Cybersécurité
sécurité informatique et réseaux

Solange Ghernaouti
Professeure à la faculté des HEC de l'université de Lausanne
Experte internationale en cybersécurité

5e édition

DUNOD

Toutes les marques citées dans cet ouvrage
sont des marques déposées par leurs propriétaires respectifs.

Illustration de couverture
Safety concept : Closed Padlock on digital background
© deepagopi 2011 - fotolia.com

11, rue Paul Bert 92240 Malakoff
www.dunod.com

ISBN 978-2-10-074734-4

Table des matières

AVANT-PROPOS

Ce livre offre une synthèse des problématiques et des éléments de solution concernant la cybersécurité et la sécurité des systèmes d'information. Il traite des aspects de maîtrise des risques, de la cybercriminalité et de la gestion stratégique et opérationnelle de la sécurité informatique et des réseaux. Il présente également les principales technologies et mesures qui permettent de réaliser des services et des fonctions de la sécurité informatique.

- Le **chapitre 1** introduit les **principes fondamentaux** et les domaines d'application de la sécurité informatique qui doivent être appréhendés de manière systémique. Il constitue la base nécessaire à la compréhension globale des différents aspects et dimensions de la cybersécurité.
- Le **chapitre 2** offre un panorama des **cyberrisques** et des différentes formes d'expression de la **cybercriminalité** et de ses impacts. Il identifie les vulnérabilités inhérentes au monde numérique, à **Internet** et au **cyberespace** ainsi que leur exploitation à des fins malveillantes. Il identifie les divers leviers d'action qui contribuent à produire de la sécurité et à lutter contre la cybercriminalité.
- Le **chapitre 3** traite des aspects liés à la **maîtrise des risques** informatiques, à la **gestion stratégique** et à la **gouvernance** de la sécurité. Les **dimensions politique, juridique et socio-économique** dans lesquelles s'inscrit la sécurité informatique sont identifiées pour insister sur la nécessité de doter les individus, les organisations et les États, de moyens suffisants et nécessaires à leur protection dans un monde numérique. Les métiers de la sécurité informatique, les acteurs, les compétences comme les notions d'organisation, de responsabilité et de mission de sécurité sont présentés.
- Le **chapitre 4** concerne les **outils méthodologiques**, les **normes**, les **méthodes**, les bonnes pratiques, les démarches à disposition pour identifier les besoins de sécurité, **définir une politique de sécurité**, mettre en place des mesures, **auditer**, **mesurer**, **évaluer**, **certifier** la sécurité. Ce chapitre traite également de la **gestion de crise**, des **plans de secours, de reprise** et **de continuité** des activités.
- Le **chapitre 5** est consacré aux principes fondamentaux de la **cryptographie** (chiffrement) mis en œuvre dans des environnements d'informatique distribuée pour offrir des services de confidentialité, d'authentification, d'intégrité, d'imputabilité et de non-répudiation. Une introduction à la **cryptographie quantique** ainsi qu'une présentation des avantages, inconvénients et limites des **systèmes de chiffrement** sont proposées. Les concepts et les mécanismes de signature numérique, de certificats numériques, d'infrastructures de gestion de clés (PKI), de tiers de confiance, d'autorité de certification sont analysés.

- Le **chapitre 6** traite des problématiques et des mesures de **sécurité des infrastructures de télécommunication** Internet. Il présente notamment la mise en œuvre de protocoles cryptographiques pour offrir des services de sécurité Internet (IPv6, IPSec), les principes de sécurité liés au routage, au contrôle d'accès, à des **réseaux privés virtuels** (VPN), à l'externalisation et au ***cloud computing***.
- Le **chapitre 7** est dédié à la sécurité des **réseaux sans fil**. Les technologies de la sécurité des réseaux cellulaires **GSM**, **GPRS**, **UMTS** sont étudiées comme celles des **réseaux locaux sans fil 802.11** et des **réseaux personnels**.
- Faisant suite à une présentation, dans les chapitres précédents, des protocoles cryptographiques implantés dans des infrastructures réseaux filaires et sans fil, le **chapitre 8** se focalise sur des mesures permettant de renforcer la sécurité des environnements par des **systèmes pare-feu** et de **protection contre les incidents.**
- Le **chapitre 9** est dédié à la protection des contenus et des principaux services applicatifs d'Internet (sécurité de la messagerie électronique, de la téléphonie sur Internet, de la navigation web, du commerce électronique, des paiements en ligne, des documents XML). Sont également abordées les notions de protection des données par le tatouage électronique, la gestion des droits numériques (DRM) et les problématiques de sécurité liées à l'usage de l'informatique personnelle et des réseaux sociaux en entreprise.
- Le **chapitre 10** traite de la **gestion de réseau** comme outil de cohérence et d'**intégration des mesures** de sécurité et des savoir-faire managérial et technologique.

Chaque chapitre comprend, entre autres, une présentation de ses objectifs, un résumé et des exercices. Un certain relief est introduit dans le texte par des **termes** mis en gras pour souligner leur importance, par la traduction anglaise du vocabulaire de la sécurité (*security vocabulary*) et par des encarts. De nombreuses références, un glossaire des principaux termes ou encore le corrigé des exercices contribuent à une meilleure assimilation des thèmes abordés.

Un glossaire et un index concluent cet ouvrage.

En traitant de manière complémentaire du management et de l'ingénierie de la sécurité, ce livre par une approche globale et intégrée permet d'appréhender toute la complexité de la cybersécurité et de développer les compétences nécessaires à sa maîtrise.

Ressources numériques

Cette édition revue et augmentée propose **plus d'une centaine d'exercices corrigés** ainsi que des compléments en ligne **téléchargeables** sur la page associée à l'ouvrage sur le site des éditions Dunod :
www.dunod.com/contenus-complementaires/9782100747344

Remerciements et dédicace

Ce livre est le fruit de mes activités de recherche, d'enseignement et de conseil développées depuis une trentaine d'années. Il est aussi celui des éditions précédentes et de mes premiers ouvrages entièrement consacrés à la sécurité, à savoir : *Stratégie et ingénierie de la sécurité des réseaux* (InterÉditions, 1998) et *Sécurité Internet, stratégies et technologies* (Dunod, 2000).

