

Cybersécurité **sécurité** **informatique** **et réseaux**

Solange Ghernaoui

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

5^e 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

Le pictogramme qui figure ci-contre mérite une explication. Son objet est d'alerter le lecteur sur la menace que représente pour l'avenir de l'écrit, particulièrement dans le domaine de l'édition technique et universitaire, le développement massif du photocopillage.

Le Code de la propriété intellectuelle du 1^{er} juillet 1992 interdit en effet expressément la photocopie à usage collectif sans autorisation des ayants droit. Or, cette pratique s'est généralisée dans les établissements

d'enseignement supérieur, provoquant une baisse brutale des achats de livres et de revues, au point que la possibilité même pour

les auteurs de créer des œuvres nouvelles et de les faire éditer correctement est aujourd'hui menacée. Nous rappelons donc que toute reproduction, partielle ou totale, de la présente publication est interdite sans autorisation de l'auteur, de son éditeur ou du Centre français d'exploitation du

droit de copie (CFC, 20, rue des Grands-Augustins, 75006 Paris).



© Dunod, 2006, 2008, 2011, 2013, 2016

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

ISBN 978-2-10-075224-9

Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5, 2^o et 3^o a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective » et, d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

Cette représentation ou reproduction, par quelque procédé que ce soit, constituerait donc une contrefaçon sanctionnée par les articles L. 335-2 et suivants du Code de la propriété intellectuelle.

TABLE DES MATIÈRES

Avant-propos	XI
Chapitre 1 • Sécurité informatique et cybersécurité	1
1.1 Objectifs de sécurité	1
1.1.1 Disponibilité	1
1.1.2 Intégrité	3
1.1.3 Confidentialité	3
1.1.4 Fonctions additionnelles	4
1.2 Domaines d'application	6
1.2.1 Sécurité physique et environnementale	6
1.2.2 Sécurité de l'exploitation	7
1.2.3 Sécurité logique, applicative et sécurité de l'information	8
1.2.4 Sécurité des infrastructures de télécommunication	9
1.2.5 Cybersécurité	11
1.3 Différentes facettes de la sécurité	11
1.3.1 Cybermenace et cyberrisque	11
1.3.2 Diriger la sécurité	13
1.3.3 Importance du juridique dans la sécurité des systèmes d'information	15
1.3.4 Éthique et formation	15
1.3.5 Architecture de sécurité	16
1.3.6 Servir une vision de société	18
Exercices	21
Solutions	21
Chapitre 2 • Cybercriminalité et sécurité informatique	27
2.1 Comprendre la menace d'origine criminelle pour une meilleure sécurité	27
2.2 Infrastructure Internet et vulnérabilités exploitées à des fins criminelles	28
2.2.1 Éléments de vulnérabilité d'une infrastructure Internet	28
2.2.2 Internet comme facteur de performance pour le monde criminel	28
2.2.3 Internet au cœur des stratégies criminelles	32
2.2.4 Risque d'origine criminelle et insécurité technologique	33
2.3 Les cyberrisques	34
2.3.1 Principaux risques pour les individus	34
2.3.2 Principaux risques pour les organisations	36
2.3.3 Principaux risques pour la nation et la société	37
2.3.4 Internet, facteur de rapprochement des mondes criminel et terroriste	39

2.3.5 Guerre sémantique et cyberhactivisme	40
2.4 Crime informatique et cybercriminalité	41
2.4.1 Éléments de définition	41
2.4.2 Écosystème cybercriminel	43
2.4.3 Marchés noirs de la cybercriminalité	45
2.5 Attaques informatiques via Internet	47
2.5.1 Étapes de réalisation d'une cyberattaque	47
2.5.2 Attaques actives et passives	48
2.5.3 Attaques fondées sur l'usurpation de mots de passe	49
2.5.4 Attaques fondées sur le leurre	52
2.5.5 Attaques fondées sur le détournement des technologies	53
2.5.6 Attaques fondées sur la manipulation de l'information	54
2.6 Faire face à la cybercriminalité	55
2.6.1 Chiffre noir de la cybercriminalité	55
2.6.2 Culture de la sécurité	55
2.6.3 Limites des solutions de sécurité	58
2.6.4 Contribuer à lutter contre la cybercriminalité et à diminuer le risque d'origine cybercriminelle	58
Exercices	61
Solutions	62
Chapitre 3 • Gouvernance et stratégie de sécurité	67
3.1 Gouverner la sécurité	67
3.1.1 Contexte	67
3.1.2 Principes de base de la gouvernance de la sécurité de l'information	68
3.2 Gérer le risque informationnel	70
3.2.1 Définitions	70
3.2.2 Principes de gestion	70
3.2.3 Projet d'entreprise orienté vers la gestion des risques	71
3.3 Connaître les risques pour les maîtriser	71
3.4 Vision stratégique de la sécurité	74
3.4.1 Fondamentaux	74
3.4.2 Mission de sécurité	76
3.4.3 Principes de base	76
3.4.4 Conditions de succès	77
3.4.5 Approche pragmatique	78
3.4.6 Bénéfices	78
3.4.7 Aspects économiques	79
3.5 Définir une stratégie de sécurité	81
3.5.1 Stratégie générale	81
3.5.2 Compromis et bon sens	81
3.5.3 Responsabilité	83
3.5.4 Nouveaux risques, nouveaux métiers	84
3.6 Organiser et diriger	85
3.6.1 Organisation structurelle	85
3.6.2 Acteurs et compétences	87

