

Cybersécurité sécurité informatique et réseaux

Solange Ghernaouti

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 photocollage. 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).

DANGER


© 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^e et 3^e al, 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

Cybersécurité, sécurité informatique et réseaux

2.3.5 Guerre sémantique et cyberhacktivisme	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

Table des matières

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

Cybersécurité, sécurité informatique et réseaux

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

Table des matières

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

Cybersécurité, sécurité informatique et réseaux

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

Table des matières

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'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)

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

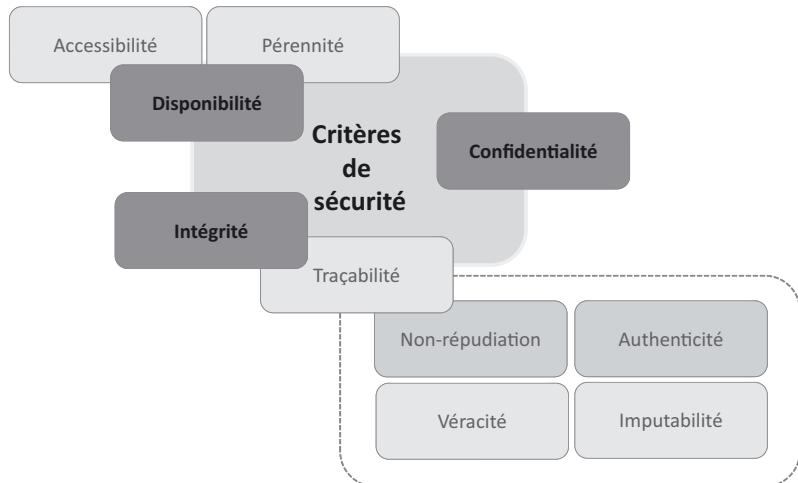


Figure 1.1 – Critères de sécurité.

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 efficace** 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 intelligibles 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

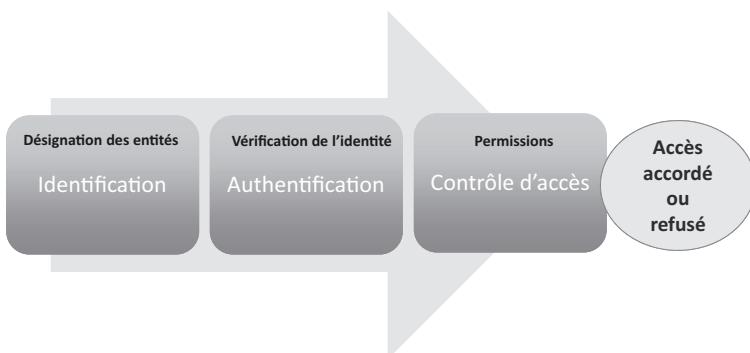


Figure 1.2 – Identification et authentification.

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.

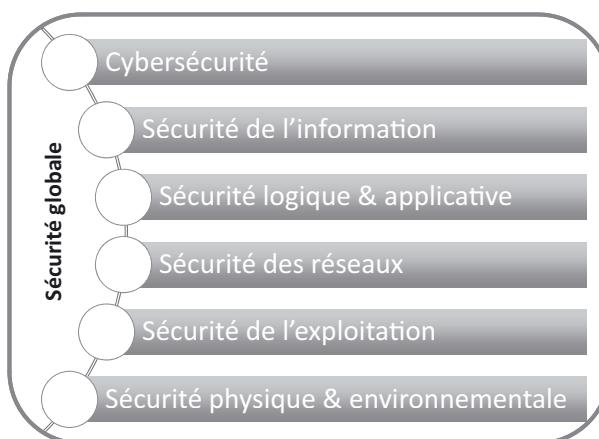


Figure 1.3 - Domaines d'application de la sécurité.

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).

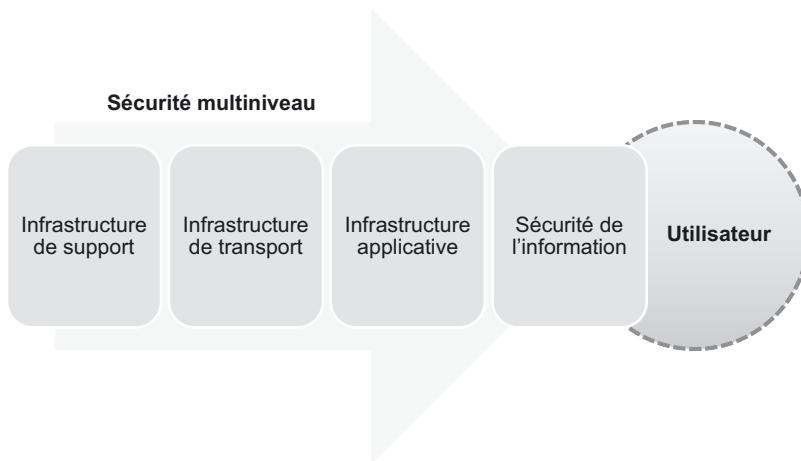


Figure 1.4 – Sécurité des infrastructures de télécommunication.

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'extrême 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 *Kubernétiké*, 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 :

- défaiillances 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'apprehender 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

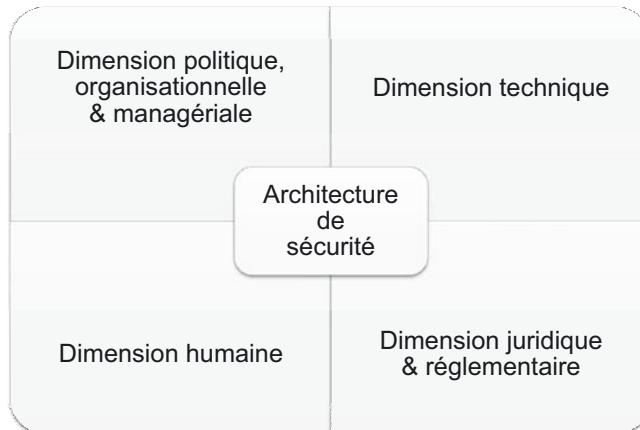


Figure 1.5 – Les différentes dimensions d'une architecture de sécurité.

éventuelles incompatibilités des différents niveaux de sécurité qui pourraient en découler.

La conception d'un système d'information sécurisé passe par la définition d'une structure conceptuelle qu'est l'**architecture de sécurité**. Celle-ci est fondamentale pour autoriser une **approche systémique** intégrant une prise en compte complète de l'ensemble des problèmes de sécurité du système d'information et de l'organisation afin de répondre de manière globale à sa **stratégie sécuritaire** et d'être en mesure d'assurer la **cohérence** et la **complémentarité** des mesures au regard des risques encourus et des exigences parfois divergentes de sécurité physique, logique, réglementaire, humaine ou managériale.

Produire de la sécurité n'est pas une affaire banale et ne se résume pas à l'implémentation de mesures de sécurité pour être en conformité réglementaire, ni à vérifier si toutes les mesures mentionnées dans une liste de bonnes pratiques existent ou non. Il s'agit de défendre les infrastructures qui sont vulnérables et attaquées, et de protéger les personnes et les biens. Dans une institution, la **cybersécurité** n'est pas un problème isolé, encore moins un problème purement technique. La cybersécurité doit répondre aux besoins de sûreté, de confiance, de bon fonctionnement. C'est un ensemble, une organisation, ce sont des conditions humaines, matérielles, économiques et politiques, des moyens et des compétences propres à garantir un état de sécurité, de mise à l'abri du danger, satisfaisant pour l'institution considérée, qu'elle soit publique ou privée.

Une Direction générale n'a pas besoin de connaître la technique pour comprendre les risques liés à un défaut de sécurité, et ce ne sont pas les experts de la sécurité qui sont en mesure de prendre des décisions stratégiques d'investissements nécessaires à la maîtrise des risques. Toutefois, les dirigeants doivent pouvoir s'appuyer sur des personnes compétentes, qui vont leur permettre d'appréhender le niveau réel d'exigences de sécurité, tout en sachant dialoguer avec les techniciens en charge de la sécurité opérationnelle, confrontés à la réalité du terrain et des menaces. Cette

personne à l'interface du stratégique et de l'opérationnel doit non seulement posséder des compétences du métier de l'entreprise, mais aussi disposer des capacités lui permettant d'être à l'aise avec des questions techniques et juridiques et de savoir anticiper les risques liés aux évolutions technologiques et des usages (BYOD, informatique en nuage, *Big Data*, objets communicants, etc.), qui ne manquent pas de générer plus d'insécurité.

Toutefois, aucune mesure de sécurité aussi robuste soit-elle ne peut pallier le manque d'intégrité des personnes en place et en charge de la sécurité ou contrer leur motivation à porter atteinte à l'organisation qu'elles sont censées servir. Il est donc devenu critique de mettre en place des actions de **cyberdéfense** qui permettent d'identifier et de stopper les incidents ayant de forts impacts de sécurité et de contrôler les mesures de sécurité mais aussi les personnes dédiées aux contrôles de sécurité...

Le véritable défi de la cybersécurité est toujours celui de convaincre, pas uniquement les directions générales des organisations, mais aussi les dirigeants en charge de l'éducation, afin de déployer une véritable politique de formation contribuant à mettre à disposition de la société, les experts capables de penser de manière transdisciplinaire et sachant appréhender les problématiques d'ordres politique, économique, managérial, technique, juridique et social nécessaires à la réalisation de la cybersécurité pour une approche réellement holistique de cette problématique qui est au cœur du développement de la société de l'information.

1.3.6 Servir une vision de société

Afin d'éviter que la société de l'information ne se transforme en une société de la défiance et de la surveillance, il est urgent d'apporter des réponses convaincantes à la nécessité de pouvoir construire la confiance dans le cyberspace et de proposer des mesures de sécurité adaptées.

Toutes les activités et pratiques utilisant l'informatique sont génératrices de données. Ces dernières sont stockées, traitées, exploitées, corrélées, communiquées par de nombreux acteurs sans pour autant que les propriétaires légitimes de ces données en soient forcément conscients ou même soient consentants (« le réseau » n'oublie jamais et les données ont une vie cachée). Il semble désormais urgent de s'interroger sur le phénomène de « massification » des données (**Big Data**) et sur le marché des données qui en découle, sur le pouvoir conféré aux acteurs qui les maîtrisent, et de maîtriser les risques pour les individus et la société ainsi générés.

Par ailleurs, nous sommes en train de construire un monde de la connectivité permanente, de la mobilité, de la communication sans fil et sans contact, un monde où les objets deviennent intelligents et communicants : c'est l'**Internet des objets**. Ainsi, les objets courants (des voitures, des feux de signalisation, par exemple) intègrent des composants informatiques et des technologies Internet. Ils sont alors capables d'une certaine autonomie et prise de décisions du fait d'une intelligence embarquée dans des programmes informatiques. Ces objets commencent à envahir l'espace public et *de facto* constituent des cibles potentielles de la cybermalveillance

car toute entité connectée à Internet est piratable. Ainsi, leur défaut de sécurité ou de robustesse peut avoir des conséquences préjudiciables à notre sécurité physique.

Toujours dans le registre de l'assistance aux personnes et aux activités de la vie courante, des robots plus ou moins sophistiqués commencent à partager notre quotidien. Capables d'influencer nos comportements et notre environnement, leur prise de contrôle par des entités malveillantes pourrait avoir des impacts négatifs pour notre société.

Par ailleurs le XXI^e siècle est celui des puces électroniques RFID, des nanotechnologies et des poussières intelligentes. La convergence entre le monde de l'électronique et le monde biologique est de plus en plus effective, notamment du fait de divers capteurs, prothèses, équipements électroniques biomédicaux implantés dans le corps humain pour pallier certaines de ses défaillances (pompe à insuline, pacemaker, etc.). Des interfaces neuronales existent déjà et permettent d'interagir avec des ordinateurs par la pensée. Si cela permet de contribuer au mieux-être de personnes, à terme leur usage généralisé, la plus grande intégration et intrication du biologique et de l'électronique, le détournement de leur usage initial pourraient conduire à des actions de « piratage » informatique y compris de la pensée humaine ! Ces nouveaux risques nous obligent à mettre en œuvre des mesures de sécurité informatique et réseaux afin de les maîtriser pour préserver nos valeurs mises en danger par la « technologisation » de la société.

La maîtrise des risques « cyber » s'inscrit dans un contexte de concurrence économique féroce et permanente – voire de guerre économique –, de recherche de profit immédiat, de crise monétaire internationale, de désordre généralisé, d'injustice sociale, de risque écologique, et d'un certain déficit de gouvernance mondiale.

Tenter de restreindre les **cyberdérides** nécessite une volonté politique, une stratégie nationale de cybersécurité, des ressources et compétences, des structures organisationnelles et des procédures ainsi qu'une coordination adaptée. Cela ne peut se faire sans des **partenariats des secteurs public et privé** (PPP, *Private Public Partnership*) et des systèmes de justice et de police efficaces au niveau national et international. Pour ce qui concerne plus particulièrement la cybercriminalité, cela oblige à prendre en considération entre autres :

- la connaissance des acteurs du monde « cyber » et de leurs modes opératoires ainsi que de l'ampleur du phénomène (qui sont les cibles, les victimes ?, quels sont les vecteurs des cyberactions nuisibles ?, à qui profite le « crime », l'économie illicite, le marché noir de la cybercriminalité ?, etc.) ;
- les besoins d'entraide internationale et les procédures réglant, entre autres, les problèmes de compétences territoriales ;
- la question de la gouvernance mondiale d'Internet.

Lutter efficacement contre la cybercriminalité passe par une approche préventive qui consiste à rendre le cyberspace moins favorable à l'expression de la criminalité et à réduire les opportunités criminelles. Par conséquent, il faut éléver le seuil de difficulté de réalisation des cyberattaques (augmenter les coûts en termes de compétences et de ressources pour le malveillant et diminuer les profits attendus) et

accroître les risques pris par les criminels d'être identifiés, localisés et poursuivis. Cela passe entre autres, par :

- la réduction du nombre de vulnérabilités techniques, organisationnelles, juridiques et humaines ;
- le renforcement de la robustesse et de la résilience des infrastructures informatiques par des mesures de sécurité technologiques, procédurales et managériales cohérentes et complémentaires ;
- une réelle capacité d'adaptation des moyens de cybersécurité et de cyberdéfense à une situation en constante évolution ;
- les moyens pour gérer les crises « cyber ».

Résumé

Obtenir un niveau de sécurité informatique suffisant pour prévenir les risques technologique et informationnel est primordial tant pour les individus que pour les organisations ou les états qui utilisent ou fournissent des services *via* les technologies du numérique. La sécurité informatique dans le contexte d'Internet et du cyberspace est le plus souvent dénommée « cybersécurité ».

Il est important de pouvoir identifier correctement les valeurs à protéger et les risques afin de déterminer les exigences de sécurité et les moyens de les satisfaire. Ceci implique une approche globale, pluridisciplinaire et systémique de la sécurité.

La sécurité informatique doit permettre de répondre aux besoins de disponibilité, d'intégrité et de confidentialité de certaines ressources.