Cette présente édition ne serait pas ce qu'elle est sans la relecture de Monsieur Gérard PÉLIKS, membre de l'Association des réservistes du chiffre et de la sécurité de l'information (ARCSI), directeur adjoint du MBA en Management de la sécurité des données numériques de l'Institut Léonard de Vinci et chargé de cours à l'Institut Mines Télécom, qu'il en soit chaleureusement remercié.

Je dédie cet ouvrage à toutes les belles personnes rencontrées sur le chemin du Cyber, avec une pensée particulière pour mes étudiants, assistants et doctorants d'hier et d'aujourd'hui.

Solange GHERNAOUTI
Chevalier de la Légion d'honneur
Professeur de l'université de Lausanne
Director, Swiss Cybersecurity Advisory & Research Group
Associate fellow, Geneva Center for Security Policy
Membre de l'Académie suisse des sciences techniques
Membre de l'association des réservistes du chiffre et de la sécurité de l'information
(www.scarg.org)

1 SÉCURITÉ INFORMATIQUE ET CYBERSÉCURITÉ

PLAN

OBJECTIFS

- ➤ Présenter le contexte, les enjeux et les principes généraux de la cybersécurité.
- ➤ Identifier les critères et les principales caractéristiques et fonctions de la sécurité informatique.
- ➤ Comprendre les champs d'application, les différents aspects et la dimension interdisciplinaire de la sécurité informatique et réseaux.
- ➤ Aborder la notion d'architecture de sécurité.

1.1 OBJECTIFS DE SÉCURITÉ

La notion de sécurité fait référence à la propriété d'un système, qui s'exprime généralement en termes de **disponibilité** (D), d'**intégrité** (I) et de **confidentialité** (C). Ces critères de base (dits *critères DIC*) sont des objectifs de sécurité que la mise en œuvre de fonctions de sécurité permet d'atteindre. Des fonctions additionnelles peuvent offrir des services complémentaires pour confirmer la véracité ou l'authenticité d'une action ou d'une ressource (notion d'**authentification**) ou encore pour prouver l'existence d'une action à des fins de **non-répudiation** ou d'**imputabilité**, ou de **traçabilité** (figure 1.1).

La réalisation de services de sécurité, tels que ceux de gestion des identités, de contrôle d'accès, de détection d'intrusion par exemple, contribue à satisfaire des exigences de sécurité pour protéger des infrastructures numériques. Ce sont des approches complémentaires d'ingénierie et de gestion de la sécurité informatique qui permettent d'offrir un niveau de sécurité cohérent au regard de besoins de sécurité clairement exprimés.

1.1.1 Disponibilité

La **disponibilité** d'une ressource est relative à la période de temps pendant laquelle le service qu'elle offre est opérationnel. Le volume potentiel de travail susceptible

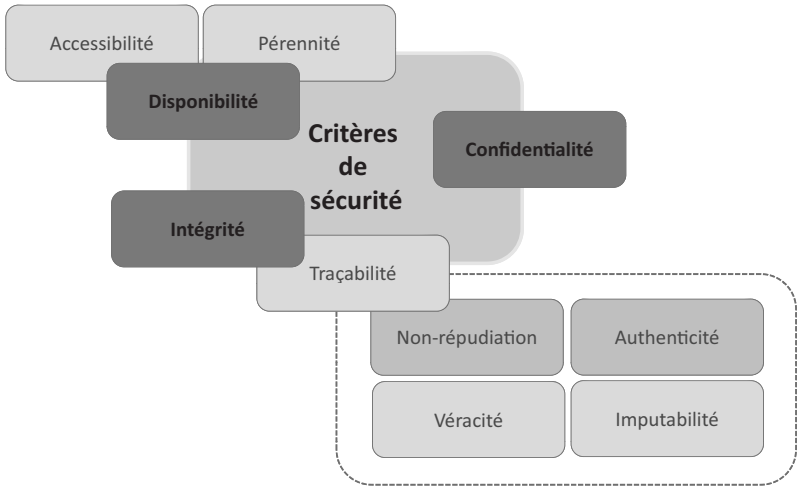

Figure 1.1 – **Critères de sécurité.**

d'être pris en charge durant la période de disponibilité d'un service détermine la **capacité** d'une ressource à être utilisée (serveur ou réseau par exemple).

Il ne suffit pas qu'une ressource soit disponible, elle doit pouvoir être utilisable avec des temps de réponse acceptables. Sa disponibilité est indissociable de sa capacité à être **accessible** par l'ensemble des ayants droit **(notion d'accessibilité)**.

La disponibilité des services, systèmes et données est obtenue par un **dimensionnement approprié** et une certaine redondance des infrastructures ainsi que par une **gestion opérationnelle** et une **maintenance efficaces** des infrastructures, ressources et services.

Un service nominal doit être assuré avec le minimum d'interruption, il doit respecter les clauses de l'engagement de service établies sur des indicateurs dédiés à la mesure de la **continuité de service**[1], assurée par le PCA (plan de continuité d'activité).

Des pertes de données, donc une indisponibilité de celles-ci, peuvent être possibles si les procédures de sauvegarde et de restitution ainsi que les supports de mémorisation associés ne sont pas gérés correctement.

Ceci constitue un **risque majeur** pour les utilisateurs. Leur sensibilisation 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. Ces outils doivent être utilisés dans le cadre d'un PRA (plan de reprise d'activité).

1. La gestion de la continuité des services est traitée au chapitre 4.

Une **politique de sauvegarde** ainsi qu'un arbitrage entre le coût de la sauvegarde et celui du risque d'indisponibilité supportable par l'organisation doivent être préalablement établis pour que la mise en œuvre des mesures techniques soit efficace et pertinente et que les utilisateurs sachent quelles sont les procédures à suivre.