3.7	Prise en compte des besoins juridiques	89
3.7.1	Infractions, responsabilités et obligations de moyens	89
3.7.2	Prendre en compte la sécurité en regard de la législation	92
3.7.3	La confiance passe par le droit, la conformité et la sécurité	93
3.8	Principes d'intelligence économique	95
3.9	Prise en compte des risques cachés	96
3.9.1	Externalisation et cloud computing	96
3.9.2	Droits fondamentaux et libertés civiles	97
3.9.3	Cyberrésilience, risque écologique et écosystème numérique	98
	Exercices	101
	Solutions	102
	Chapitre 4 • Politique de sécurité	109
4.1	De la stratégie à la politique de sécurité	109
4.2	Propriétés d'une politique de sécurité	111
4.3	Méthodes et normes contribuant à la définition d'une politique de sécurité	112
4.3.1	Principales méthodes françaises	112
4.3.2	Normes internationales ISO de la série 27000	114
4.3.3	Méthodes et bonnes pratiques	125
4.3.4	Modèle formel de politique de sécurité	126
4.4	De la politique aux mesures de sécurité	126
4.4.1	Classification des ressources	126
4.4.2	Mesures de sécurité	127
4.5	Continuité et gestion de crises	129
4.5.1	Définitions et objectifs	129
4.5.2	Démarche de déploiement d'un plan de continuité	129
4.5.3	Plans de continuité et de reprise	130
4.5.4	Dispositifs de secours et plan de secours	133
4.5.5	Plan d'action	136
4.6	Place de l'audit des systèmes d'information en matière de sécurité	137
4.6.1	Audit des systèmes d'information	137
4.6.2	Référentiel CobiT	138
4.7	Mesurer l'efficacité de la sécurité	139
4.7.1	Métriques de sécurité	139
4.7.2	Modèle de maturité	141
4.8	Certification des produits de sécurité	142
4.8.1	Critères Communs	142
4.8.2	Acteurs concernés par les Critères Communs	143
4.8.3	Principales limites des Critères Communs	144
4.8.4	Principes de base des Critères Communs	144
4.8.5	Vocabulaire et concepts	145
	Exercices	148
	Solutions	148

Chapitre 5 • La sécurité par le chiffrement	153
5.1 Principes généraux	153
5.1.1 Vocabulaire	153
5.1.2 Algorithmes et clés de chiffrement	154
5.2 Principaux systèmes cryptographiques	155
5.2.1 Système de chiffrement symétrique	156
5.2.2 Système de chiffrement asymétrique	157
5.2.3 Quelques considérations sur la cryptanalyse	159
5.2.4 Cryptographie quantique	161
5.2.5 Principaux algorithmes et techniques	163
5.3 Services offerts par la mise en œuvre du chiffrement	165
5.3.1 Optimisation du chiffrement par une clé de session	165
5.3.2 Vérifier l'intégrité des données	166
5.3.3 Authentifier et signer	167
5.3.4 Rendre confidentiel et authentifier	170
5.3.5 Offrir un service de non-répudiation	170
5.4 Infrastructure de gestion de clés	170
5.4.1 Clés secrètes	170
5.4.2 Objectifs d'une infrastructure de gestion de clés	171
5.4.3 Certificat numérique	172
5.4.4 Organismes de certification	174
5.4.5 Exemple de transaction sécurisée par l'intermédiaire d'une PKI	175
5.4.6 Cas particulier d'autorité de certification privée	176
5.4.7 Limites des solutions basées sur des PKI	177
5.5 Apport des blockchains	179
Exercices	180
Solutions	181
Chapitre 6 • La sécurité des infrastructures de télécommunication	185
6.1 Protocole IPv4	185
6.2 Protocoles IPv6 et IPSec	188
6.2.1 Principales caractéristiques d'IPv6	188
6.2.2 Principales caractéristiques d'IPSec	189
6.2.3 En-tête d'authentification (AH)	190
6.2.4 En-tête de confidentialité-authentification (ESP)	190
6.2.5 Association de sécurité	191
6.2.6 Implantation d'IPSec	192
6.2.7 Gestion des clés de chiffrement	193
6.2.8 Modes opératoires	194
6.2.9 Réseaux privés virtuels	194
6.3 Sécurité du routage	195
6.3.1 Contexte	195
6.3.2 Principes généraux d'adressage	196
6.3.3 Gestion des noms	198
6.3.4 Principes généraux de l'acheminement des données	203
6.3.5 Sécurité des routeurs et des serveurs de noms	205