Les télécommunications (infrastructures et services) répondent à une problématique de sécurité peu différente de celle des ressources informatiques dont la résolution répond aux mêmes impératifs techniques, organisationnels, managériaux juridiques et humains. Protéger les informations lors de leur transfert ne suffit pas car ces dernières sont tout aussi vulnérables, sinon plus, lorsqu'elles sont manipulées, traitées et mémorisées.

La sécurité informatique sera effective dans la mesure où l'on saura mettre en place des mesures de protection homogènes et complémentaires des ressources informatiques et de télécommunication, mais aussi de l'environnement qui les héberge. Toutefois, outre des mesures de sécurité proactives de protection des valeurs, il est nécessaire de prévoir des mesures réactives pour pallier la survenue d'incidents non sollicités, qu'ils soient d'origine criminelle ou qu'ils relèvent d'erreurs ou de catastrophes naturelles.

Aux aspects purement techniques de la sécurité, il faut associer la mise en œuvre efficace de procédures d'exploitation et de gestion. Par ailleurs, le personnel de l'organisation doit être formé aux mesures de sécurité et doit s'engager à les respecter. Ainsi, la sécurité informatique fait également appel à l'intégrité des personnes qui conçoivent, gèrent, utilisent les infrastructures informatiques et à une gestion appropriée des ressources humaines.

Exercices

1.1 Faites un tableau récapitulatif identifiant les capacités des systèmes, les critères de sécurité et les types de mesures de sécurité permettant de les satisfaire.

1.2 Quels sont les objectifs de la sécurité informatique ?

1.3 Expliquez la notion d'architecture de sécurité. À quels besoins correspond-elle ? Expliquez de quelle manière les différentes dimensions qui la composent sont complémentaires.

1.4 Dans un réseau de télécommunication, à quels besoins correspondent les notions d'identification et d'authentification, quels services permettent-ils de réaliser ?

1.5 En matière de sécurité informatique, faut-il privilégier une démarche proactive ou réactive ?

1.6 Justifiez que la sécurité informatique et réseau relève d'une problématique de gestion.

1.7 Pourquoi doit-on appréhender la sécurité de manière globale ?

1.8 Expliquez de quelle manière le critère de non-répudiation contribue à la sécurité informatique.

1.9 Quelles peuvent être les origines d'un défaut de sécurité informatique ?

1.10 Pourquoi en matière de sécurité informatique, la sécurité physique est importante ?

1.11 Qu'est-ce que la cybersécurité ?

Solutions

1.1 Du point de vue de la sécurité informatique, les systèmes doivent offrir les caractéristiques suivantes (tableau 1.1) :

- **Capacité d'un système à pouvoir être utilisé** — cela correspond à la disponibilité des ressources et des services, fonction de leur dimensionnement correct et d'une certaine redondance des ressources, mais également des procédures de sauvegarde, de reprise et d'exploitation adaptées aux besoins de fonctionnement.
- **Capacité d'un système à exécuter les actions et à rendre les services que l'on attend de lui dans des conditions de performance et d'utilisation adaptées** — cela traduit un besoin de continuité, de durabilité, de fiabilité, de convivialité et de sûreté de fonctionnement.

Chapitre 1 • Sécurité informatique et cybersécurité

- Capacité d'un système à ne permettre l'accès aux données en lecture ou en écriture qu'aux personnes et processus autorisés** — pour offrir confidentialité et intégrité des données. Ceci est assuré par des processus de contrôle d'accès, d'erreur, de cohérence et par des mécanismes de chiffrement.

Tableau 1.1 - Capacité des systèmes, objectifs et moyens de sécurité.

Capacité d'un système à	Objectifs de sécurité	Moyens de sécurité
Pouvoir être utilisé	Disponibilité Accessibilité Pérennité	Dimensionnement Gestion système/réseau Redondance Procédures d'exploitation et de sauvegarde PCA et PRA
Exécuter des actions	Intégrité Sûreté de fonctionnement Fiabilité Durabilité Continuité Exactitude	Conception Performance Ergonomie Qualité de service Maintenance opérationnelle
Permettre l'accès aux entités autorisées	Confidentialité Intégrité	Contrôle d'accès Gestion des identités Authentification Contrôle d'erreur, de cohérence Chiffrement Signature électronique Détection, prévention d'intrusion
Prouver des actions	Non-répudiation Imputabilité Traçabilité Authenticité Conformité aux lois Auditabilité	Notarisation Enregistrement, traçabilité Signature électronique Mécanismes de preuve Chiffrement

- Capacité d'un système à prouver que des actions, transactions ont bien eu lieu** à des fins de traçabilité, de preuve, d'imputabilité, de contrôle, d'audit ou de non-répudiation d'actions ou d'événements.

Ces diverses capacités permettent des services de qualité dans des conditions déterminées et peuvent être appréhendées comme des critères de sécurité ou des compétences de sécurité. Leur réalisation passe par la mise en œuvre de mesures spécifiques de sécurité contribuant à bâtir la confiance que peut avoir un utilisateur envers son environnement informatique.

Être sûr d'une identité, d'une source, d'une entité, d'une information ou qu'une action s'est correctement déroulée, permet d'effectuer des tâches contribuant à rendre un service de bonne qualité. Pour que ces critères quantitatifs de confiance aient un sens, les utilisateurs doivent adopter un code de conduite cohérent vis-à-vis de l'exploitation et de l'usage des ressources.

1.2 Les principaux objectifs de la **sécurité informatique** sont de réaliser la disponibilité, l'intégrité, la confidentialité des infrastructures informatiques (données, services, systèmes). Diverses mesures de sécurité permettent de les atteindre. Parmi elles nous pouvons citer : le contrôle d'accès, le chiffrement des données, la signature électronique, la gestion des incidents, des erreurs, des dysfonctionnements, des intrusions, le cloisonnement d'environnements...

1.3 Une **architecture de sécurité** est une structure qui fixe les dimensions organisationnelles, économiques, managériales, techniques, légales et humaines dans lesquelles les solutions de sécurité doivent s'inscrire.

Pour une organisation, l'architecture de sécurité permet de limiter le cadre d'appréhension globale de la sécurité et d'identifier tous les éléments (outils, procédures, mesures, réglementations, personnes, etc.) qui la composent. Définir une architecture de sécurité oblige à traiter les problèmes de sécurité de manière systémique et renforce la cohérence et la complémentarité des solutions de sécurité retenues. Cela contribue également à réaliser un référentiel de sécurité servant à la mise en place de l'évaluation et de l'audit de sécurité.

1.4 Les **notions d'identification et d'authentification** possèdent un rôle pivot fondamental à partir duquel différents services de sécurité peuvent se réaliser, dont le contrôle d'accès aux ressources mises en réseau afin d'autoriser aux ayants droit uniquement l'usage des ressources sollicitées. Ceci contribue à réaliser la confidentialité, l'intégrité, la traçabilité, l'imputabilité et la facturation des services.

1.5 Le choix d'une **démarche proactive ou réactive** dépendra du comportement et de la stratégie de gestion des risques des organisations. Une démarche proactive, à travers l'identification des actifs à protéger et l'analyse des risques (vulnérabilité, menace, impact, probabilité), permet de prévenir les incidents, de maîtriser et de minimiser la probabilité et l'impact des risques. Une démarche réactive met l'accent sur la maîtrise de l'incident de sécurité, sur le comportement après sinistre pour stopper l'événement causant le dommage et limiter les pertes afin de pouvoir continuer l'activité et retourner à un état normal le plus vite possible. Une démarche proactive peut également intégrer les éléments d'une démarche réactive, dans la mesure où celle-ci doit être anticipée, planifiée, organisée et gérée.

Dans la mesure où le risque zéro n'existe pas, les deux démarches sont à prendre en compte et sont tout aussi importantes.

1.6 Le rôle de la **sécurité informatique** est de diminuer le risque à un niveau acceptable dans un contexte donné et dépend de l'importance accordée par les managers aux actifs à protéger et aux risques encourus. Le risque peut être également assurable. Les sociétés d'assurance pouvant éventuellement couvrir les frais de remise en route des systèmes, le manque à gagner dû à l'indisponibilité ou au dysfonctionnement des systèmes.

Le but est d'atténuer le risque. Pour ce faire, il faut bien connaître toutes les composantes du risque et avoir une vision globale et cohérente des valeurs et mesures de

sécurité. La sécurité informatique doit être appréhendée d'une manière globale. Elle passe par la définition d'une politique de sécurité, la motivation et la formation du personnel, la mise en place des mesures ainsi que l'optimisation des solutions. Si un audit prouve que les mesures pour diminuer le risque ont été mises en place, la police d'assurance sera moins coûteuse.

L'utilisation seule d'outils ou de technologies ne peut pas résoudre les problèmes de sécurité d'une organisation. Les outils sont de peu d'utilité s'ils sont mal gérés ou mal utilisés. Leur choix comme leur implantation, leur réalisation opérationnelle et leur usage dépendent d'opérations de management et s'intègrent dans des processus de gestion plus globaux comme la gestion de la qualité, des ressources humaines, du budget, etc. La maîtrise des risques et de la sécurité est avant tout une question de gestion (gestion des droits d'accès, des identités, des procédures de mises à jour des antivirus, des sauvegardes, des outils de sécurité, etc.).

Les technologies de sécurité (authentification forte, chiffrement, pare-feu, systèmes de prévention d'intrusions, etc.) permettent d'apporter une réponse particulière à un problème de sécurité spécifique, à un instant donné. Elles ne tiennent aucunement compte de la dimension humaine de l'insécurité, ni du contexte dynamique dans lequel elles doivent s'insérer. Une approche purement technologique ne peut pas être une réponse satisfaisante au besoin de maîtrise des risques. Elle ne peut garantir une protection totale, ni répondre spécifiquement à la maîtrise des risques d'origines accidentelle, criminelle ou d'erreur. Pour toutes ces raisons, il est nécessaire de traiter la sécurité informatique en tenant compte des besoins de gestion, des dimensions organisationnelles, économiques, juridiques et humaines du contexte à protéger.

1.7 La sécurité doit être appréhendée de **manière globale** du fait que les infrastructures informatiques et télécoms sont constituées de nombreux éléments et acteurs dont le niveau global de sécurité est toujours celui du maillon le plus faible. Par analogie, une porte blindée est de peu d'utilité si les fenêtres restent ouvertes !

La sécurité repose sur la cohérence et la complémentarité des moyens et mesures, qui doivent satisfaire de manière harmonieuse les besoins de sécurité d'ordres économique, managérial, organisationnel, technique, et juridique.

1.8 La **non-réputation** permet de ne pas pouvoir nier (ou rejeter) qu'un événement a eu lieu. Cette notion est généralement associée à celles de responsabilité des entités, de traçabilité des événements et d'auditabilité des systèmes *via* les fichiers de journalisation (*logs*), à des fins de preuve ou d'imputabilité des actions ou événements.

1.9 L'origine d'un problème de sécurité informatique peut être de plusieurs natures et liée à :

- a) des erreurs non intentionnelles : erreurs de conception, de mise en œuvre, de gestion, ou d'utilisation (maîtrise des risques insuffisante, maîtrise des technologies en place défaillante, mauvaises manipulation, configuration et gestion

opérationnelle des systèmes inadéquates, changements de l'environnement qui créent des faiblesses, manque de rigueur, incohérences, etc.) ;

- b) des erreurs intentionnelles ou à des malveillances ;
- c) des catastrophes naturelles (feu, dégât des eaux, etc.) ;

1.10 La **sécurité physique** est tout aussi importante que la sécurité logique et lui est complémentaire car les critères de sécurité peuvent être mis à mal par exemple si une personne mal intentionnée peut accéder physiquement aux environnements informatiques et télécoms (serveurs, salle machines, infrastructures télécoms...) pour les voler, les altérer, les détruire, ajouter des composants de surveillance, etc. De plus, il faut pouvoir offrir aux systèmes informatiques un environnement énergétique adéquat (alimentation électrique, système de refroidissement, etc.) et des locaux résistants aux événements naturels. La sécurité physique comprend tous les dispositifs techniques, humains et procéduraux permettant de renforcer la protection physique des locaux et des systèmes.

1.11 La **cybersécurité** fait référence à la sécurité informatique et réseaux qui répond à la prise en compte des risques « cyber » qui peuvent affecter les individus, les organisations et les États. Les cyberrisques sont générés par l'usage extensif des technologies Internet et des services associés, qu'ils soient accessibles par des ordinateurs, des téléphones intelligents ou des tablettes par exemple.

CYBERCRIMINALITÉ ET SÉCURITÉ INFORMATIQUE

2

PLAN

- 2.1 Comprendre la menace d'origine criminelle pour une meilleure sécurité
- 2.2 Infrastructure Internet et vulnérabilités exploitées à des fins criminelles
- 2.3 Les cyberrisques
- 2.4 Crime informatique et cybercriminalité
- 2.5 Attaques informatiques *via* Internet
- 2.6 Faire face à la cybercriminalité

OBJECTIFS

- Identifier les caractéristiques et les vulnérabilités d'Internet exploitées à des fins criminelles.
- Offrir un panorama des cyberrisques.
- Présenter l'écosystème cybercriminel.
- Définir les notions de crime informatique et de cybercriminalité.
- Présenter les invariants relatifs aux principaux types de cyberattaques.
- Analyser les limites des approches sécuritaires actuelles ainsi que les comportements de gestion du cybercrime par les organisations.
- Proposer des éléments de la maîtrise du risque informatique d'origine cybercriminelle et de lutte contre la cybercriminalité.

2.1 COMPRENDRE LA MENACE D'ORIGINE CRIMINELLE POUR UNE MEILLEURE SÉCURITÉ

Afin de déterminer quelles sont les mesures de sécurité informatique qui doivent être mises en place pour contribuer à satisfaire les exigences de disponibilité, d'intégrité ou de confidentialité des ressources, il faut connaître l'origine des menaces qui peuvent être de trois natures différentes (figure 2.1) :

- les **erreurs**, les pannes ou les accidents auxquels on associe l'incompétence (erreurs de conception, de dimensionnement, d'administration système, de

programmation, d'utilisation, ou encore la mise hors tension électrique d'origine accidentelle) ;

- les **catastrophes naturelles** (inondation, foudre, tremblement de terre, etc.) ;
- la **malveillance** (sabotage, vol, destruction, etc.).

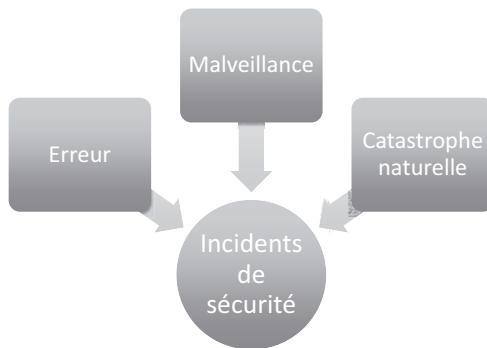


Figure 2.1 – Triple origine des incidents de sécurité.