1.1.2 Intégrité

Le critère d'**intégrité** des ressources physiques et logiques (équipements, données, traitements, transactions, services) est relatif au fait qu'elles sont demeurées intactes, qu'elles n'ont pas été détruites (altération totale) ou modifiées (altération partielle) à l'insu de leurs propriétaires tant de manière intentionnelle qu'accidentelle. Une fonction de sécurité appliquée à une ressource pour préserver son intégrité permet de la protéger contre une menace de corruption ou de destruction.

Se prémunir contre l'altération des données et avoir la certitude qu'elles n'ont pas été modifiées lors de leur stockage, de leur traitement ou de leur transfert contribue à la qualité des prises de décision basées sur celles-ci.

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

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 d'application, systèmes d'exploitation, environnements d'exécution, procédures de sauvegarde, de reprise et de restauration des données).

Des contrôles d'intégrité[2] peuvent être effectués pour s'assurer que les données n'ont pas été modifiées lors de leur transfert par des attaques informatiques qui les interceptent et les transforment (notion d'**écoutes actives)**. En revanche, ils seront de peu d'utilité pour détecter des écoutes passives, qui portent atteinte non à l'intégrité des données mais à leur confidentialité. En principe, lors de leur transfert, les données ne sont pas altérées par les protocoles de communication qui les véhiculent en les encapsulant. L'intégrité des données peut être prouvée par les mécanismes de signature électronique.

1.1.3 Confidentialité

La notion de **confidentialité** est liée au maintien du secret, elle est réalisée par la protection des données contre une divulgation non autorisée (notion de protection en lecture).

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

- limiter et contrôler leur accès afin que seules les personnes habilitées à les lire ou à les modifier puissent le faire ;

2. Voir chapitre 5.

- les rendre inintelligibles en les chiffrant de telle sorte que les personnes qui ne sont pas autorisées à les déchiffrer ne puissent les utiliser.

Le **chiffrement des données** (ou **cryptographie**)[3] contribue à assurer la confidentialité des données et à augmenter leur sécurité lors de leur transmission ou de leur stockage. Bien qu'utilisées essentiellement lors de transactions financières et commerciales, les techniques de chiffrement sont encore peu mises en œuvre par les internautes de manière courante.

1.1.4 Fonctions additionnelles

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[4]) 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 ou de la destination d'un message, par exemple). L'identification et l'authentification des ressources et des utilisateurs permettent d'imputer la responsabilité de la réalisation d'une action à une entité qui pourra en être tenue responsable et devra éventuellement en rendre compte.

Ainsi, l'enregistrement et l'analyse des activités permettent la **traçabilité** des événements. Garder la mémoire des actions survenues à des fins d'analyse permet de reconstituer et de comprendre ce qui s'est passé lors d'incidents afin d'améliorer la sécurité, d'éviter que des erreurs ne se répètent ou éventuellement d'identifier des fautifs. Cela permet par exemple d'analyser le comportement du système et des utilisateurs à des fins d'optimisation, de gestion des incidents et des performances, de recherche de preuves, ou encore d'audit.

L'authentification doit permettre de vérifier l'identité d'une entité afin de s'assurer, entre autres, de l'authenticité de celle-ci. Pour cela, l'entité devra prouver son identité, le plus souvent en donnant une information spécifique qu'elle est censée être seule à détenir telle que, par exemple, un mot de passe ou une empreinte biométrique.

Tous les mécanismes de contrôle d'accès logique aux ressources informatiques nécessitent de gérer l'identification, l'authentification des entités et la gestion des droits et permissions associés (figure 1.2). C'est également sur la base de l'identification des personnes et des accès aux ressources que s'établissent des fonctions de facturation et de surveillance.

3. Le chiffrement des données est traité au chapitre 5.
4. Le contrôle d'accès est traité au chapitre 6.

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 peuvent être associées les notions d'imputabilité, de traçabilité ou encore parfois d'auditabilité**.**

Attribuer une action à une entité déterminée (ressource ou personne) relève de l'**imputabilité**, qui peut être réalisée par un ensemble de mesures garantissant l'enregistrement fiable d'informations pertinentes relatives à un événement.

L'établissement de la **responsabilité** d'une personne vis-à-vis **d'un acte** nécessite l'existence de mesures d'identification et d'authentification des individus et d'imputabilité de leurs actions.

La **traçabilité** permet de reconstituer une séquence d'événements à partir des données numériques laissées dans les systèmes lors de leurs réalisations. Cette fonction comprend l'enregistrement des opérations, de la date de leur réalisation et leur imputation. Elle permet, par exemple, de retrouver l'adresse IP d'un système à partir duquel des données ont été envoyées. Afin de garder la trace d'événements, on recourt à des solutions qui permettent de les enregistrer (de les journaliser), à la manière d'un journal de bord, dans des fichiers (*log*).

L'**auditabilité** d'un système se définit par sa capacité à garantir la présence d'informations nécessaires à une analyse, postérieure à la réalisation d'un événement (courant ou exceptionnel), effectuée dans le cadre de procédures de contrôle et d'audit. L'audit peut être mis en œuvre pour diagnostiquer ou vérifier l'état de la sécurité d'un système, pour déterminer s'il y a eu ou non violation de la politique de sécurité[5], quelles sont les ressources compromises, ou encore par exemple pour déceler et examiner les événements susceptibles de constituer des menaces de sécurité.

Les coûts liés à la journalisation n'étant pas négligeables et la capacité mémoire des journaux n'étant pas infinie, l'administrateur système ou le responsable sécurité ont tout intérêt à identifier les **événements pertinents**, qui pourront faire l'objet d'analyse ultérieure lors de la survenue d'incidents, de procédures d'audit ou

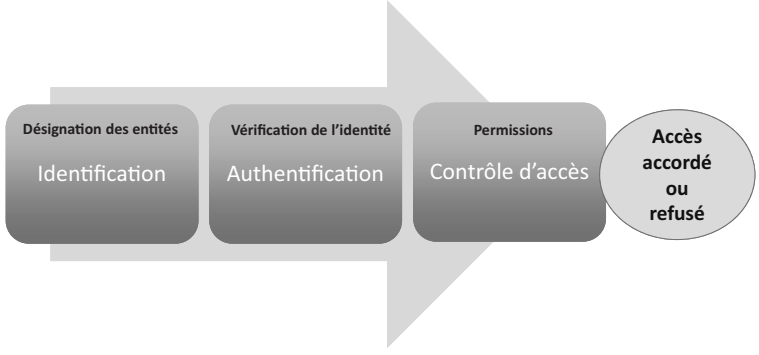

Figure 1.2 – Identification et authentification.