6.4	Sécurité et gestion des accès	206
6.4.1	Degré de sensibilité et accès aux ressources	206
6.4.2	Principes généraux du contrôle d'accès	207
6.4.3	Démarche de mise en place du contrôle d'accès	209
6.4.4	Rôle et responsabilité d'un fournisseur d'accès dans le contrôle d'accès	209
6.4.5	Certificats numériques et contrôles d'accès	209
6.4.6	Gestion des autorisations d'accès via un serveur de noms	211
6.4.7	Contrôle d'accès basé sur des données biométriques	212
6.5	Sécurité des réseaux	214
6.5.1	Protection de l'infrastructure de transmission	214
6.5.2	Protection du réseau de transport	215
6.5.3	Protection des flux applicatifs et de la sphère de l'utilisateur	215
6.5.4	Protection optimale	216
6.5.5	Sécurité du cloud	217
	Exercices	220
	Solutions	221
	Chapitre 7 • La sécurité des réseaux sans fil	225
7.1	Mobilité et sécurité	225
7.2	Réseaux cellulaires	226
7.3	Sécurité des réseaux GSM	227
7.3.1	Confidentialité de l'identité de l'abonné	227
7.3.2	Authentification de l'identité de l'abonné	228
7.3.3	Confidentialité des données utilisateur et de signalisation	230
7.3.4	Limites de la sécurité GSM	231
7.4	Sécurité des réseaux GPRS	231
7.4.1	Confidentialité de l'identité de l'abonné	231
7.4.2	Authentification de l'identité de l'abonné	231
7.4.3	Confidentialité des données de l'utilisateur et de signalisation	232
7.4.4	Sécurité du cœur du réseau GPRS	233
7.5	Sécurité des réseaux UMTS	234
7.5.1	Confidentialité de l'identité de l'abonné	234
7.5.2	Authentification mutuelle	234
7.5.3	Confidentialité des données utilisateurs et de signalisation	237
7.5.4	Intégrité des données de signalisation	238
7.6	Réseaux locaux sans fil 802.11	239
7.6.1	Principes de base	239
7.6.2	Sécurité 802.11	240
7.6.3	Renforcer la sécurité (norme 802.11i)	242
7.7	Réseaux personnels sans fil	248
	Exercices	249
	Solutions	250
	Chapitre 8 • La sécurité par pare-feu et la détection d'incidents	255
8.1	Sécurité d'un intranet	255
8.1.1	Risques associés	255

8.1.2 Éléments de sécurité d'un intranet	256
8.2 Principales caractéristiques d'un pare-feu	258
8.2.1 Fonctions de cloisonnement	258
8.2.2 Fonction de filtre	260
8.2.3 Fonctions de relais et de masque	262
8.2.4 Critères de choix d'un pare-feu	263
8.3 Positionnement d'un pare-feu	264
8.3.1 Architecture de réseaux	264
8.3.2 Périmètre de sécurité	265
8.4 Système de détection d'intrusion et de prévention d'incidents (IDS)	267
8.4.1 Définitions	267
8.4.2 Fonctions et mode opératoire	267
8.4.3 Attaques contre les systèmes de détection d'intrusion	272
Exercices	273
Solutions	273
Chapitre 9 • La sécurité des applications et des contenus	277
9.1 Messagerie électronique	277
9.1.1 Une application critique	277
9.1.2 Risques et besoins de sécurité	278
9.1.3 Mesures de sécurité	278
9.1.4 Cas particulier du spam	279
9.2 Protocoles de messagerie sécurisés	281
9.2.1 S/MIME	281
9.2.2 PGP	282
9.2.3 Recommandations pour sécuriser un système de messagerie	283
9.3 Sécurité de la téléphonie Internet	284
9.3.1 Contexte et éléments d'architecture	284
9.3.2 Éléments de sécurité	286
9.4 Mécanismes de sécurité des applications Internet	287
9.4.1 Secure Sockets Layer (SSL) – Transport Layer Security (TLS)	287
9.4.2 Secure-HTTP (S-HTTP)	289
9.4.3 Authentification des applications	289
9.5 Sécurité du commerce électronique et des paiements en ligne	290
9.5.1 Contexte du commerce électronique	290
9.5.2 Protection des transactions commerciales	290
9.5.3 Risques particuliers	291
9.5.4 Sécuriser la connexion entre l'acheteur et le vendeur	291
9.5.5 Sécurité des paiements en ligne	292
9.5.6 Sécuriser le serveur	294
9.5.7 Notions de confiance et de contrat dans le monde virtuel	295
9.6 Sécurité des documents XML	296
9.6.1 Risques et besoins de sécurité liés à l'usage de documents XML	296
9.6.2 Signatures XML	297
9.6.3 Chiffrement/déchiffrement XML	299