Connaître l'origine des problèmes permet de mieux les anticiper, les détecter et les contrer. C'est pour cela qu'il est nécessaire de s'intéresser aux menaces d'origine criminelle et ainsi à la cybercriminalité, à la manière dont elle s'exprime, à ses acteurs, à leur motivation, afin de les prévenir et d'intervenir le plus efficacement possible lors de la survenue de cyberattaques et de mettre les contre-mesures indispensables au bon endroit pour en diminuer les effets.

2.2 INFRASTRUCTURE INTERNET ET VULNÉRABILITÉS EXPLOITÉES À DES FINS CRIMINELLES

2.2.1 Éléments de vulnérabilité d'une infrastructure Internet

Il existe toujours un contexte plus ou moins favorable à l'expression de la cybercriminalité. Les opportunités criminelles sont liées aux ressources ciblées, à leurs vulnérabilités ainsi qu'à la motivation et aux compétences des acteurs malveillants. Connaître les vulnérabilités et les réduire contribue à la maîtrise du risque informatique d'origine criminelle. La figure 2.2 résume les principales sources de vulnérabilités d'une infrastructure Internet.

2.2.2 Internet comme facteur de performance pour le monde criminel

L'actualité est là pour nous le rappeler quotidiennement, il est désormais un fait avéré que la majorité des systèmes informatiques ne sont pas suffisamment protégés

2.2 • Infrastructure Internet et vulnérabilités exploitées à des fins criminelles

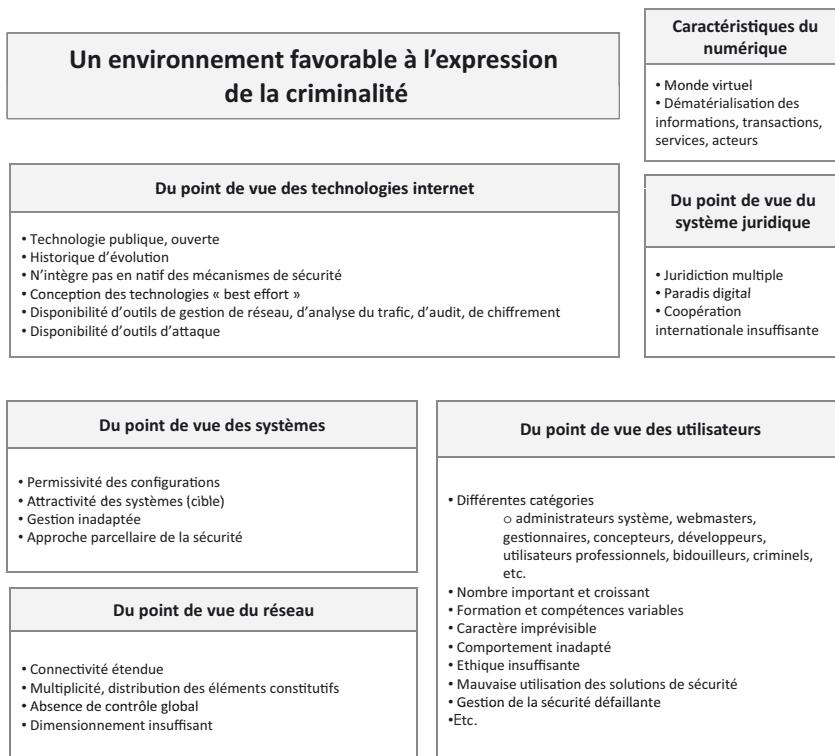


Figure 2.2 – Caractéristiques d'Internet exploitées à des fins criminelles.

puisque'ils font l'objet d'attaques, d'intrusions, d'altérations ou encore par exemple de vols de données et de propriété intellectuelle. Les infrastructures informationnelles possèdent un certain niveau d'insécurité qui profite aux acteurs malveillants qui savent en tirer parti. De plus, les caractéristiques d'Internet et la manière dont nous l'utilisons favorisent l'expression de la cybercriminalité. Cela est lié notamment à :

- l'exposition des ressources et au nombre de cibles potentielles ;
- la dématérialisation ;
- l'existence de vulnérabilités managériales, techniques et humaines liées aux systèmes d'information (défauts de conception, de mise en œuvre, de gestion, de contrôle, incomptérence ou incohérence des mesures de sécurité, etc.) ;
- la réalité d'une économie parallèle et d'un marché noir de la cybercriminalité ;
- la disponibilité de logiciels malveillants, d'outils et de compétences cybercriminelles à vendre ou à louer dans le Darknet ;
- la possibilité d'anonymiser, d'usurper ou de créer de fausses identités pour ne pas être tenu responsable d'actions délictueuses ;
- la capacité de passer par de multiples intermédiaires (systèmes, réseaux, pays) pour masquer l'origine des attaques et empêcher l'identification des auteurs ;

- l'existence de paradis digitaux ;
- la difficulté à poursuivre un crime informatique transnational ;
- les diverses défaillances des systèmes juridiques, procéduraux et d'entraide judiciaire internationale pour lutter efficacement contre la cybercriminalité ;
- l'usage de monnaies virtuelles qui permettent d'alimenter le Darknet à moindre risque.

Dès lors, les possibilités d'exploitation des vulnérabilités et de réalisation d'actes malveillants sont nombreuses. La réalité de ces derniers : accès indus, exploitation frauduleuse de ressources, infection, détérioration, destruction, modification, divulgation, déni de service, vol, prise en otage des ressources informatiques, chantage, escroqueries... met, d'une certaine façon, en évidence une maîtrise insuffisante du risque informatique d'origine criminelle et les limites des approches sécuritaires actuelles.

 De par sa nature et ses caractéristiques, Internet procure une couche d'isolation protectrice aux criminels. La couverture internationale du réseau Internet permet aux criminels d'agir au niveau mondial, à grande échelle et très rapidement, en s'affranchissant des distances.

Dématérialisation

La fragilité fondamentale du monde numérique est inhérente à la **dématérialisation** (numérisation) de l'**information**. En effet, en devenant **immatérielle**, l'information **numérique** acquiert une **double vulnérabilité, physique et logique**, relative à son support et à sa valeur informationnelle (cf. figure 2.3). La numérisation de l'information assure l'**indépendance** physique et logique de celle-ci du fait de la séparation entre le contenu d'une information (sa signification, sa représentation) et son contenant (le support physique sur lequel le contenu est temporairement transcrit : mémoire vive, disque dur, clé USB, cédérom, fibre optique d'un réseau, onde hertzienne de transmission, etc.). La notion de donnée d'origine n'a plus de sens puisque les copies à l'identique et à l'infini sont possibles. Dès lors, comment définir le vol de données qui se traduit par leur copie par des personnes non autorisées alors que les données existent toujours ? Le vol étant par définition « la soustraction frauduleuse de la chose d'autrui », ici on ne soustrait pas, on copie.

De plus, la dématérialisation des informations, des activités, des échanges ainsi que l'usage par les criminels de solutions de chiffrement, de stéganographie¹, et d'anonymat autorisent des liaisons entre criminels sans contact physique, de manière flexible et le plus souvent en toute impunité. Ainsi, ils peuvent s'organiser en équipes, planifier des actions illicites et les réaliser soit de manière classique, soit par le biais des technologies de l'information en réalisant des cyberattaques.

1. Voir le chapitre 5 pour les techniques de chiffrement. La stéganographie fait référence aux techniques qui permettent de cacher, dissimuler une information sensible dans une autre non significative voire anodine (texte, image, photo...) sans modification apparente de cette dernière.

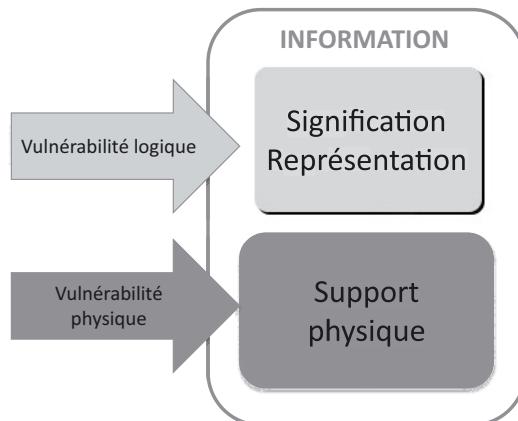


Figure 2.3 - Double vulnérabilité de l'information numérique.



Le cyberespace étend le champ d'action de la criminalité classique et offre de nouvelles possibilités d'enrichissement et de prise de pouvoir. Dans ce contexte, Internet peut être considéré comme étant un catalyseur d'actions abusives, déviantes ou illicites et un outil de la performance criminelle.

Universalisation et dépendance

La généralisation de la mise en réseau Internet des ressources informatiques et informationnelles et leur ouverture sur le monde font qu'elles deviennent des **cibles** faciles et attrayantes pour la réalisation de délits.



Les infrastructures informatiques et télécoms, les services et applications, les données, en fait toutes les ressources interconnectées sont devenues des cibles et aussi des moyens de réalisation de la criminalité.

L'**uniformisation** et l'adoption universelle des technologies Internet, la **dépendance** des individus, des organisations et des États à ces mêmes technologies, ainsi que l'**interdépendance** des infrastructures introduisent un **degré de vulnérabilité** et un facteur de risque pour la société. Cela peut porter préjudice aux individus, mettre en péril la compétitivité et la pérennité des organisations, la stabilité de l'économie, la souveraineté des États ou encore porter atteinte à la **sécurité publique** et à la **sécurité nationale**.

Disponibilité d'outils

La disponibilité d'outils d'exploitation des failles des systèmes, l'existence de bibliothèques d'attaques qui offrent une large gamme de logiciels malveillants capitalisant le savoir-faire criminel dans un programme, les kits tout prêts pour fabriquer des virus et autres logiciels malveillants contribuent à la réalisation d'attaques informatiques et à l'expression de comportements malveillants.



Le **cyberespace**, où les actions se réalisent à distance, caché derrière un écran et éventuellement derrière de fausses identités ou des identités usurpées, facilite pour certains le passage à l'illégalité, sans parfois que les auteurs aient pris conscience de la dimension illégale et criminelle des actes perpétrés et des peines qu'ils encourrent².

Relative impunité

Les criminels tirent parti de l'aterritorialité d'Internet, des juridictions multiples, de l'inexistence dans certains États de lois réprimant le crime informatique. De plus, la relative inefficacité des systèmes de justice et de police, des mesures de prévention et de dissuasion les confortent dans un **sentiment d'impunité** stimulant leur créativité criminelle. En cybercriminalité, la prise de risque est souvent minimale au regard de la profitabilité des actions.



À l'instar des paradis fiscaux, il existe des **paradis numériques** où un malfaiteur peut agir ou héberger des serveurs et des contenus illicites en toute impunité.

Ainsi, le fait de pouvoir agir à partir de pays qui ne pénalisent pas le crime informatique et qui, de ce fait, constituent des refuges à des opérations transnationales, ainsi qu'une coopération internationale une entraide judiciaire insuffisante, sont des avantages largement exploités par les criminels.

Toutefois, bien que le cyberespace ne possède pas de frontières géographiques à proprement parler, l'internaute se situe toujours dans un espace géographique et temporel déterminé où **tout ce qui est illégal Off line est aussi illégal On line** car le cadre juridique du pays duquel il est ressortissant s'applique. Son comportement est en principe régi par des pratiques de morale et d'éthique relevant des valeurs de la société dont il est le citoyen.

2.2.3 Internet au cœur des stratégies criminelles

Les différentes formes d'expression de la **cybercriminalité** ont pour dénominateur commun de faire courir relativement peu de risque à leur auteur et d'engendrer des gains et des dommages potentiels bien supérieurs aux ressources nécessaires pour les réaliser. Les criminels ont bien compris la profitabilité qu'ils peuvent tirer d'Internet pour optimiser leur action criminelle traditionnelle (crime économique, escroqueries, trafics de stupéfiants, traite d'êtres humains, espionnage, vente illégale d'armes...). Par ailleurs Internet leur permet également la réalisation de vieux délits avec de nouveaux moyens (enrichissement illicite, blanchiment d'argent, harcèle-

2. Thierry Breton dans son rapport *Chantier sur la lutte contre la cybercriminalité* souligne que « *le caractère virtuel des échanges [...] sur Internet favorise le franchissement des barrières de l'illégalité, les internautes ayant le sentiment que les bornes morales ou légales de la vie réelle ne s'appliquent pas au cyberespace, ce dernier leur apparaissant complètement “désincarné”* ». Rapport remis à Monsieur le ministre de l'Intérieur, de la Sécurité intérieure et des Libertés locales le 25 février 2005. http://www.telecom.gouv.fr/fonds_documentaire/rapports/cybercriminalite.pdf

ment, incitation à la haine raciale...) et la réalisation de nouveaux faits délictueux (vol, détérioration de ressources informatiques, intrusion dans des systèmes informatiques, usurpation d'identité numérique, propagande pour des organisations criminelles...).

Les technologies de l'information permettent l'extension de la criminalité dans le cyberespace, qui devient alors un champ d'actions et une source additionnelle d'opportunités criminelles. Il autorise la réalisation de fraudes ou de délits habituels via l'outil informatique et le cyberespace.



L'exploitation efficace d'Internet permet aux criminels de réaliser des délits en s'exposant à un niveau de risque minime, tout en s'assurant la maximisation des profits. Les diverses formes de la cybercriminalité sont le prolongement naturel de la **criminalité classique**.

L'information, bien immatériel de toutes les organisations, est au cœur de leurs stratégies, de leurs processus de décision et d'organisation. Cela est également vrai pour les organisations criminelles et terroristes. Les technologies de l'information sont aussi un facteur de production et d'efficacité et un élément de performance au service d'acteurs malveillants. Ainsi, Internet est un vecteur privilégié du **crime économique** qui n'est pas uniquement réservé à la criminalité organisée car il est à la portée de tous.

2.2.4 Risque d'origine criminelle et insécurité technologique

Les **vulnérabilités**, la **maîtrise insuffisante** des technologies, la réalité de la **cybercriminalité**, sont des composantes de l'**insécurité** générée par l'usage extensif des technologies du numérique. Cela constitue de nouvelles menaces susceptibles de frapper n'importe quelle entité, n'importe quand, n'importe où. Il s'agit d'un **risque structurel** et permanent. Trois attitudes peuvent être adoptées face à un risque : l'ignorer, le transférer ou le maîtriser. À l'heure de la société de l'information, le risque informatique dû à un défaut de sécurité ou de robustesse des infrastructures ne peut pas être ignoré des individus, des organisations et des États. L'idée de pouvoir transférer le risque informatique via des mécanismes d'assurance ne peut pas satisfaire les besoins d'usage rationnel et performant des technologies. Il reste donc à le **maîtriser** par des actions de sécurité efficaces³.

