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 978-2-10-075224-9

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

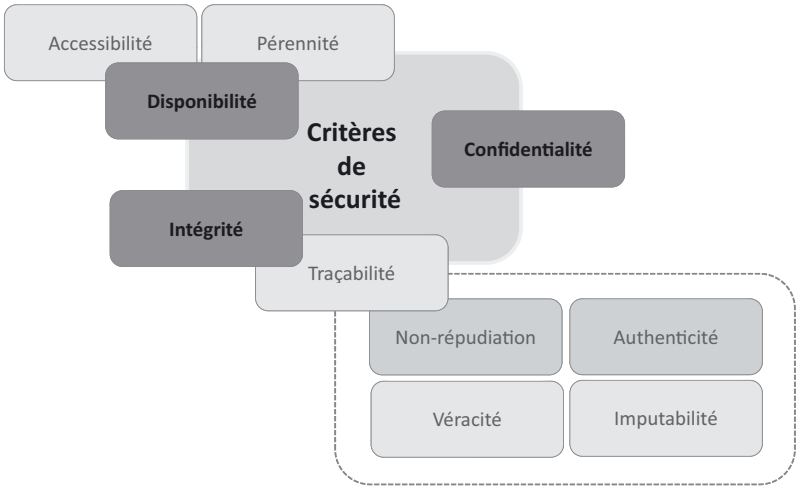

Figure 1.1 – **Critères de sécurité.**

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

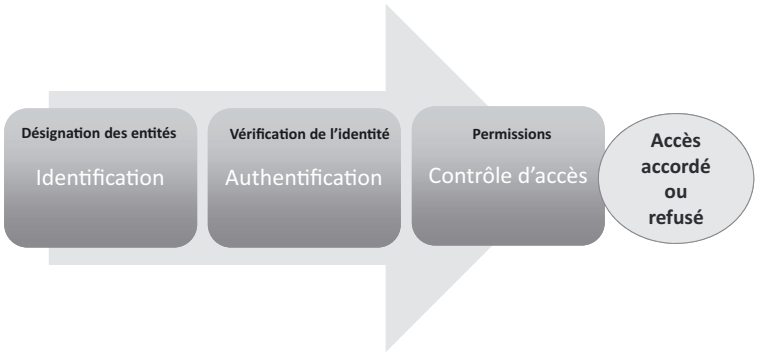

Figure 1.2 – Identification et authentification.

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