5. La politique de sécurité fait l'objet du chapitre 4.

d'actions en justice, et la **durée de rétention** des informations contenues dans ces journaux. La durée de rétention des données peut être fixée par des réglementations sectorielles ou par la loi, comme c'est le cas par exemple pour les fournisseurs d'accès et de services Internet, qui doivent garder toutes les données de connexion des internautes. Cela permet, lors d'enquêtes policières, d'identifier à partir des adresses IP les internautes soupçonnés d'avoir enfreint la loi.

Le mot anglais ***security***, qui signifie une résistance à une malveillance, se traduit en français par « **sûreté** », alors que le mot ***safety***, qui signifie une résistance à une panne, se traduit par « **sécurité** ». Pour simplifier, nous emploierons indifféremment par la suite le mot « sécurité » pour la résistance à une panne ou à une malveillance.

1.2 Domaines d'application

Pour une organisation, toutes les sphères d'activité de l'informatique et des réseaux de télécommunication sont concernées par la sécurité d'un système d'information.

En fonction de son domaine d'application, la sécurité informatique peut se décliner en (figure 1.3) :

- sécurité physique et environnementale ;
- sécurité de l'exploitation ;
- sécurité des réseaux ;
- sécurité logique, sécurité applicative et sécurité de l'information ;
- cybersécurité.

1.2.1 Sécurité physique et environnementale

La **sécurité physique** et **environnementale** concerne tous les aspects liés à la maîtrise des systèmes et de l'environnement dans lequel ils se situent.

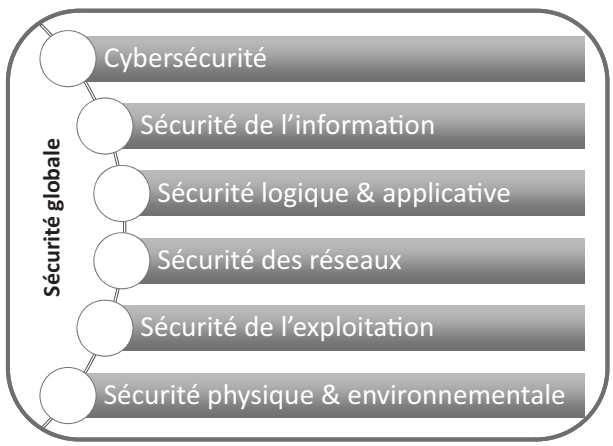

Figure 1.3 – Domaines d'application de la sécurité.

Sans vouloir être exhaustif, nous retiendrons que la sécurité physique repose essentiellement sur :

- la protection des sources énergétiques et de la climatisation (alimentation électrique, refroidissement, etc.) ;
- la protection de l'environnement (mesures *ad hoc* notamment pour faire face aux risques d'incendie, d'inondation ou encore de tremblement de terre… pour respecter les contraintes liées à la température, à l'humidité, etc.) ;
- des mesures de gestion et de contrôle des accès physiques aux locaux, équipements et infrastructures (avec entre autres la traçabilité des entrées et une gestion rigoureuse des clés d'accès aux locaux) ;
- l'usage d'équipements qui possèdent un bon degré de sûreté de fonctionnement et de fiabilité ;
- la redondance physique des infrastructures et des sources énergétiques ;
- le marquage des matériels pour notamment contribuer à dissuader le vol de matériel et éventuellement le retrouver ;
- le plan de maintenance préventive (tests, etc.) et corrective (pièces de rechange, etc.) des équipements, ce qui relève également de la sécurité de l'exploitation des environnements.

1.2.2 Sécurité de l'exploitation

La **sécurité de l'exploitation** doit permettre un bon fonctionnement opérationnel des systèmes informatiques. Cela comprend la mise en place d'outils et de procédures relatifs aux méthodologies d'exploitation, de maintenance, de test, de diagnostic, de gestion des performances, de gestion des changements et des mises à jour.

La sécurité de l'exploitation dépend fortement de son **degré d'industrialisation**, qui est qualifié par le niveau de supervision des applications et l'automatisation des tâches. Bien que relevant de la responsabilité de l'exploitation, ces conditions concernent très directement la conception et la réalisation des applications elles-mêmes et leur intégration dans un système d'information.

Les points clés de la sécurité de l'exploitation sont les suivants :

- gestion du parc informatique ;
- gestion des configurations et des mises à jour ;
- gestion des incidents et suivi jusqu'à leur résolution ;
- plan de sauvegarde ;
- plan de secours ;
- plan de continuité ;
- plan de tests ;
- inventaires réguliers et, si possible, dynamiques ;
- automatisation, contrôle et suivi de l'exploitation ;
- analyse des fichiers de journalisation et de comptabilité ;
- gestion des contrats de maintenance ;

- séparation des environnements de développement, d'industrialisation et de production des applicatifs.

La **maintenance** doit être préventive et régulière, et conduire éventuellement à des actions de réparation, voire de remplacement des matériels défectueux.

Au-delà du coût d'une panne entraînant le remplacement des équipements, le **risque d'exploitation** se traduit par une interruption de service ou une perte de données qui peuvent avoir des conséquences préjudiciables pour l'entreprise.

Notons que le domaine de la sécurité de l'exploitation peut, dans une certaine mesure, rejoindre celui des télécommunications, si l'on considère que c'est au niveau des procédures d'exploitation que l'on fixe les paramètres servant à la facturation de l'utilisation des ressources informatiques ou de télécommunication. Toutefois, ceci est plus spécifiquement relatif à la gestion de la comptabilité et à la maîtrise du risque financier. C'est également lors de l'exploitation des ressources que l'on vérifie l'adéquation du niveau de service offert, par rapport à celui spécifié dans un contrat de service et à sa facturation.