En matière de sécurité informatique, à défaut de connaître les potentiels des agresseurs et leur motivation, ou de pouvoir imaginer toutes les fraudes ou malveillances possibles, il est primordial de **diminuer les vulnérabilités**, de **ne pas exposer inutilement les ressources** de l'organisation, de mettre en place des démarches proactives et réactives de maîtrise des risques informatiques et de gérer la sécurité. Ce serait une erreur de penser que des mesures efficaces de sécurité puissent se fonder

3. Voir les chapitres 3 et 4 pour la gestion des risques et la dimension managériale de la sécurité. Les chapitres suivants traitent des mesures techniques de la sécurité informatique.

uniquement sur la peur, qu'elle soit individuelle ou collective. Elles doivent s'inscrire dans une approche globale d'appréhension des réalités sociales, économiques, culturelles et politiques dans le respect des **droits fondamentaux** et des principes démocratiques de notre société.

2.3 LES CYBERRISQUES

Outre le risque majeur de **dépendance** aux infrastructures informationnelles et à leurs fournisseurs, une manière d'identifier les risques liés à l'usage d'Internet est de les distinguer :

- d'une part en fonction des conséquences qu'ils engendrent sur les victimes, à savoir : les individus, les organisations et les États ;
- et d'autre part en fonction des critères de sécurité des systèmes informatiques impactés par ces risques.

2.3.1 Principaux risques pour les individus

Via leurs équipements connectés à Internet, les usagers peuvent être **victimes** de diverses actions malveillantes :

- harcèlement, intimidation, chantage, diffamation, mise à mal de leur réputation, incivilités, etc. ;
- réception de contenus malveillants, offensifs ou non désirés (virus, spam, pornographie dure, scène de violence, incitation à la haine raciale et à la xénophobie, propagande, etc.) ;
- surveillance, une traçabilité ou profilage excessif, et à des écoutes environnementales (atteinte à la vie privée et à l'intimité numérique, espionnage) ;
- vol de données (données personnelles, informations confidentielles, propriété intellectuelle, etc.), vol d'équipements (ordinateur, clé USB, CD-Rom, etc.) et à la destruction de valeurs ;
- usurpation d'identité ;
- canulars, escroqueries, chantages, fraudes, abus en tout genre ;
- désinformation et à la manipulation d'opinion (influence) ;
- détournement de leurs capacités informatiques et à la prise de contrôle de leurs systèmes par des entités tierces.

Internet permet de communiquer avec potentiellement tout le monde (et donc n'importe qui) alors qu'il est difficile de vérifier qui se cache derrière une identité virtuelle ou un pseudo. Tous les acteurs d'Internet peuvent agir de manière bienfaisante et/ou malveillante, loyale et/ou déloyale. Il n'existe pas de mécanisme « de sécurité » qui permet de garantir la bonne foi de ces derniers. C'est à l'internaute de rester vigilant et de décider par lui-même si ce qu'il « voit » de l'autre est vrai ou faux, s'il peut lui accorder sa **confiance** ou non. De plus, un sentiment de « confiance et de proximité » que rien ne permet de justifier ni de garantir de manière fiable et durable est le plus souvent entretenu par les fournisseurs de

services. L'impression d'être « entre amis » génère un **faux sentiment de sécurité** qui peut avoir des répercussions désastreuses sur la vie des personnes.

Les manipulateurs, menteurs, escrocs et prédateurs, cachés derrière un écran et de fausses identités, sont très actifs sur les réseaux sociaux, les systèmes de messageries, les forums de discussion, les sites de rencontre ou de ventes aux enchères par exemple. Ils sont là où se trouvent leurs victimes potentielles et excellent dans la manipulation et l'abus de confiance pour conduire leurs proies à réaliser leurs desseins. Nul ne peut être totalement à l'abri, certains sont des professionnels de l'arnaque, de la soumission de l'autre et savent séduire et menacer pour imposer leur volonté. Les enfants, les adolescents, les personnes crédules, celles à la recherche désespérée de l'âme sœur sont souvent les plus vulnérables. Les prédateurs et escrocs de tout acabit possèdent une grande habileté pour se faire passer pour le confident, la copine, la personne de confiance, celle que la victime rêve de rencontrer, le vendeur qui propose la bonne affaire, etc. Les prédateurs sexuels savent opérer des phases de séduction plus ou moins longues qui amènent la victime à livrer des informations personnelles, voire des photos, des vidéos souvent de plus en plus osées et à proposer des rendez-vous. Leur procédé est pernicieux, basé sur une spirale graduelle dans laquelle la personne est aspirée, mettant habilement en jeu des sentiments de confiance, de honte ou de culpabilité. Cela peut s'accompagner de menaces ou de récompenses.

Tout commence généralement par des échanges tout à fait anodins, un questionnement banal entre amis qui ne suscite pas la méfiance, les questions devenant progressivement de plus en plus précises et intrusives. Il est courant que des enfants notamment soient amenés ensuite à rencontrer physiquement leur bourreau. En effet, rien n'empêche les mineurs comme les pédophiles d'être présents sur un site de socialisation. Ces derniers pourront profiter de ce moyen de communication et d'un contexte favorable « entre amis » pour établir une relation électronique qui pourra donner lieu à la réalisation d'actes sexuels devant une webcam permettant ensuite d'exercer des chantages et des pressions sur la personne en la menaçant de diffuser ses images, ou encore à des rencontres bien réelles.

Rappelons que les actions qui relèvent de la pornographie juvénile, de la sollicitation, de la séduction d'enfants par Internet, de l'exploitation des enfants en ligne, ou la possession d'images, de films et de documents qui illustrent l'agression ou l'exploitation sexuelle des jeunes sont illégales. Il ne faut jamais oublier que derrière des images ou vidéo de pornographie enfantine il y a toujours de vraies **victimes**.

Parmi les fraudes très bien organisées, dont peuvent être victimes tous les internautes du monde, citons des grands classiques tels que par exemple :

- l'escroquerie de loterie, aux sentiments, aux organismes de bienfaisance, à l'héritage, etc. ;
- les jeux en ligne frauduleux, les sites de paris truqués, avec une énorme possibilité de corruption des acteurs des jeux et de paris ;
- les fausses offres d'emploi qui consistent à faire jouer le rôle d'intermédiaire dans des processus de blanchiment d'argent ou d'activités de recel ;

- la fraude sur carte de crédit et sur carte bancaire, le vol de données confidentielles ;
- etc.

Ces derniers points sont le plus souvent réalisés par des actions de **phishing** en abusant de la crédulité, de la naïveté ou de la servabilité des personnes. Outre les informations personnelles livrées de plein gré par l'utilisateur légitime, les cas de pertes ou de vols de données personnelles, qui ne sont pas tous dus à des actions de piratage informatique, ne se comptent plus. Les origines en sont multiples, parmi elles la perte ou le vol physique d'ordinateurs et de téléphones portables, de clés USB, y compris par des prestataires de services et des sociétés tierces.

2.3.2 Principaux risques pour les organisations

Parmi les risques spécifiques aux institutions, qu'elles soient privées ou publiques, retenons notamment les risques suivants liés :

- à l'**espionnage industriel et économique** (vol/perte de secrets des affaires, de valeurs immatérielles, de savoir-faire, etc.) ;
- aux atteintes à la propriété intellectuelle, au droit des marques, etc. ;
- aux attaques concurrentielles (vol de fichiers clients, de prix, de fournisseurs, de plan de fusion-acquisition, etc.) ;
- aux attaques sémantiques (rumeurs, fausses informations, manipulation d'information, désinformation, etc.) ;
- aux atteintes à l'image, à la réputation, à la fiabilité, etc. ;
- à l'incapacité à produire, à fonctionner (dysfonctionnements, indisponibilité des services, perte de qualité, altération des processus décisionnels, etc.) ;
- à la falsification et à la défiguration de sites web ;
- à l'infection des ressources informatiques, au détournement des capacités informatiques de l'organisation ;
- à la prise de contrôle de tout ou partie des ressources informatiques de l'organisation à des fins de chantages (prise en otage des ressources informatiques, menace de divulgation d'information, chiffrement de fichier puis monnayage de la clé pour déchiffrer, etc.) ou pour les impliquer dans des cyberattaques ;
- à la criminalité économique ;
- à la non-conformité aux lois et aux réglementations liées aux données et à l'informatique ;
- etc.

Des extorsions de fonds contre des sociétés sont également monnaie courante et se basent sur des menaces et sur du **chantage**, sur la prise en otage des ressources informatiques (verrouillage des ressources par chiffrement et demande de rançon, généralement en bitcoins, menaces d'attaques en déni de services des serveurs, de blocage de compte de l'entreprise ou de divulgation de données confidentielles).

Remarquons que dans la grande majorité des cas, l'informatique des artisans, des petites et moyennes entreprises est à risque car peu de ces structures ont les moyens

nécessaires à la prise en compte des besoins de cybersécurité, contrairement aux plus grandes organisations qui pour la plupart ont intégré des mesures de gestion de risque et de sécurité.

2.3.3 Principaux risques pour la nation et la société

Certaines attaques informatiques peuvent viser les systèmes contrôlant les **infrastructures critiques** nécessaires au bon fonctionnement d'un pays et induire des conséquences dommageables pour la population, l'économie et la sécurité nationale. Sont considérées comme vitales pour la société les infrastructures relevant des secteurs de l'énergie, des transports, des télécommunications, de la finance, de la santé, de l'approvisionnement en eau et en nourriture, de l'industrie chimique, de l'armée. Certaines infrastructures indispensables au bon fonctionnement du gouvernement, de l'administration et à la diplomatie internationale peuvent aussi être considérées comme critiques. Elles sont toutes tributaires de l'informatique.

Les systèmes de production et de distribution d'électricité conditionnent le fonctionnement de la plupart de toutes les autres infrastructures critiques. Cela induit une réelle interdépendance, qui peut avoir des effets dominos et être à l'origine de **risques systémiques** dont les impacts peuvent être catastrophiques. Si les commanditaires de cyberattaques sur des infrastructures vitales sont des États, ces attaques peuvent s'inscrire dans une **stratégie de guerre informatique** offensive ou défensive, d'intimidation ou de rétorsion. Ainsi, le brouillage des communications, les attaques informatiques sur les systèmes de contrôle aérien ou ferroviaire ou de contrôle des pipelines et des réseaux de distribution du gaz ou encore sur des usines de fabrication de produits indispensables à la vie économique tels que ceux de la finance, de la chimie industrielle, par exemple, pourraient être considérés comme étant des actes de guerre. Par de telles attaques, la population civile ne serait pas épargnée. Le maintien si possible en permanence de la capacité de fonctionnement des infrastructures critiques, ou la limitation de l'ampleur des dommages en cas de défaillance des systèmes, est donc de première importance.

Des cyberattaques sur des systèmes de contrôle des infrastructures critiques sont de nature à porter atteinte à la sécurité et à la **sûreté publique** en entraînant notamment de la panique, en générant de la terreur et en mettant en danger les capacités de survie, voire en induisant des pertes humaines. En effet, dans certaines circonstances, selon la motivation des acteurs de cyberattaques ciblant le domaine de l'énergie (électricité, centrales nucléaires) ou les systèmes d'épuration des eaux par exemple, les transports (les réseaux télécoms, les réseaux ferroviaires, le contrôle aérien), le domaine relatif à la santé (hôpitaux, fabrication de médicaments), l'atteinte de ces infrastructures vitales peut constituer un objectif privilégié du **cyberterrorisme**. Une forme particulière du terrorisme dont l'objectif est de créer des sentiments d'insécurité jusque dans ce qui est considéré comme le fondement des relations socio-économiques de certaines communautés dont l'économie représente le mode de vie à combattre, peut être réalisée par des cyberattaques.

À ce jour, la définition du **cyberterrorisme** n'est pas claire. Le plus simple serait sans doute de considérer le cyberterrorisme comme du terrorisme appliqué au **cyberespace**. Or, dans son sens courant et d'après le dictionnaire, le terrorisme fait référence à l'emploi systématique de la violence pour atteindre un but politique.

Dans ce cadre d'appréhension du concept de terrorisme, nous sommes en droit de nous demander de quelle manière des actes portant atteinte à l'intégrité de systèmes ou de données informatiques constituent une violence physique ou morale suffisamment importante pour générer la peur et constituer des moyens de pression contribuant à la réalisation d'objectifs politiques déterminés.



Remarquons également que les terroristes ont largement adopté les facilités de communication offertes par Internet pour faire du prosélytisme, de la recherche de fonds et de cibles, pour s'organiser, communiquer, recruter, préparer des actions, être performants, etc.

Internet permet de servir des **stratégies indirectes** qui, même en temps de paix, peuvent contribuer à affaiblir un secteur d'activité, une entreprise, un pays, et fournir ainsi des avantages concurrentiels à certains acteurs socio-politico-économiques. Cela peut être particulièrement le cas lors d'attaques contre des sociétés piliers de l'**économie nationale**, le système financier, les algorithmes de *trading* à haute fréquence, comme des influences sur les cours de la bourse par diffusion d'informations fausses, ou encore par la manipulation de l'opinion publique. Des cyberattaques peuvent entraîner des réactions contribuant à l'effondrement de l'économie ou à la ruine de certains acteurs. À cela s'ajoute le risque de prise en otage des ressources informatiques d'une organisation publique ou privée pour exercer un **chantage**, et menacer de stopper les activités ou de divulguer des données confidentielles est courant (notion de terrorisme informatique et économique) et les impacts directs et indirects peuvent être durablement désastreux.

Internet permet d'effectuer des actions de **propagande** et de manipulation d'opinion pour justifier des actes d'agression ou de défense, ou encore de pousser au réflexe nationaliste en transformant des internautes en **cyberpatriotes** ou **cyberactivistes**. L'information est utilisée dans des campagnes de manipulation et d'influence, et peut être considérée comme une arme de soutien à tous types de conflits. Des pressions médiatiques ou psychologiques peuvent être infligées aux adversaires et peuvent toucher une population et ses dirigeants.

De nos jours, le cyberspace est devenu un **champ de bataille économique et militaire**. La guerre dans le cyberspace utilise des moyens non militaires (au sens traditionnel du terme) et Internet modifie également l'art de faire la guerre : sans soldat, mais avec des informaticiens, sans arme à feu mais avec des informations et du code informatique. Les ordinateurs télécommandés après leur prise de contrôle par des programmes informatiques lancés ou commandités par des militaires (notion de *botnets* militaires) sont comparables à des combattants infiltrés et commandés à distance. Dès lors, le **piratage informatique** pourrait être considéré comme une arme de guerre et la distinction entre ce qui relève du domaine civil et du domaine militaire devient malaisée à effectuer.

Par ailleurs, il est extrêmement difficile, voire impossible, d'attribuer des actes de guerre informatique à une entité ou d'en prouver la responsabilité directe ou indirecte du fait des intermédiaires techniques, du recours éventuel à des mercenaires ou à l'usage de *botnets* télécommandés à partir de serveurs de commande et contrôle répartis sur différents points de la planète. L'ennemi est invisible, voire inconnu, et la riposte difficile à mener (le risque de se tromper de cible même dans un état de **légitime défense** est un frein à la contre-attaque informatique). Dans ce contexte d'asymétrie, le coût de la défense est bien supérieur à celui de l'attaque. Par ailleurs, il est difficile d'attaquer sur Internet sans passer par des infrastructures traversant des pays neutres ou alliés. Dans le cyberespace, la notion de frontières géographiques et de distances s'estompe.

