle que par exemple un mot de passe (un code, un mot de passe, une empreinte biométrique, etc.).

Tous les mécanismes de contrôle d'accès logique aux ressources informatiques nécessitent de gérer l'identification et l'authentification des entités (figure 1.2).

1.1.5 Non-répudiation

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 et éventuellement d'auditabilité.

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.

---

1. Le chiffrement des données est traité au chapitre 5.
2. Le contrôle d'accès est traité au chapitre 6.