1.2.3 Sécurité logique, applicative et sécurité de l'information

La **sécurité logique** fait référence à la réalisation de mécanismes de sécurité par logiciel contribuant au bon fonctionnement des programmes, des services offerts et à la protection des données. Elle s'appuie généralement sur :

- la qualité des développements logiciels et des tests de sécurité ;
- une mise en œuvre adéquate de la **cryptographie** pour assurer intégrité et confidentialité ;
- des **procédures de contrôle d'accès logique, d'authentification** ;
- des procédures de détection de logiciels malveillants, de détection d'intrusions et d'incidents ;
- mais aussi sur un dimensionnement suffisant des ressources, une certaine redondance ainsi que sur des procédures de **sauvegarde** et de restitution des informations sur des supports fiables, éventuellement spécialement protégés et conservés dans des lieux sécurisés pour les applications et données critiques.

La sécurité logique fait également référence à la **sécurité applicative** qui doit tenir compte des besoins de sécurité dans le développement et l'implémentation des logiciels, et satisfaire à des exigences de contrôle de qualité. Le cycle de vie des logiciels, comme leur intégration dans des environnements de production, doit également satisfaire aux exigences de sécurité en termes de disponibilité, de continuité des services, d'intégrité ou de confidentialité.

La **sécurité applicative** comprend le développement pertinent de solutions logicielles (ingénierie du logiciel, qualité du logiciel) ainsi que leur intégration et exécution harmonieuses dans des environnements opérationnels.

Elle repose essentiellement sur l'ensemble des facteurs suivants :

- une méthodologie de développement (en particulier le respect des normes de développement propres à la technologie employée et aux contraintes d'exploitabilité) ;
- la robustesse des applications ;
- des contrôles programmés ;
- des jeux de tests ;
- des procédures de recettes ;
- l'intégration de mécanismes de sécurité, d'outils d'administration et de contrôle de qualité dans les applications ;
- la sécurité des progiciels (choix des fournisseurs, interface sécurité, etc.) ;
- l'élaboration et la gestion des contrats (les relations avec des sous-traitants éventuels comprenant des clauses d'engagement de responsabilité) ;
- un plan de migration des applications critiques ;
- la validation et l'audit des programmes ;
- la qualité et la pertinence des données ;
- un plan d'assurance sécurité.

Bien **protéger l'information**, c'est avant tout comprendre son rôle, son importance stratégique et l'impact des décisions qu'elle permet de prendre. C'est également assurer son **exactitude** et sa **pérennité** pour le temps nécessaire à son exploitation et à son archivage. Une **classification des données** permet de qualifier leur **degré de sensibilité** (normale, confidentielle, etc.) et de les protéger en fonction de ce dernier. Ainsi, à partir d'un tableau mettant en relation le type de données et leur degré de sensibilité, la nature et le nombre de protections peuvent être déterminés et des mesures de sécurité *ad hoc* développées. Par ailleurs, du point de vue de l'utilisateur, une bonne sécurité doit lui assurer le respect de son intimité numérique (*privacy*) et la protection de ses données personnelles.

1.2.4 Sécurité des infrastructures de télécommunication

La **sécurité des télécommunications** consiste à offrir à l'utilisateur final et aux applications communicantes, une connectivité fiable de « bout en bout ». Cela passe par la réalisation d'une **infrastructure réseau** sécurisée au niveau des accès au réseau et du transport de l'information (sécurité de la gestion des noms et des adresses, sécurité du routage, sécurité des transmissions à proprement parler) et cela s'appuie sur des mesures architecturales adaptées, l'usage de plates-formes matérielles et logicielles sécurisées et une gestion de réseau de qualité.

La sécurité des télécommunications ne peut à elle seule garantir la sécurité des informations. Elle ne constitue qu'un maillon de la chaîne sécuritaire car il est également impératif de sécuriser l'**infrastructure informatique** dans laquelle s'exécutent les programmes. Pris au sens large, cela comprend la sécurité physique et environnementale des systèmes (poste de travail de l'utilisateur, serveur ou système d'information (figure 1.4).

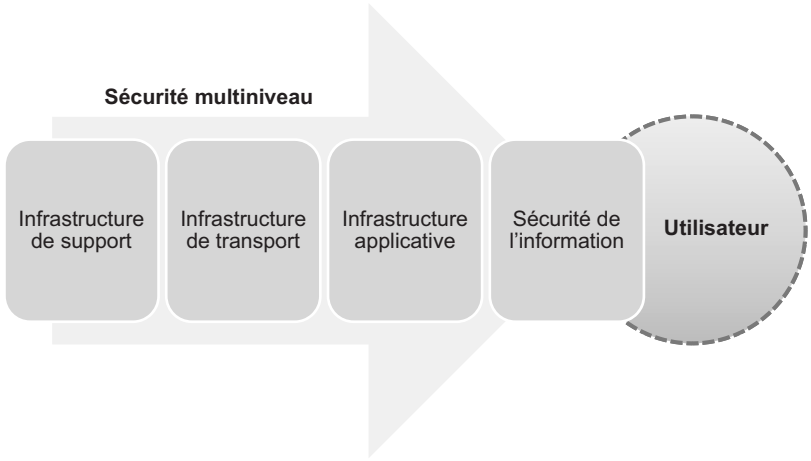

Figure 1.4 – Sécurité des infrastructures de télécommunication.

Pour que les infrastructures informatiques et télécoms soient cohérentes, performantes et sécurisées de manière optimale, l'**infrastructure de sécurité** (outils, procédures, mesures) et la gestion de la sécurité doivent être réalisées de manière sécurisée. Les solutions de sécurité doivent être également sécurisées (notion de **récursivité de la sécurité**).