Les cyberattaques, en fonction de leur nature, de leur intensité et de leurs cibles, peuvent invalider les défenses d'un adversaire, déstabiliser son renseignement, contribuer à porter atteinte au moral de sa population, altérer des processus de décision et de production, voire paralyser ses centres stratégiques ou encore bloquer ses moyens de communication. Ainsi, plus les États sont développés, plus leur capacité militaire et leur pouvoir économique sont dépendants des technologies du numérique, plus ils peuvent être fragilisés puisque *de facto*, ils sont plus vulnérables aux attaques informatiques majeures.

Au-delà des actions criminelles ayant pour objectif la recherche de profit, la prise de pouvoir ou d'influence, le potentiel d'Internet permet également d'attiser des conflits. Toutes les actions cybercriminelles ne relèvent pas du terrorisme ou de la guerre entre États. Cependant, Internet et le cyberespace introduisent de nouveaux risques pour la société. Ils permettent de soutenir un projet politique et peuvent être utilisés dans un but conflictuel, voire éventuellement pour commettre des dégâts chez l'ennemi sans combattre, en réduisant son pouvoir dans les domaines économique, scientifique ou culturel.

Désormais, l'un des meilleurs moyens de remporter la victoire est de contrôler et non de tuer, notamment par le biais de la maîtrise de l'informatique et des réseaux de télécommunications, des informations, de la cybersécurité et par celle du renseignement stratégique et économique.

2.3.4 Internet, facteur de rapprochement des mondes criminel et terroriste

Les **terroristes** utilisent Internet comme outil de communication efficace pour revendiquer, médiatiser, influencer et terroriser, effectuer des actions de propagande et réaliser du renseignement, pour recruter, former, entraîner, récolter des fonds, transférer des fonds, rechercher des cibles, organiser, planifier des opérations et communiquer.

Au travers d'Internet et du cyberespace, le monde criminel voit dans le monde terroriste principalement une source de profit et une manière de monter en puissance. Les terroristes font appel aux services des cybercriminels pour d'une part soutenir leurs capacités financières et les faire fructifier et d'autre part pour acquérir

le pouvoir de frappe informatique permettant de générer la terreur. Internet est pour les organisations terroristes à la fois un espace de combat et de soutien opérationnel et logistique.

Louer, acheter des programmes malveillants, des réseaux de *botnets*, des compétences contribuent à :

- pirater et s'introduire dans des systèmes informatiques ;
- à s'attaquer à des systèmes informatiques considérés comme étant des cibles et des symboles à détruire ;
- défigurer des sites web et y laisser des messages de revendication ;
- effectuer des attaques plus ou moins spectaculaires pour une médiatisation des actions ;
- générer de la panique à des fins de déstabilisation ;
- faire éventuellement diversion pour frapper dans le monde réel ou déstabiliser l'organisation des secours et les processus de gestion de crises en parallèle à des actions terroristes classiques ;
- mener des attaques portant atteinte à l'environnement (centres informatiques d'usines chimiques par exemple, de traitement des eaux, bioterrorisme, etc.).

Le type d'agression informatique ne suffit pas à définir avec certitude la motivation ou les objectifs d'une personne ou d'un groupe organisé. Ceci constitue une des difficultés de la lutte contre le crime informatique car il est nécessaire de disposer d'informations complémentaires pour caractériser l'**intention criminelle**. En l'absence d'éléments concrets, sans revendication ni auteur présumé d'une attaque, notamment en ce qui concerne celles en déni de service, il est difficile de distinguer si elles relèvent du cyberterrorisme ou de la cybercriminalité. En effet, la connaissance de la cible ne permet pas de faire la distinction entre un acte malveillant dû à un petit délinquant, un mercenaire, un escroc ou encore à un terroriste.

2.3.5 Guerre sémantique et cyberhacktivisme

Aucun État n'est à l'abri de cyberactions visant à lui nuire. La sécurité intérieure d'un pays, sa sécurité publique sont confrontées à de nouvelles formes d'expression de menaces liées à l'usage extensif des technologies de l'information et du numérique. Internet peut être au service de l'espionnage et du renseignement, de la manipulation de l'information, des rumeurs, ou de toutes formes d'intoxication ou de campagnes de déstabilisation. Ce qui semble le plus préjudiciable car invérifiable de manière absolue ce sont les nouvelles formes de **guerre sémantique** car les dommages ne sont pas directement mesurables. C'est en réalité une guerre liée au symbole – qui peut relever d'un processus d'intimidation générant de la peur et qui peut alimenter le discours du cyberterrorisme. Le caractère invisible, imprécis et multiforme de la menace rend cette dernière encore plus dangereuse. Il faut être extrêmement prudent quant à l'origine des attaques informatiques car elles peuvent s'inscrire dans une vaste campagne de manipulation pour incriminer certains acteurs.

Les possibilités de **manipulation des opinions** sont sans fin et peuvent avoir des conséquences plus ou moins importantes pour les individus, les organisations ou les États qui en font les frais. Certaines manipulations de l'information peuvent porter atteinte à l'intégrité morale ou physique des personnes. Il s'agit ainsi de ne pas oublier la guerre économique que se livrent les institutions, tant sur un plan national qu'international. La cybercriminalité est avant tout une criminalité économique, qui s'exprime dans un contexte plus large de guerre de l'information, par l'information et pour l'information.

Les outils des attaques informatiques sont identiques quelles que soient les finalités des attaques (politique, économique, criminelle ou terroriste). Seule varie la motivation de leurs auteurs et l'importance des conséquences pour les structures concernées. Il est donc important d'inscrire la cybersécurité dans un **continuum sécurité-défense** pour une meilleure protection des **territoires numériques**.

Le **cyberhacktivisme** est une forme de protestation basée sur l'usage de cyberattaques pour défendre des idéologies ou des objectifs politiques. Hackers patriotiques ou **cyberdissidents** concentrent leurs attaques contre des cibles considérées comme hostiles, ce qui se traduit entre autres par des dénis de service ou des défigurations de sites web. L'hacktiviste peut également utiliser toute la panoplie des outils de communication Internet (blogs, réseaux sociaux, YouTube, etc.) pour informer, dénoncer ou tenter de convaincre et rassembler des personnes à sa cause. Le **hacker-activiste** peut penser que son activité de piratage est légitimée par l'existence même d'Internet et par la passion qu'il nourrit à son égard. Il est parfois complexe de comprendre les motivations qui animent les hacktivistes. Leurs actes relèvent-ils d'une action citoyenne, d'une recherche de reconnaissance, du fanatisme, du mysticisme, de la lutte contre les totalitarismes ou encore de la criminalité ou du terrorisme ?

2.4 CRIME INFORMATIQUE ET CYBERCRIMINALITÉ

2.4.1 Éléments de définition

Chaque technologie peut avoir des usages détournés ou abusifs et être porteuse de potentialités criminelles. Bien que l'OCDE⁴ ait défini en 1983 la notion d'infraction informatique comme étant « *tout comportement illégal, immoral ou non autorisé qui implique la transmission et/ou le traitement automatique de données* », celle de cybercriminalité recouvre un concept à géométrie variable, sujet à de multiples définitions et interprétations selon les pays.

La notion de cybercriminalité peut être déduite de celle de **crime informatique**, délit pour lequel un système informatique est l'objet du délit et/ou le moyen de le réaliser. Ainsi, le **cybercrime** est une forme du crime informatique qui fait appel aux technologies Internet pour sa réalisation. Par extension, cela englobe tous les crimes

4. Organisation de coopération et de développement économiques (www.ocde.org).

relatifs aux technologies du numérique et aux équipements qui intègrent de l'électronique, consoles de jeux, cartes à puce, tablettes, téléphone, etc.

Le fait que la **criminalité** et la **délinquance** relèvent du **droit pénal** des nations engendre de multiples définitions, caractéristiques ou typologies du crime informatique. La **Convention sur la cybercriminalité du Conseil de l'Europe**⁵ (dite Convention de Budapest du 23.11. 2001), sans pour autant définir explicitement le terme de cybercriminalité, n'en définit pas moins les infractions relevant de celle-ci pour répondre, comme l'explique son préambule, notamment à « [...] la nécessité de mener, en priorité, une politique pénale commune destinée à protéger la société de la criminalité dans le cyberspace, notamment par l'adoption d'une législation appropriée et par l'amélioration de la coopération internationale [...] préoccupés par le risque que les réseaux informatiques et l'information électronique soient utilisés également pour commettre des infractions pénales et que les preuves de ces infractions soient stockées et transmises par le biais de ces réseaux [...] ».

Outre les différents délits identifiés par cette convention, celle-ci met l'accent sur « la nécessité d'une coopération entre les États et l'industrie privée dans la lutte contre la cybercriminalité, et le besoin de protéger les intérêts légitimes dans l'utilisation et le développement des technologies de l'information [...] une coopération internationale en matière pénale accrue, rapide et efficace [...] pour faciliter la détection, l'investigation et la poursuite, tant au plan national qu'au niveau international ».

Ainsi, le préambule de la convention délimite le pourtour de la cybercriminalité en inscrivant sa lutte dans le contexte de la protection des droits humains fondamentaux.

« Gardant à l'esprit la nécessité de garantir un équilibre adéquat entre les intérêts de l'action répressive et le respect des droits de l'homme fondamentaux, tels que garantis dans la Convention de sauvegarde des droits de l'homme et des libertés fondamentales du Conseil de l'Europe (1950), dans le Pacte international relatif aux droits civils et politiques des Nations unies (1966), ainsi que dans d'autres conventions internationales applicables en matière de droits de l'homme, qui réaffirment le droit à ne pas être inquiété pour ses opinions, le droit à la liberté d'expression, y compris la liberté de rechercher, d'obtenir et de communiquer des informations et des idées de toute nature, sans considération de frontière, ainsi que le droit au respect de la vie privée [...] Conscients également du droit à la protection des données personnelles, tel que spécifié, par exemple, par la Convention de 1981 du Conseil de l'Europe pour la protection des personnes à l'égard du traitement automatisé des données à caractère personnel ».

Le monde virtuel confère au crime la capacité à être automatisé, autorisant une réalisation à grande échelle (cyberépidémie), permettant d'être commis à distance via les réseaux (ubiquité du criminel, dans le temps et dans l'espace) et, avec ou non, des effets à retardement (figure 2.4).

5. Conseil de l'Europe – STCE no. 185 – Budapest 23.XI. 2001. <http://conventions.coe.int/Treaty/fr/Treaties/Html/185.html>

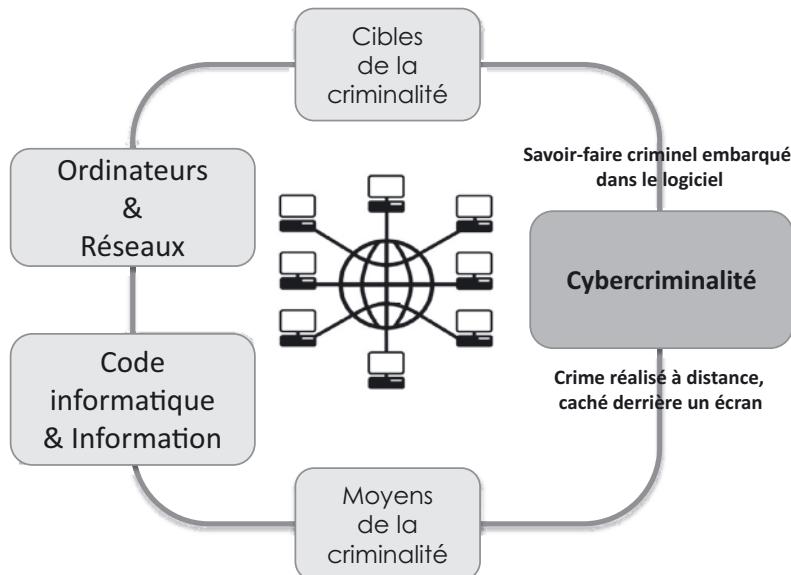


Figure 2.4 - Caractéristiques du crime informatique.

2.4.2 Écosystème cybercriminel

Les acteurs de la cybercriminalité, leurs modes opératoires et outils, les processus qu'ils mettent en œuvre pour maximiser leur profit tout en diminuant les risques d'être condamnés par la justice constituent un écosystème particulier. L'**écosystème cybercriminel** est, comme tout écosystème vivant et dynamique, en permanente adaptation pour tirer parti des nouvelles opportunités du marché, des nouvelles cibles et vulnérabilités, des nouveaux outils et vecteurs de la cybercriminalité. Il possède ses structures propres, mais utilise les acteurs licites d'Internet et bénéficie de leurs services. C'est le cas notamment des entités intervenant comme support à des transactions financières comme, par exemple, Western Union.



L'écosystème cybercriminel fait partie et est indissociable de l'écosystème numérique et de notre société.

Lorsque l'on considère l'écosystème cybercriminel, il ne faut pas oublier de prendre également en considération tous les acteurs licites c'est-à-dire des personnes morales ou physiques qui selon les circonstances peuvent être des cibles ou des relais volontaires ou involontaires de la cybercriminalité. Cette dernière distinction peut être motivée par exemple par le fait que des utilisateurs peuvent être leurrés et devenir, à leur insu, un maillon de la chaîne cybercriminelle. C'est le cas lorsque la machine d'un internaute ou le serveur d'une organisation servent de relais et sont devenus des machines *zombies* d'un réseau de *botnet*⁶ pour effectuer des attaques en déni de service sur des ordinateurs tiers. En revanche, un internaute peut également

tout à fait consciemment, par conviction ou motivation idéologique, politique, économique ou religieuse par exemple, « prêter » sa machine à un réseau de *botnet* pour contribuer à des actions d'hacktivisme. Des organisations privées ou publiques, tout à fait licites, peuvent aussi, pour défendre leurs intérêts, être amenées à utiliser les mêmes armes que les cybercriminels. Cela peut s'inscrire dans une démarche de **cybersécurité offensive et défensive**. Par ailleurs, dès lors que les organisations représentent des valeurs convoitées par les cybercriminels (institutions bancaires ou commerciales par exemple qui offrent des services en ligne), ou qu'elles sont productrices de valeurs, de services, de logiciels ou de solutions technologiques ou de sécurité, elles font partie *de facto* de l'écosystème cybercriminel. Leur présence dans le cyberspace, comme celle des internautes (très visibles à travers des réseaux sociaux par exemple), motive la présence des cybercriminels et le déploiement de leurs activités.