9.7 Marquage de documents et droits numériques	299
9.7.1 Tatouage numérique de documents	299
9.7.2 Gestion des droits numériques	300
9.8 Le BYOD, les réseaux sociaux et la sécurité	302
Exercices	305
Solutions	306
Chapitre 10 • La sécurité par la gestion de réseau	311
10.1 Intégration des technologies de sécurité	311
10.1.1 Interopérabilité et cohérence globale	311
10.1.2 Externalisation et investissement	312
10.2 Gestion de systèmes et réseaux	313
10.3 Gestion du parc informatique	314
10.3.1 Objectifs et fonctions	314
10.3.2 Quelques recommandations	315
10.4 Gestion de la qualité de service réseau	316
10.4.1 Indicateurs de qualité	316
10.4.2 Évaluation et efficacité	317
10.5 Gestion comptable et facturation	318
10.6 Gestion opérationnelle d'un réseau	318
10.6.1 Gestion des configurations	319
10.6.2 Surveillance et optimisation	320
10.6.3 Gestion des performances	320
10.6.4 Maintenance et exploitation	321
10.6.5 Supervision et contrôle	323
10.6.6 Documentation	324
10.7 Gestion de systèmes par le protocole SNMP	325
Exercices	328
Solutions	335
Glossaire	345
Index	364

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'impudabilité 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)

SÉCURITÉ INFORMATIQUE ET CYBERSÉCURITÉ

1

PLAN

- 1.1 Objectifs de sécurité et fonctions associées
- 1.2 Domaines d'application de la sécurité informatique
- 1.3 Différentes facettes de la sécurité

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

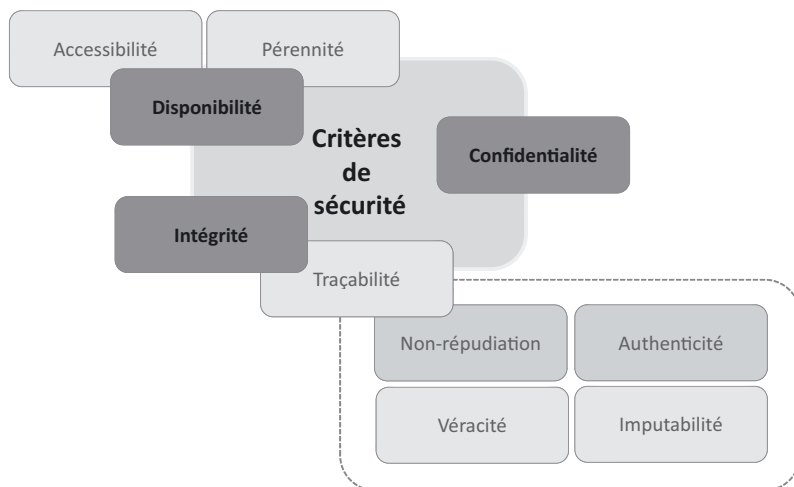


Figure 1.1 – Critères de sécurité.

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'intégrité² 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'accès⁴) 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 sécurité⁵, 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

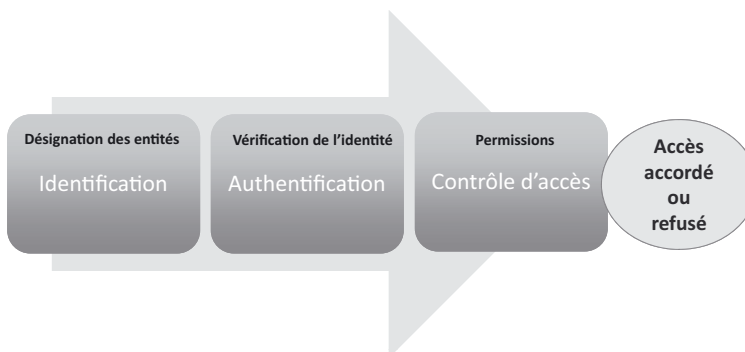


Figure 1.2 – Identification et authentification.