La sécurité des télécommunications est peu différente de celle que l'on doit mettre en œuvre pour protéger les systèmes. Bien que vulnérables, les réseaux de télécommunication ne le sont pas plus que les systèmes d'extrémité ou que les personnes qui les conçoivent, les gèrent ou les utilisent.

Un environnement informatique et de télécommunication sécurisé implique la sécurisation de tous les éléments qui le composent. La sécurité globale est toujours celle du maillon le plus faible. Implanter des mécanismes de chiffrement pour rendre les données transférées confidentielles est de peu d'utilité si d'aucuns peuvent y accéder lorsqu'elles sont manipulées par des plates-formes matérielles et logicielles non correctement sécurisées.

L'implantation de mesures de sécurité doit répondre à des besoins de sécurité clairement identifiés à la suite d'une **analyse des risques** spécifiquement encourus par une organisation. Les besoins s'expriment en termes d'exigences de sécurité à satisfaire au travers d'une **politique de sécurité** (cf. chapitre 4). De plus, un système sécurisé, mobilisant d'importants moyens sécuritaires, aussi pertinents soient-ils, ne pourra être efficace que s'il s'appuie sur des personnes intègres et sur un code d'utilisation adéquat des ressources informatiques pouvant être formalisé par une **charte** de sécurité. Souplesse et confiance réciproque ne peuvent se substituer à la rigueur et au contrôle imposés par le caractère stratégique des enjeux économiques et politiques que doivent satisfaire les systèmes d'information et les réseaux de télécommunications.

Il ne faut jamais oublier que dans le domaine de la sécurité, la confiance n'exclut pas le contrôle ! La sécurité, en tant que propriété d'un système, peut être qualifiable (notion d'assurance de sécurité qui fait référence à la quantification de la qualité de la sécurité). En revanche, la confiance est une relation binaire entre deux entités qui relève du sentiment.

1.2.5 Cybersécurité

Désormais, un grand nombre d'activités sont réalisées *via* Internet et le cyberespace. La racine « **cyber** » provient du mot **cybernétique**, qui avait été formé en français en 1834 pour désigner la « science du gouvernement », à partir du grec *Kubernêtiké*, signifiant « diriger, gouverner ». Terme repris en 1948, par Norman Wiener aux États-Unis et qui a donné naissance à la cybernétique (*cybernetics*), science constituée par l'ensemble des théories relatives au contrôle, à la régulation et à la communication entre l'être vivant et la machine.

Depuis lors, le préfixe « cyber » est devenu relatif à l'environnement informatique et aux activités rendues possibles par les technologies du numérique et Internet. Le cyberespace (l'ensemble des infrastructures numériques, des données et des services mis en réseaux) est une extension de notre espace naturel qui reflète notre société avec ses réalités politique, économique, sociale et culturelle. Mais contrairement à la terre, à la mer, à l'air et à l'espace-extra atmosphérique, le cyberespace est une pure création de l'être humain qui ne relève pas de la nature.

La cybersécurité concerne la sécurité informatique et des réseaux des environnements connectés à Internet et accessibles *via* le cyberespace. Elle peut être mise en défaut, entre autres, par des cyberattaques informatiques. Du fait de l'usage extensif d'Internet, de nouvelles menaces sont apparues générant des risques additionnels dont les impacts, de niveaux d'importance variables, peuvent affecter les individus, les organisations ou les États.

1.3 Différentes facettes de la sécurité

1.3.1 Cybermenace et cyberrisque

Une **menace** est un signe par lequel se manifeste ce que l'on doit craindre. Une cybermenace est une menace qui, si elle se concrétisait, affecterait le bon fonctionnement des ordinateurs, des réseaux de télécommunication et de tous les services et activités humaines qui en dépendent. Elle est liée au fait que les systèmes informatiques et les équipements électroniques sont vulnérables et, dans la mesure où ils sont connectés et accessibles *via* Internet, peuvent constituer des cibles de cyberattaques. Les cybermenaces sont le plus souvent associées à l'usage malveillant des technologies Internet et à la criminalité (notion de cybercriminalité). De nombreuses cybermenaces existent, elles recouvrent des réalités diverses en fonction des cibles touchées (ordinateur personnel, infrastructure informatique et télécom d'une organisation publique ou privée, infrastructures critiques, système de contrôle et d'acquisition de données

SCADA- [*Supervisory Control And Data Acquisition*]), de leurs origines (civile ou militaire), de leurs auteurs (vandale, criminel, activiste, terroriste, mercenaire, etc.). Il est primordial de pouvoir identifier au plus tôt les indicateurs qui permettent d'anticiper l'apparition de cybermenaces, les signaux faibles, afin d'empêcher leur réalisation ou de diminuer leur occurrence de survenue et la gravité de leurs impacts. Le risque est un danger plus ou moins prévisible qui est fonction des menaces et des vulnérabilités existantes.

Dès lors que des menaces et des vulnérabilités existent, il y a un risque relatif à l'éventualité qu'un événement non sollicité survienne et provoque des conséquences préjudiciables. Toutefois, un risque peut également être porteur d'opportunités et générer des bénéfices pour l'entité qui l'assume.

L'évaluation d'une menace tient compte de l'ampleur et de l'importance des dégâts qu'elle peut occasionner si elle devient réalité. Cela s'exprime le plus souvent par un degré de dangerosité, qui de manière habituelle peut se catégoriser en trois niveaux : faible, moyen et élevé. Dans une démarche de gestion de risques, il est important de pouvoir identifier le plus correctement possible les menaces et leurs combinaisons, ce qui est parfois difficile. Prises isolément, des menaces de niveau faible ou moyen ne sont pas forcément graves. En revanche, associées et combinées entre elles dans des scénarios de réalisation particuliers de risques et d'interdépendances, elles peuvent devenir extrêmement préjudiciables. En tout état de cause, les personnes, les institutions et l'État doivent être préparés à la maîtrise des risques « cyber », à la gestion de crises parfois complexes lors de la concrétisation des menaces, afin de pouvoir continuer à fonctionner et revenir à la situation normale d'avant la crise (notion de résilience).