De plus, l'écosystème cybercriminel serait incomplet si on n'y intégrait aussi les **forces de justice et de police** qui œuvrent de manière opérationnelle et très concrète à la lutte contre la cybercriminalité. Elles conduisent des investigations criminelles et peuvent être amenées à mettre en place des pièges (notion de pot de miel, *honey pot*, leurre). Elles utilisent le même savoir-faire cognitif que celui des cybercriminels. Elles peuvent s'appuyer sur des compétences techniques spécifiques de policiers spécialement formés, d'experts civils externes ou encore s'appuyer sur les compétences de véritables cybercriminels, qu'ils soient repentis ou qu'ils n'aient pas d'autre choix que celui de collaborer avec la police. Ces derniers peuvent alors devenir des partenaires à part entière et agir en tant qu'indicateur ou contribuer activement à leurrer des cybercriminels, à tracer les activités criminelles et à démasquer les acteurs délictueux, en mettant en œuvre leur savoir-faire technique et leur connaissance du milieu cybercriminel.

Comme lors d'investigations classiques, les cyberinvestigations demandent un véritable savoir-faire policier car il ne suffit pas d'être un bon technicien pour être un bon **investigateur** en cybercriminalité. Ce dernier peut parfois agir sous pseudonyme lors d'infiltrations numériques pour mener des opérations de chasse aux pédophiles sur Internet par exemple.

L'écosystème cybercriminel profite de toutes les facilités offertes par les technologies du numérique, et des failles humaines, technologiques, juridiques ou procédurales, que cela soit sur le plan national ou à l'échelle internationale. Cela est facilité notamment par le fait que :

- tous les pays ne disposent pas forcément de la même volonté politique de lutter contre la cybercriminalité, ni des structures organisationnelles ou des ressources permettant de le faire ;
- les procédures liées à l'entraide internationale des forces de justice et de police sont souvent complexes et longues ;

6. La prise de contrôle de certaines machines, à l'insu de leurs propriétaires légitimes suite à une infection virale, transforme ces machines en « zombies » intégrés dans des réseaux de machines (les *botnets*) qui sont pilotés à distance pour réaliser des cyberattaques.

- les traces numériques peuvent être brouillées, effacées ou fausses. De plus, les traces numériques sont difficiles à collecter et à interpréter. Elles ne permettent pas toujours de remonter jusqu'à l'identité des criminels ;
- les cybercrimes se réalisent le plus souvent en impliquant de multiples acteurs aux compétences particulières et savoir-faire spécialisés dans des tâches spécifiques, séparées et restreintes (qui prises isolément peuvent paraître relativement mineures). Ces acteurs se regroupent en fonction de projets criminels à durée déterminée. Ils se constituent en équipes virtuelles réparties dans le monde entier. Ils travaillent ensemble pour des missions ciblées en recrutant des compétences ou en utilisant les outils nécessaires pour mener à bien une activité criminelle, en prenant le moins de risque possible.

Les cybercriminels disposent d'une souplesse et d'une réactivité très grandes, qualités que ne peuvent pas forcément posséder les acteurs et les structures de la lutte contre la cybercriminalité.

2.4.3 Marchés noirs de la cybercriminalité

Les cybercriminels sont des acteurs rationnels et suivent la **loi du marché** de l'offre et de la demande. Ils sont avant tout des criminels qui ont su extrapoler leurs activités, savoir-faire et modes d'action dans le cyberspace. Comme il existe, dans le monde réel, des **marchés noirs** et une **économie illicite**, il en est de même dans le cyberspace. Les marchés noirs de la cybercriminalité fonctionnent sur la base économique des marchés classiques et ont pour seuls objectifs performance et rentabilité. Il s'agit de marchés noirs bien réels qui alimentent toute la chaîne des acteurs de la cybercriminalité sur Internet. Ces **marchés noirs** s'appuient sur les outils de communication et de mise en relation de l'Internet dans le web profond (**deep web**), qui n'est pas directement accessible *via* des moteurs de recherche (notion de **dark web, darknet**). Ils utilisent les mêmes mécanismes, savoir-faire et outils que ceux liés à la publicité en ligne, au marketing et au e-commerce licites. Les marchés noirs de la cybercriminalité se trouvent à toutes les étapes de la réalisation des cybercrimes, de leur préparation à leur monétisation. De plus, Internet contribue largement à la valorisation de leurs bénéfices.

Parmi les scénarios impliquant des marchés noirs, il est possible par exemple :

- d'acheter un kit de phishing en ligne (Forum/shop), de l'installer sur un serveur *bullet proof* (plateformes matérielles et logicielles où aucune force de l'ordre n'interviendra), de l'exploiter (réaliser du phishing), de collecter des données obtenues par phishing et de revendre ces données *via* des forums, des shops, des services de transactions financières, etc. ;
- de vendre et d'acheter des **exploits** (codes malveillants qui exploitent des vulnérabilités, logiciels d'intrusion, virus (*malwares*), **rançongiciels** (*ransomware*) permettant de réaliser des cyberattaques et du chantage) ;
- de louer des machines zombies et de mettre en œuvre des *botnets* pour réaliser des **attaques en déni de service distribué (DDoS)** ou d'envoyer des spams ;

- de vendre et d'acheter en gros ou au détail des données personnelles (identifiants bancaires, etc.).

Le tout est bien souvent réalisé en utilisant une monnaie virtuelle telle que le bitcoin.

Les marchés noirs de la cybercriminalité s'articulent beaucoup autour des besoins suivants :

- découverte de vulnérabilités qui peuvent être exploitées pour réaliser des attaques. Un avantage concurrentiel est procuré aux premiers acteurs ayant découvert des failles et qui savent les monétiser à des fins malveillantes. Toutefois, la majorité des fournisseurs de services propose des récompenses afin d'éviter l'usage criminel de ces vulnérabilités (notion de *Bug Bounty*) ;
- disposer d'outils exploitant ces vulnérabilités ;
- s'appuyer sur des personnes qui contribuent à réaliser des cybercrimes (spécialistes en informatique et télécoms, en ingénierie sociale, experts en sécurité, hackeurs, développeurs de code, utilisateurs victimes ou complices, mules pour le transfert d'argent par exemple, etc.).

Précisons aussi qu'il existe un vrai marché de vente des failles trouvées dans les applications, certaines failles pouvant se monnayer plusieurs centaines de milliers d'euros.

Les marchés noirs de la cybercriminalité suivent les fluctuations du marché, qui peuvent être fortement dépendantes du cycle de vie des vulnérabilités. En effet les vulnérabilités non encore connues, qualifiées de **0-day** et pour lesquelles il n'existe pas de solution de sécurité, sont les plus onéreuses (et donc les plus rentables pour ceux qui les commercialisent). Elles sont aussi les plus efficaces pour ceux qui les exploitent. Toutefois, plus elles sont exploitées ou plus leurs impacts sont forts, plus il est possible que des contre-mesures de sécurité soient créées. Les vulnérabilités, et par conséquent les exploits, deviennent moins avantageux pour les criminels, ils se déprécient et finissent par devenir obsolètes.

L'équilibre de l'écosystème cybercriminel se maintient si dans le temps les acteurs obtiennent des gains financiers bien supérieurs aux risques d'être poursuivis par les forces de l'ordre. Cela dépend des risques réels, qui peuvent être plus ou moins bien maîtrisés et contrôlés selon les stratégies criminelles développées, mais aussi selon la perception de ces risques. Entre la maximisation des valeurs issues de la cybercriminalité, la rapidité des gains, et les risques d'être pris, certains cybercriminels ont su développer une réelle **intelligence économique** dynamique et adaptive au service du crime.

Le **blanchiment d'argent** est dénommé « le crime des crimes » dans la mesure où il existe du fait d'activités initiales illégales (argent du crime) et que les revenus générés par le blanchiment permettent de réaliser d'autres crimes.

Ainsi, comme tous les criminels qui profitent des infrastructures technologiques mises en place, les blanchisseurs de fonds recourent de plus en plus à Internet afin de pouvoir utiliser légalement des capitaux générés par les activités criminelles telles

que le trafic de drogue, la vente illégale d'armes, la corruption, le proxénétisme, la pédophilie, etc.



Internet permet alors en toute impunité, ou presque, la réinsertion de l'argent sale dans les circuits économiques par le biais de transferts de flux, d'investissements et de capitalisation.

Les placements boursiers ou les casinos en ligne, le e-commerce, avec des ventes de produits et services fictifs contre paiement réel générant des bénéfices justifiés, le e-banking, les transactions du foncier et de l'immobilier *via* le Net, la création de sociétés virtuelles « écran » ou encore les porte-monnaie électroniques, les **crypto-monnaies**, peuvent être utilisés pour effectuer les opérations nécessaires au blanchiment. Ce sont des activités incontrôlables et les poursuites en justice se révèlent parfois impossibles. En ayant recours à certains services dématérialisés, l'internaute peut favoriser inconsciemment le développement du blanchiment d'argent sur Internet. Les entreprises peuvent également être fortuitement impliquées dans ce processus, et éventuellement en subir des conséquences judiciaires et commerciales.

2.5 ATTAQUES INFORMATIQUES VIA INTERNET

2.5.1 Étapes de réalisation d'une cyberattaque

L'ingéniosité des attaquants peut être parfois sans limite. Généralement, ils savent s'adapter et exploiter efficacement les ressources disponibles et les vulnérabilités, de manière permanente et dynamique. Bien qu'il soit impossible de dresser un panorama exhaustif des types et des moyens d'attaques⁷, il est toutefois possible d'en dégager certains invariants.

Comme le montre la figure 2.5, la réalisation de cyberattaques suit une **méthodologie d'attaque** qui se décompose communément en plusieurs étapes. La première est relative à la connaissance de la cible par une collecte d'informations et la recherche de vulnérabilités la concernant.

Cela consiste essentiellement à prendre connaissance des mécanismes et des niveaux de sécurité en vigueur concernant l'identification, l'authentification, le contrôle d'accès, la cryptographie, la surveillance et à identifier les failles techniques, organisationnelles et humaines de l'environnement. De plus, l'attaquant pourra tirer parti de la naïveté ou de la crédulité des utilisateurs pour leur soutirer des informations facilitant la création d'une attaque (notion d'**ingénierie sociale**⁸, *social engineering*). Ainsi, il pourra obtenir leurs clés d'entrée dans les systèmes informatiques (identification de l'utilisateur et mot de passe), pénétrer les systèmes et effectuer toutes sortes d'opérations de lecture ou d'écriture.

7. Ce qui d'ailleurs n'est pas la vocation de cet ouvrage, qui en aucun cas ne souhaite inciter, encourager la pratique d'attaques informatiques ou donner des éléments précis pour les réaliser.

8. Manipulation d'une personne pour l'inciter à livrer des informations sensibles à son insu.

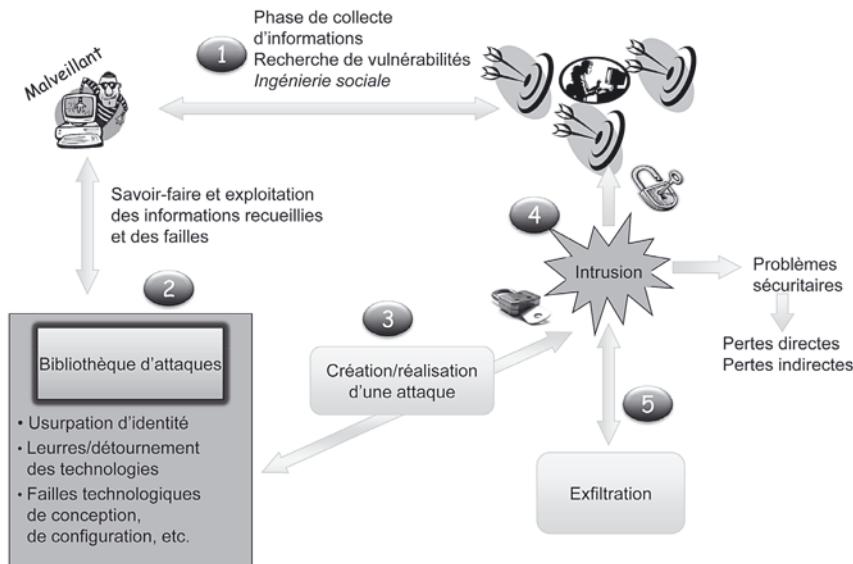


Figure 2.5 – Phases caractéristiques du déroulement d'une attaque.

Le fraudeur s'emploie également à détecter et à exploiter les défauts ou **failles de sécurité**. Celles-ci peuvent être publiquement connues mais non encore réparées (non *patchées*). Il pourra alors utiliser les outils d'attaques préexistants et éventuellement disponibles en ligne (phase 2), les paramétrier en fonction de ses besoins ou encore en créer de toutes pièces pour accéder au système ciblé et exécuter son action malveillante (phase 3).

Il s'ensuit une phase d'**exfiltration** (phase 4) qui a pour objectifs d'une part de faire en sorte que l'attaque ne puisse être détectée ou du moins ni facilement ni rapidement et, d'autre part, que l'attaquant ne laisse pas de trace pouvant servir à son identification. Pour contribuer à cela, il tente de rester anonyme, il utilise de fausses identités ou des alias (pseudonymes), il usurpe l'identité numérique d'utilisateurs, il brouille les pistes en passant par plusieurs systèmes intermédiaires par exemple. L'enjeu pour le malveillant est alors de ne pas laisser la trace de son passage et de son maintien dans les systèmes visités. En effet, pour sa sécurité personnelle, dans la mesure où il a perpétré un **acte illégal** aux suites judiciaires parfois lourdes, il a tout intérêt à savoir effacer toute information qui permet de lier la preuve de sa présence et de ses actions illicites à des données qui autorisent sa localisation et son identification.

2.5.2 Attaques actives et passives

Les attaques qui modifient les données sont dites **actives**, tandis que celles relevant de l'écoute – interception sans altération des données – sont qualifiées de **passives** (figure 2.6).

De manière générale, les cyberattaques se fondent principalement sur :

- le détournement du mode opératoire normal des ressources (protocoles de communication, caractéristiques des systèmes d'exploitation, etc.) ;
- l'exploitation des failles et des vulnérabilités des ressources ;
- leurre des personnes et des systèmes.

Quelques types d'attaques et principes généraux sont présentés ci-après afin de mettre en évidence d'une part la manière dont les capacités informatiques peuvent être abusées et d'autre part de comprendre le type de mesure de sécurité à mettre en œuvre pour les protéger.

La **malveillance informatique** a souvent une origine interne, même si elle est réalisée à distance. Elle est à la portée des personnes en charge de l'administration des systèmes et de la gestion opérationnelle de l'environnement informatique ou de celles habilitées à accéder aux ressources.

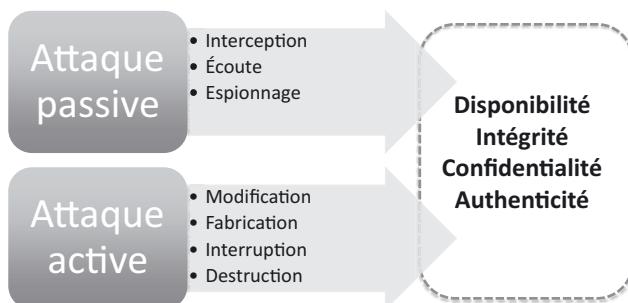


Figure 2.6 – Attaques passives et actives.