Un **faible niveau** de dangerosité relève généralement de la nuisance. Entre dans cette catégorie, la réception de messages publicitaires, de lettres d'information envoyées sans le consentement initial de l'internaute, de spams (pourriels), surchargeant la boîte aux lettres électronique des usagers, qui se trouvent alors contraints de trier les messages non sollicités de ceux qui les concernent vraiment, de les effacer ou d'effectuer éventuellement des demandes de désabonnement, etc. Cela entraîne des pertes de temps et d'énergie et divers désagréments avec parfois la perte de messages pertinents du fait qu'ils ont été noyés parmi les spams. Le spam publicitaire pour des médicaments contrefaits n'est pas forcément grave, à moins qu'il n'entraîne la prise de produits inefficaces ou néfastes à la santé des personnes.

Les menaces de **niveau moyen** de dangerosité sont celles dont les impacts sont maîtrisables, mais nécessitent des ressources pour diminuer leur survenue ou pour réagir après incident. C'est le cas, par exemple, lorsque des programmes nuisibles se sont installés dans la machine de l'utilisateur et dont la charge de malveillance ne s'est pas encore déclenchée. Il peut s'agir par exemple d'un « cheval de Troie » : une fois installé dans la machine, ce virus permet à des entités externes et hostiles de prendre le contrôle de l'ordinateur infecté pour espionner, voler, détruire des données ou lancer des attaques informatiques sur d'autres systèmes.

La réalisation d'une menace de **niveau élevé** de dangerosité entraîne des dysfonctionnements, des dégâts et des coûts fortement préjudiciables au fonctionnement des organisations et de la société.

Il ne suffit pas de cartographier l'ensemble des cybermenaces envisageables, ni de se protéger des menaces les plus dangereuses et les plus probables. Il faut tenir compte de la corrélation et de l'interaction des menaces, dans des scénarios de risques possibles (approche combinatoire des risques). Bien qu'il soit toujours difficile de tout prévoir, la part d'imprévisibilité ou d'ingéniosité des malveillants peut parfois être anticipée, s'il existe une bonne connaissance du contexte, des valeurs à protéger et de leurs vulnérabilités.

La vulnérabilité des systèmes informatiques est avérée, révélant leur caractère non robuste et l'existence de failles (logicielles ou matérielles) exploitables pour effectuer des actions malveillantes. Ainsi par exemple, il peut exister des :

- défaillances de conception, de mise en œuvre, de gestion ou d'utilisation des environnements informatiques ;
- déficits ou absences de comportement averti de l'utilisateur, d'hygiène informatique et sécuritaire ;
- carences ou limites des solutions de sécurité. Ainsi par exemple, des logiciels antivirus, même à jour, ne détectent que les virus connus. Ils ne sont d'aucune utilité pour de nouveaux virus.

Si une menace a un fort degré de dangerosité mais qu'elle n'a qu'une chance infime de se concrétiser par une attaque, ou si inversement une menace a de fortes chances de se concrétiser par des attaques, mais à faible degré de dangerosité, elles ne sont pas à considérer avec autant de soucis que des attaques à degré moyen de dangerosité mais dont la probabilité d'occurrence est importante. Il est alors nécessaire de pouvoir définir le paramètre de **probabilité d'occurrence** en classant cette probabilité en quatre niveaux :

- la menace ne devrait pas se concrétiser par une attaque ;
- la menace pourrait bien se concrétiser ;
- la menace devrait se concrétiser ;
- la menace va se concrétiser et se concrétiser à plusieurs reprises.

Ainsi, en combinant la probabilité d'occurrence d'une attaque et sa dangerosité, il est possible d'attribuer un degré d'importance à une information pour mieux la protéger.

1.3.2 Diriger la sécurité

La sécurité informatique d'une organisation doit s'appréhender d'une **manière globale et stratégique** (notion de stratégie de sécurité) et s'appuie sur :

- la définition d'une politique de sécurité ;
- la motivation et la formation du personnel ;
- la mise en place de mesures proactives et réactives ;

- l'optimisation de l'usage des technologies de l'information et des communications (TIC) ainsi que de celui des solutions de sécurité.

L'utilisation seule d'outils de sécurité ne peut pas résoudre les problèmes de sécurité d'une organisation. En aucun cas, ils ne se substituent à une **gestion cohérente** de l'appréhension des risques et des problématiques de sécurité. Les besoins de sécurité doivent être clairement identifiés et constamment réévalués au regard des risques encourus et de leur évolution.

La prolifération désordonnée d'outils de sécurité non intégrés dans un processus continu de gestion ne peut qu'entraver l'usage, alourdir l'exploitation ou encore dégrader les performances d'un système d'information sans offrir un niveau de sécurité adapté.

La sécurité informatique passe également par une gestion rigoureuse des ressources humaines, des systèmes informatiques, des réseaux, des locaux, de l'infrastructure environnementale, et des mesures de sécurité. La **maîtrise de la sécurité informatique** est avant tout une question de gestion dont les outils, technologies ou solutions de sécurité constituent une partie liée à la réalisation opérationnelle des environnements sécurisés. Des outils comme ceux de chiffrement ou les pare-feu ne permettent pas de sécuriser correctement un environnement à protéger s'ils ne sont pas inscrits dans une démarche de gestion précise des risques et s'ils ne sont pas accompagnés de procédures qui régissent leur utilisation ou configuration. Ainsi, piloter la sécurité correspond à la volonté de **maîtriser les risques** liés à l'usage des technologies de l'information, les coûts engendrés pour se protéger des menaces et au déploiement des moyens nécessaires pour gérer les incidents ou les situations de crise, pour réagir à une situation non sollicitée mettant en danger la performance du système d'information et celle de l'organisation. Gouverner la sécurité informatique s'inscrit dans une dimension humaine, organisationnelle, managériale et économique des organisations répondant à une volonté politique de leur direction pour maîtriser les risques et protéger les valeurs.