2.5.3 Attaques fondées sur l'usurpation de mots de passe

Il est plus facile de s'approprier les paramètres de connexion des ayants droit que de forcer les protections logicielles des mécanismes de contrôle d'accès. Parfois, le mot de passe est tellement évident (prénom de la personne, des membres de sa famille, 123456, etc.) qu'il est facile à deviner. Par ailleurs, il est possible que les malveillants obtiennent toutes les informations nécessaires à la construction d'une attaque par :

- **complicité interne** (les identifiants et paramètres de connexion peuvent être volontairement communiqués par les utilisateurs ou administrateurs systèmes) ;
- **leurre des personnes** en se faisant passer pour un administrateur réseau, un fournisseur de service, et en demandant, pour des raisons techniques par exemple, les paramètres de connexion. Dans trop de cas, les utilisateurs donnent leurs identifiants, mots de passe et informations normalement confidentielles. Cela relève des techniques de manipulation et d'intelligence sociale et de l'ingénierie sociale (*social engineering*) qui peuvent s'appuyer sur des techniques de phishing.



Phishing : mot dérivé des termes **phreaking**, (détournement de communications des centraux téléphoniques analogiques) et de **fishig** (pêche à la ligne). Il s'agit de leurrer les internautes afin de les inciter à livrer eux-mêmes, sur un site web ou en répondant à des messages, leurs informations sensibles (identifiants, mots de passe, numéros de compte, etc.), qui seront ensuite exploitées à des fins malveillantes.

Certains individus malveillants ne sont pas forcément des génies de l'informatique, mais ils ont su, en revanche, développer un certain savoir-faire en matière d'escroquerie et obtenir pernicieusement les clés correspondant aux serrures des systèmes qu'ils désirent pénétrer.

Par ailleurs, d'aucuns sauront **accéder** à des fichiers de mots de passe protégés ou encore les **intercepter** lorsqu'ils sont véhiculés en clair par les protocoles de communication (écoute passive par surveillance [*monitoring*] des paquets IP).

Des logiciels d'analyse du trafic (*sniffer*) sont courants et largement utilisés à des fins de gestion de réseau, certains étant généralement livrés en standard avec divers systèmes d'exploitation, d'autres étant accessibles en *freeware* sur le réseau. Ils s'exécutent sur n'importe quel ordinateur en reniflant (*sniffing*) et en analysant les données en transit sur les lignes, afin d'extraire les mots de passe transmis en clair par l'utilisateur lors de sa demande de connexion.



Un **sniffer** est une entité passive qui écoute et enregistre les données qui le traversent. Ne les modifiant pas, sa présence est pour cette raison très difficile à déceler. Pour restreindre son champ d'action, une parade envisageable consiste à fortement segmenter le réseau, à le cloisonner par des mesures d'architecture, afin que le *sniffer* ne soit effectif que sur un segment du réseau.

L'**écoute passive** des données en transit peut conduire, après utilisation des mots de passe capturés, à des intrusions illicites sur des systèmes. Une protection à apporter aux mécanismes de transfert est de chiffrer les mots de passe de manière à ce qu'ils ne soient plus directement exploitables. En effet, leur utilisation dépend alors de la capacité du délinquant à « casser » (craquer) les mots de passe chiffrés préalablement capturés.

En cas de capture de mots de passe chiffrés, l'individu malveillant tentera par exemple de deviner le mot de passe en essayant toutes les permutations possibles pouvant constituer une clé pour déchiffrer le mot de passe. Cette action est facilitée s'il connaît l'algorithme de chiffrement utilisé. Il s'agit là de l'**attaque en force brute** (*brute force attack*). Une alternative à cette attaque est celle dite d'**attaque par dictionnaire** (*dictionary attack*), ou *Rainbow tables*, qui revient à deviner le mot de passe chiffré, par comparaisons successives avec des listes de mots de passe, eux aussi chiffrés, contenus dans des dictionnaires d'empreintes.



Tester le niveau d'efficacité des mots de passe des utilisateurs est une des mesures de contrôle et de validation de la sécurité que le responsable sécurité doit effectuer régulièrement. Pour cela, il utilise des mécanismes identiques à ceux utilisés par les malveillants pour les obtenir et les déchiffrer.

Pour détourner des mots de passe, on peut également introduire dans le poste de travail de l'usager un logiciel espion (espiogiciel, *spyware*) ou encore un **cheval de Troie**. Il s'agit alors d'un petit programme qui se substitue généralement à celui qui permet d'effectuer le *login* et demande à l'utilisateur son identification et son mot de passe. Ce dernier fournit les informations demandées en croyant avoir à faire à son propre environnement d'exécution. Le mot de passe est alors directement capté et mémorisé par le cheval de Troie, qui le transmet à un serveur auquel se connectera le fraudeur⁹.

Par ailleurs, des systèmes de gestion de contrôle d'accès peuvent comporter des **portes dérobées** matérielles ou logicielles (*backdoors*) permettant de contourner les mécanismes de sécurité en place afin d'autoriser des accès illicites à ceux qui les maîtrisent.

Des **périphériques multimédia activés** à l'insu de l'utilisateur, comme des **dispositifs logique ou physique d'espionnage** (enregistreur de frappe, *keylogger*, etc.) permettant de surveiller et de capter de l'information sans le consentement de l'utilisateur, autorisent ainsi un intrus à s'approprier des informations confidentielles. Il convient donc que l'utilisateur soit extrêmement vigilant et connaisse bien son environnement informatique. Les périphériques de capture (webcam, micro, etc.) devraient être systématiquement désactivés lorsque leur usage n'est pas demandé par l'utilisateur, et il faudrait que de tels périphériques alertent ce dernier lorsqu'ils sont actifs.

Pour qu'un système d'authentification fonctionne, il est nécessaire de sauvegarder dans un **serveur**, et de manière sûre, les paramètres de connexion et d'authentification des utilisateurs. L'accès illicite au fichier qui les stocke est souvent possible. Il est donc impératif de protéger correctement l'accès aux serveurs et aux données d'authentification.

La faiblesse dans le choix des mots de passe (noms courants de personnes, de vedettes, de vins, d'animaux, de personnages de bandes dessinées ou de dessins animés, d'objets, mots du dictionnaire, dates, etc.), la puissance de calcul des ordinateurs et l'existence banalisée de logiciels qui permettent de les casser, de les craquer font que le contenu d'un **fichier de mots de passe** chiffré peut devenir accessible. Le temps d'exécution nécessaire à la réalisation de cette activité peut éventuellement être rédhibitoire pour un petit délinquant.

Du côté du **serveur d'authentification**, il faut impérativement protéger l'accès au fichier de mots de passe et donc ne pas autoriser d'**accès anonymes** sur ce type de serveur, et désactiver le protocole TFTP (*Trivial File Transfer Protocol*), qui permet d'accéder à des fichiers sans contrôle d'authentification. On peut également masquer le fichier de mots de passe en faisant pointer son contenu vers un autre fichier qui,

9. Entre-temps, l'utilisateur n'a pas pu se connecter puisque le véritable programme de connexion ne s'est pas exécuté. Il a vu apparaître à son écran le message du type erreur, mot de passe incorrect. Il pense automatiquement qu'il a effectué une erreur de saisie, il se « relogue » et redonne son mot de passe, qui cette fois sera traité par le véritable programme de *login*.

lui, contient véritablement l’information sensible. En réalité, on introduit un **masque** et on retarde uniquement, sans vraiment l’empêcher, l’accès aux mots de passe.

Une méthode d’authentification qui propose une protection contre l’utilisation de mots de passe dérobés est celle fondée sur l’utilisation de **mots de passe à usage unique**. Celle-ci est largement mise en œuvre, entre autres, pour effectuer des transactions financières. Ainsi, par exemple, si l’on dispose d’un périphérique de lecture adapté du côté de l’utilisateur, on peut utiliser une **Smart Card** (carte sécurité) qui génère, à chaque transaction, un mot de passe unique et différent. Par ailleurs, il existe des **cartes réseau PCMCIA** (*Personal Computer Memory Card International Association*) qui se substituent aux *Smart Cards* et à leur unité de lecture pour exécuter elles-mêmes la procédure d’authentification. Ces deux versions d’authentification, outre le fait qu’à chaque usage le mot de passe est différent, évitent la mémorisation et la saisie de mots de passe longs et complexes par l’usager.

Tout système possède une faille et ce type d’authentification n’échappe pas à cette règle. En fait, la procédure d’authentification est fondée sur la **synchronisation temporelle** du client et du serveur. Certains savent exploiter cette caractéristique à des fins malveillantes, en captant, à son émission, un mot de passe pour le réutiliser tout de suite après une **désynchronisation** déclenchée par la modification des horloges des systèmes. Toutefois, cela nécessite de la part du fraudeur des moyens et des efforts importants.

Des environnements et des transactions pourront également être protégés par la mise en place de systèmes d’identification fondés sur une caractéristique physique de la personne comme une empreinte digitale par exemple (identification biométrique). Plus difficile et contraignant à mettre en œuvre, ce système d’authentification n’est pas toujours optimal dans la mesure où il est tributaire des modifications inhérentes à tout organe vivant.



Quel que soit le mode d’interception, les utilisateurs ignorent généralement que leurs mots de passe ont été capturés par des cyberprédateurs.

Un internaute peut se voir accusé des malveillances commises par l’usurpateur de ses paramètres de connexion. Il est considéré comme responsable jusqu’à ce qu’il ait pu prouver son innocence ! La preuve de l’innocence est à la charge des victimes. De ce fait, on comprend l’importance à accorder à la protection des identifiants de connexion.

2.5.4 Attaques fondées sur leurre

Dans son acception courante, le **pirate informatique** est la traduction française du terme anglo-saxon **hacker**, qui désigne une personne qui pénètre virtuellement dans un système informatique, alors qu’elle n’en a pas le droit *a priori*.

Le mot *hacking* trouve son origine dans le vocabulaire de cuisine, signifiant le hachage « menu-menu » des aliments. Par extrapolation, il qualifie désormais les activités qui consistent à découper très finement (décortiquer) le mode de fonctionnement d’un ordinateur, afin d’en comprendre tous les rouages et éventuellement les

détourner. Il réside toujours une différence entre le fait de comprendre les limites des protections, de rechercher des failles et celui de les exploiter à des fins malveillantes. La limite peut être ténue ou parfois la tentation grande.

Désormais, le *hacking* possède une connotation négative et représente généralement l'ensemble des opérations permettant de s'introduire sans autorisation (par leurre et détournement des technologies) et donc de manière illégale dans un système appartenant à un tiers. Ainsi, sur cette base, l'**intrusion éthique** « *ethical hacking* » est un oxymore car il allie deux mots opposés sémantiquement. Dans la majorité des cas, il s'agit de tests d'intrusions réalisés dans le cadre d'une démarche sécuritaire, par des personnes mandatées, pour tester la robustesse des accès à des environnements informatiques, ce qui n'est alors pas illégal mais autorisé par les mandants. Ces personnes sont tenues, par contrat, à la discréetion la plus absolue. Il ne faut pas croire qu'il faille toujours posséder un haut niveau de compétences informatiques pour cela. En effet, généralement il est plus simple et plus rapide d'exploiter la crédulité des employés ou de les leurrer pour les inciter à livrer leurs paramètres de connexion et ainsi obtenir des droits d'accès au système informatique pour s'y introduire.

En fait, plusieurs méthodes existent pour pénétrer un système en le leurrant. Elles se basent sur les sources de vulnérabilités des environnements Internet mais aussi sur certaines caractéristiques du mode opératoire des protocoles, des systèmes d'exploitation, des processeurs ainsi que sur des configurations ou une gestion défaillante des systèmes. Il suffit alors d'exploiter les informations relatives à ces situations.

La réalisation de malveillances fondées sur le leurre se base sur l'usurpation d'identité, des paramètres de connexion, d'adresses IP (*IP spoofing*), sur des modifications affectant le routage (redirection de flux de données), sur le vol de connexions TCP ou sur le détournement de flux applicatifs (*man in the middle attacks*) par exemple. Elles exploitent les possibilités intrinsèques des divers protocoles de communication d'Internet (forme d'**escroquerie électronique**).

2.5.5 Attaques fondées sur le détournement des technologies

Une attaque conduisant à un déni ou refus de service (**DoS**, *Denial of Service*) peut être réalisée en sollicitant excessivement des ressources. Ne possédant pas la capacité de traiter un tel afflux de demandes, les systèmes ciblés, surchargés par un trop grand nombre de requêtes « normales », s'effondrent et deviennent indisponibles. La majorité des **attaques en déni de service** (figure 2.7) se font de manière distribuée à partir de multiples machines intégrées à des réseaux de *botnets* (**DDoS**, *Distributed Denial of Service*). Les attaques occasionnant un déni de service sont considérées par la loi comme un acte criminel. Il peut par exemple s'agir d'attaque par inondation de messages (*mailbombing*), consistant à submerger la boîte aux lettres électronique d'un utilisateur ce qui entraîne, outre des désagréments, des dénis de service.

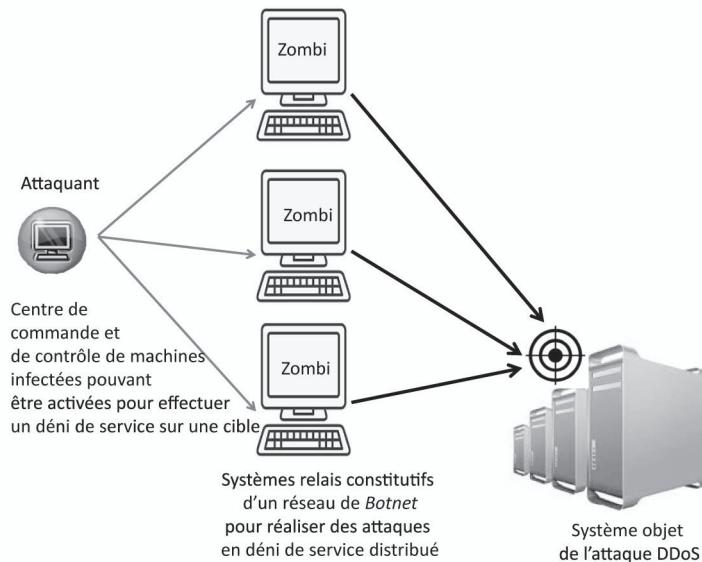


Figure 2.7 – Attaque en déni de service distribué.