Ainsi, la sécurité repose sur la complémentarité et la cohérence de ces dimensions. **Elle n'est jamais acquise définitivement**. La constante évolution des besoins, des systèmes, des menaces ou des risques rend instable toute mesure de sécurité. Cela se traduit par un problème de gestion de la qualité constante dans un environnement dynamique et évolutif. Dans ce contexte, la sécurité informatique ne peut s'appréhender que comme un **processus continu de gestion** afin de répondre de manière optimale (en termes de coût et de niveau de sécurité) aux besoins de production de l'organisation et de protection de ses actifs.

Pour beaucoup d'entreprises, l'outil informatique est un levier essentiel dans leur activité et leur développement. Dans ce cas, l'indisponibilité de l'outil informatique ou son dysfonctionnement constituent un risque majeur. Il peut toutefois être réduit par une gestion rigoureuse des ressources et de leur sécurité.

La démarche de sécurité informatique comme la démarche qualité participent à satisfaire les exigences de rentabilité et de compétitivité des entreprises dont la performance peut être accrue par un système d'information correctement sécurisé.

En effet, il ne faut pas perdre de vue la finalité de celui-ci qui est de permettre à l'organisation qui le met en œuvre de réaliser des services ou des produits dont la qualité et les critères de sécurité sont garantis.

1.3.3 Importance du juridique dans la sécurité des systèmes d'information

La **responsabilité** des acteurs (responsable sécurité ou directeur de systèmes d'information par exemple) est de plus en plus invoquée lors de sinistre où les ressources informatiques qu'ils gèrent sont l'objet ou le moyen d'une fraude. Il est nécessaire que les responsables puissent démontrer que des mesures suffisantes de protection du système d'information et des données ont été mises en œuvre afin de se protéger contre un **délit de manquement à la sécurité** (à défaut d'une obligation de résultat, il existe une **obligation de moyens** concernant la sécurité). L'article 1383 du Code civil français nous rappelle que chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence.

Les responsables d'entreprises eux-mêmes doivent être extrêmement attentifs à l'égard du droit concernant les technologies et les traitements numériques, et s'assurer que leur système d'information est en conformité juridique et réglementaire. Désormais, les enjeux juridiques liés à la sécurité informatique sont devenus prépondérants et doivent être pris en compte dans la mise en place de solutions de sécurité, qu'ils soient relatifs à la conservation des données, à la responsabilité des prestataires ou des hébergeurs, à la gestion des données personnelles des clients, à la surveillance des événements informatiques générés par l'activité des employés, à la propriété intellectuelle, aux contrats informatiques ou encore à la signature électronique par exemple. L'**intelligence juridique** devient l'un des facteurs clés du succès de la réalisation de la sécurité informatique des organisations.

Le droit dans le domaine du numérique peut devenir un atout stratégique pour les organisations qui le maîtrisent.

1.3.4 Éthique et formation

Il est nécessaire d'éduquer, d'informer, de sensibiliser et de former aux technologies de traitement de l'information et des communications, et non uniquement à la sécurité et aux mesures de dissuasion. La sensibilisation aux problématiques de sécurité ne doit pas se limiter à la promotion d'une certaine **culture de la sécurité** et de son éthique. En amont de la culture sécuritaire, il doit exister une véritable culture de l'informatique.

Une **éthique sécuritaire** et des bonnes pratiques doivent être développées au sein de l'organisation. Cela doit se traduire par une **charte informatique** reconnue par chacun et par un engagement personnel à la respecter, quelle que soit sa place dans la hiérarchie.

Cette charte déontologique d'utilisation des ressources informatiques et des services Internet doit notamment comprendre des clauses relatives :

- à son domaine d'application ;
- à la définition des moyens et des procédures d'accès aux ressources informatiques et aux services Internet ;
- aux règles d'utilisation professionnelle, rationnelle et loyale des ressources ;
- aux procédures de sécurité ;
- au bon usage des ressources (y compris des données manipulées et transférées) ;
- aux conditions de confidentialité ;
- au respect de la législation concernant les logiciels ;
- au respect de l'intégrité des systèmes informatiques ;
- au rappel des principales lois en vigueur à respecter ;
- aux moyens de contrôle du respect de la charte (surveillance des employés) ;
- aux sanctions encourues en cas de non-respect.

En ce qui concerne la surveillance, les moyens mis en œuvre doivent être proportionnels aux buts recherchés et le personnel de l'organisation et leurs représentants doivent être avertis de l'existence des moyens utilisés.

Des **actions de sensibilisation, d'information ou de formation** sur les enjeux, les risques et les mesures préventives et dissuasives de sécurité sont nécessaires pour éduquer l'ensemble du personnel à adopter une démarche sécurité (cohérence des technologies, des procédures, des compétences humaines). La signature de la **charte informatique** ou **charte de sécurité** doit s'accompagner de moyens fournis aux signataires afin qu'ils puissent la respecter.

1.3.5 Architecture de sécurité

L'**architecture de sécurité** reflète l'ensemble des dimensions organisationnelle, juridique, humaine et technologique de la sécurité informatique à prendre en considération pour une appréhension complète de la sécurité d'une organisation (figure 1.5). Définir une architecture globale de la sécurité permet de visualiser la dimension générale et la nature transversale de la sécurité informatique d'une entreprise et d'identifier ses diverses facettes et composantes afin de pouvoir les développer de façon cohérente, complémentaire et harmonieuse. Cela facilite l'intégration de mesures, de procédures et d'outils de sécurité.

Une démarche d'assurance des actifs, de gestion des risques, comme le respect des procédures, la formation, le comportement éthique des utilisateurs ou la conformité réglementaire sont autant de points à identifier dans un cadre d'architecture de sécurité. Ainsi, les critères de la sécurité pourront être réalisés judicieusement par le biais de mesures et de procédures complémentaires.

En outre, disposer d'un cadre architectural permet de disposer d'un **référentiel de sécurité** qui facilite la réalisation opérationnelle de la sécurité ainsi que son évaluation lors d'audits. Cette approche permet également de pouvoir identifier les critères minimaux de sécurité pour chacun des éléments ainsi que leurs interactions et les