La plupart des attaques ciblent les systèmes jouant un rôle important dans la réalisation de services (serveurs web, routeurs, serveurs de noms, etc.). Elles peuvent être perpétrées en tirant parti des failles de leur système d'exploitation et utiliser, par exemple, ses caractéristiques internes, notamment celles de leur gestion de certaines **zones tampon** (*buffer overflow attack*) entraînant des dysfonctionnements graves pouvant conduire à l'arrêt des systèmes. Les attaques en déni de service sont des armes largement utilisées par les membres du groupe d'hacktivistes *Anonymous*, dont le slogan est « *We are Anonymous. We are Legion. We do not forgive. We do not forget. Expect us.* »

2.5.6 Attaques fondées sur la manipulation de l'information

Certaines attaques consistent en une modification de la page d'accueil d'un site web (**defacement attack**). Les pirates substituent les données officielles d'un site et les remplacent selon leur motivation, par certains contenus (graffitis). Pour les entités victimes, les conséquences peuvent être très importantes en termes d'image. Des réputations peuvent être durablement ternies surtout si la confiance est un élément fondamental du positionnement stratégique de la cible visée (banques, hôpitaux, etc.). Des variantes plus lucratives de ce type d'attaque ont pour objectif de rediriger l'utilisateur, lors d'action de phishing par exemple, vers un faux site ressemblant exactement à celui auquel il s'est initialement connecté (notion de redirection, ou de **pharming** quand l'attaque porte sur les serveurs de noms de domaines), afin de lui soustraire des informations confidentielles (mots de passe, numéro de carte bancaire, etc.). Il est possible de s'attaquer à des sites d'information et de modifier le contenu de certaines pages ou dépêches pour provoquer des mouvements de panique, ou faire

fluctuer le cours d'actions d'une société par exemple. Ces actions de désinformation relèvent de l'**infoguerre** (*infowar*) et permettent de mener des **attaques sémantiques** (*semantic attack*). Elles touchent au sens même des informations et croyances qui servent à chacun pour former son jugement.

2.6 FAIRE FACE À LA CYBERCRIMINALITÉ

2.6.1 Chiffre noir de la cybercriminalité

Il existe une réelle difficulté à obtenir les chiffres relatifs à la cybercriminalité et à estimer ses coûts direct et indirect pour la société. Le chiffre noir de la cybercriminalité, qui représente le nombre de crimes inconnus des services de police dans la mesure où aucune plainte n'a été déposée, est considérable. Il indique l'écart entre la malveillance connue et celle bien réelle. Ce manque de statistiques officielles trouve largement ses origines dans le fait que les organisations :

1. ignorent qu'elles sont victimes d'une malveillance, notamment pour toutes attaques passives (détournement transparent de données, de flux, écoutes clandestines, introduction non détectée dans des systèmes, etc.), ou n'en prennent conscience qu'*a posteriori*, lorsque toute action de réaction devient obsolète ;
2. ne souhaitent pas forcément communiquer sur le fait qu'elles ont été victimes, ce qui révélerait leur vulnérabilité technologique ou défaillance sécuritaire ;
3. ne savent pas gérer une situation de crise ;
4. n'ont pas une confiance suffisante dans les instances de justice et de police et dans leur compétence pour traiter ce type de problème ;
5. ne sont pas persuadées de l'intérêt de la démarche de révélation du délit (espoir faible d'obtenir réparation, doute sur l'aide effective qui pourrait être apportée durant une période de crise, sur la réactivité des instances judiciaires, etc.) ;
6. pensent que la démarche est complexe, lourde, onéreuse, consommatrice d'énergie, de temps, de ressources, alors que les entreprises sont focalisées sur la résolution de l'incident afin d'assurer la continuité des services ;
7. ont de la difficulté à comprendre l'incident, son origine, à identifier, à collecter, à préserver des traces ;
8. préfèrent gérer seules leurs cyberproblèmes.

2.6.2 Culture de la sécurité

Il faut distinguer les organisations qui possèdent une culture de la sécurité, telle que spécifiée dans les directives de l'OCDE¹⁰ et qui se sont dotées de moyens financiers, organisationnels, humains et technologiques pour gérer la sécurité de leur système

10. Lignes directrices de l'OCDE régissant la sécurité des systèmes et des réseaux d'information : vers une culture de la sécurité. Recommandation du conseil de l'OCDE, 25 juillet 2002 (<http://www.oecd.org/dataoecd/16/22/15582260.pdf>).

d'information, de celles qui ne l'ont pas. Ces dernières subissent et ne maîtrisent aucunement le risque informatique. Dans tous les autres cas, des réponses variées, qui tiennent compte des situations à maîtriser et du degré de compétence et d'expérience des entreprises en matière de sécurité, sont apportées. Ainsi, les organisations définissent leur stratégie de sécurité en fonction de leurs valeurs, de leurs besoins et de la manière dont elles appréhendent les risques.

Les mesures peuvent se décliner en mesures préventives, palliatives, correctives, de protection, de dissuasion ou de réaction. À ces mesures d'ordre organisationnel, technique ou juridique, il faut associer la définition et la réalisation des plans de gestion de crise, de continuité de service, des stratégies de contrôle, d'évaluation, de suivi et d'optimisation des politiques, mesures, solutions et procédures de sécurité, sans oublier la prise en compte des besoins d'assurance du risque et des démarches de veille technologique.

Dans une mise en perspective historique de l'évolution de la cybercriminalité, qui tient compte de la réalité de l'actualité, de grandes tendances ont émergé en termes de type d'actions malveillantes. Retenons trois catégories significatives de cybercrimes du point de vue de la réaction des entreprises face à ces délits :

- les programmes malveillants ;
- l'intrusion dans les systèmes ;
- la prise en otage des ressources, le chantage.

Programmes malveillants

En dépit du déploiement de moyens techniques, des sommes investies par les fournisseurs de service pour le bloquer, et malgré l'annonce faite par les autorités de vouloir combattre ce fléau et les condamnations de spammeurs prolifiques, le spam continue à être une nuisance et un vecteur d'infection.



Spam : mot dérivé de *SPiced hAM* (*Spiced Pork And Meat*, sorte de pâté en boîte) ayant fait l'objet d'un sketch des Monty Python, le mot est tellement répété qu'il en devient une nuisance.

Des **programmes malveillants** ou indésirables s'exécutant à l'insu de l'utilisateur existent généralement sous couvert d'outils d'aide à la navigation, à la connexion, à la personnalisation des services : **téléchargeur** et **implanteur** (*down-loader*), **keyloggers**, **bot-robots**, **logiciels publicitaires** (*adware* : *advertising software*) ou **logiciels espions** (*spyware* : *spying software*). Ce sont pour la plupart des outils de capture d'informations (vol d'informations, capture de mots de passe, de trafic), d'appropriation de ressources, ou d'attaques. Ils permettent de diffuser et de piloter des outils d'attaques en **déni de service distribué** (DDoS). Les vecteurs d'introduction de tels logiciels peuvent être des logiciels gratuits ou en démonstration, des sites pornographiques ou de jeux par exemple.

Quel que soit leur mode d'introduction, même s'ils sont installés avec l'accord implicite de l'utilisateur, ce qui peut être le cas des *adwares* mais jamais des

spywares, leur usage est détourné. Le plus souvent, ils s'exécutent en l'**absence de consentement des utilisateurs**, collectent et transfèrent leurs données à leur insu.

La **détection** et la **désinstallation** de tels logiciels sont parfois difficiles. De manière générale, l'internaute ne possède pas les compétences ou les outils nécessaires pour maîtriser ce risque.

Les **virus** n'ont plus pour objectif principal de faire dysfonctionner, de voler ou de détruire des données, ils sont également des vecteurs de réalisation de la criminalité économique et constituent des moyens d'enrichissement considérable pour leurs auteurs.

Il semble que la prise en compte, par les organisations, de la propagation des virus par la messagerie électronique soit meilleure de nos jours. En effet, on constate une progression de l'usage et de la gestion des antivirus et des antispams sur les serveurs de messagerie et sur les postes de travail des utilisateurs. Parallèlement, les entreprises ont également adopté un plan de sensibilisation des utilisateurs à ce type de problèmes.

Intrusion dans les systèmes

L'intrusion dans les systèmes peut conduire par exemple à de l'espionnage, à l'hébergement de contenus illicites, à l'installation de programmes malveillants, à la prise de contrôle des systèmes, à la falsification de sites web, au vol de données, à des dénis de service. Toutefois, le vol de données peut résulter tout simplement de vol de matériel (ordinateurs portables, serveurs, clés USB...).

Les **plans d'action et de réaction** à ce type de cybercrime dépendent essentiellement de la détection de ce dernier. Cela est fonction du niveau d'adoption des mesures de sécurité et de gestion des systèmes (existence d'outils de surveillance, de détection d'incidents, d'audit actif, d'évaluation de performances, d'identification de comportements anormaux, d'analyse de trafic, d'administration système, d'existence de plan de secours...). La réponse sera graduée et variera en fonction du processus d'attaque, de la phase de réalisation, de l'importance et de la cible de l'attaque, et en fonction des moyens et compétences à disposition pour réagir et mettre en place des mesures pour que cela ne se reproduise pas.

Le responsable sécurité s'attachera à **limiter** la propagation d'une attaque, à **réduire** les impacts de l'attaque et à **réparer** les atteintes ou dégâts engendrés. Éventuellement, il cherchera à comprendre l'incident et à en identifier l'origine.

Chantage

Lors de procédures de chantage (annonce d'attaques, de divulgation de données, de blocage de systèmes pouvant conduire à des interruptions de services, à des incapacités à produire, à une détérioration de l'image, ou à des pertes de crédibilité ou de savoir-faire par exemple) avec des demandes de rançons d'un montant variable, pouvant aller de quelques centaines à plusieurs dizaines de milliers d'euros, diverses

attitudes sont adoptées selon le contexte. En effet, les alternatives offertes aux organisations sont les suivantes :

- ignorer la demande ;
- signifier à l'attaquant que l'entreprise possède des moyens d'identifier le malveillant, ce qui peut être vrai ou relever d'un processus d'intimidation/dissuasion (qui peut être efficace) ;
- payer la rançon demandée ;
- ajuster les mesures de sécurité afin de protéger au mieux l'environnement menacé ou de réduire les impacts de l'attaque annoncée ;
- dénoncer aux autorités compétentes la tentative de *racket*.

Pour faire face à l'augmentation des risques cybercriminels, certaines organisations se réapproprient les fondamentaux de la sécurité pour préserver la disponibilité, l'intégrité et la confidentialité de leurs ressources informationnelles. Elles peuvent être amenées à reconsiderer les notions d'ouverture de leur système d'information, d'accessibilité et de connectivité étendue. Cela suppose de segmenter fortement l'architecture du système d'information, d'en isoler certaines parties et de limiter les informations et services en ligne, de mettre en place des mesures de contrôle et de surveillance.

2.6.3 Limites des solutions de sécurité

Quelles que soient les motivations des acteurs de la criminalité informatique, celle-ci engendre toujours des conséquences économiques non négligeables fragilisant les organisations. C'est du ressort de la **sécurité informatique** de contribuer à réduire le risque technologique encouru.

 Les solutions de sécurité sont des réponses statiques à un problème dynamique mais sont surtout le plus souvent encore, des réponses d'ordre technologique à des problèmes humains, managériaux, économiques ou politique.

La sécurité informatique doit, d'une part, s'adapter aux paradigmes mouvants de l'informatique et des télécommunications et, d'autre part, à celui de la criminalité, tout en s'inscrivant dans une logique de rentabilité pour l'organisation qui la met en œuvre. Or, la multiplicité des éléments matériels, logiciels, réseaux et des acteurs impliqués comme l'inexpérience et l'inconscience de certains utilisateurs, favorise l'expression de la criminalité informatique.

 L'inadéquation plus que l'insuffisance des moyens de protection aux risques réels détermine un **état d'insécurité** qui profite aux criminels.

2.6.4 Contribuer à lutter contre la cybercriminalité et à diminuer le risque d'origine cybercriminelle

Mettre en place des mesures efficaces de **lutte contre la cybercriminalité** doit s'appuyer sur la connaissance des acteurs, de leurs motivations et de leurs manières d'agir. Cela demande de comprendre quelle est leur vision stratégique, quels sont les

moyens opérationnels qu'ils utilisent, comment ils sont organisés, quelle est la répartition des tâches, de quelle manière leurs agents sont recrutés, comment ils sont rémunérés, quels sont les processus, quels sont leurs modèles économiques, comment l'argent du crime est blanchi, etc.

Autant de questions auxquelles il est difficile d'apporter des réponses catégoriques puisque les criminels ont tout intérêt à agir dans l'ombre et en toute discréction. L'obscurité, comme la corruption d'ailleurs, apporte une couche d'isolation protectrice aux activités délictueuses et aux criminels de toutes sortes.

L'ampleur des activités cybercriminelles, la nature des cybercriminels pouvant aller de M. et M^{me} Tout-le-Monde à des spécialistes de l'informatique ou de la grande criminalité organisée, en passant par des mercenaires à la solde des plus offrants, comme le champ d'action mondial des cybercriminels contribuent à la difficulté de dresser un panorama définitif des acteurs de la cybercriminalité ou de quantifier à sa juste valeur les coûts que la cybercriminalité fait porter sur la société.

Par ailleurs, la nature **dynamique** du phénomène cyber criminel, dont les acteurs s'organisent en fonction d'opportunités qui évoluent sans cesse, ne permet pas de figer une image. Plutôt qu'une vue statique, des tendances peuvent être dégagées, sur une période donnée, de la perception du phénomène cybercriminel, selon des indicateurs retenus et la finalité des études ou des observations.

La majorité des acteurs de la sécurité informatique, actifs au niveau international, possèdent leurs propres éléments de mesure et d'analyse de la cybercriminalité. C'est le cas par exemple des sociétés comme Verizon, Kaspersky, RSA, McAfee, PWC, pour n'en citer que quelques-unes. De plus, au niveau national comme au niveau international, des études, concernant les cyberproblèmes au sens large sont régulièrement publiées. Il existe très peu d'études de victimologie et lorsqu'elles existent elles concernent un échantillon de crimes, de la population d'auteurs et de victimes concernées, par pays. De plus, il semblerait que moins de 20 % des cybercrimes soient rapportés aux services de justice et police. À cela s'ajoute que le vol d'informations numériques est difficilement identifiable et quantifiable (les données sont juste copiées) comme le sont d'ailleurs l'espionnage, les attaques passives, la surveillance abusive des activités, la désinformation, la manipulation d'opinion par exemple.

Les **études empiriques** sur la cybercriminalité sont difficiles à réaliser. Qu'elles soient le fait des acteurs de la sécurité, d'observatoires scientifiques ou issues du monde la recherche académique, elles ne font généralement que dresser un état des lieux plus ou moins complet, plus ou moins juste, d'un phénomène mouvant. Par définition, elles surviennent *a posteriori*, après la réalisation des délits, lorsque les impacts de la cybercriminalité sont observables, mesurables et donc préjudiciables. Elles peuvent servir dans les organisations de levier pour une **démarche proactive et préventive** de la lutte contre la cybercriminalité. Cela consiste pour l'essentiel en mesures techniques, procédurales, légales et organisationnelles qui contribuent à augmenter le niveau et le nombre de difficultés pour réaliser des cybercrimes, en augmentant la prise de risques pour les criminels et en diminuant les incitations et les profits attendus.

Lutter contre la cybercriminalité suppose également :

- la mise en place, d'infrastructures et de services ICT **résilients** et **robustes** ;
- la mise à disposition de mesures de sécurité compréhensibles, contrôlables, efficaces et efficientes, facilement implantables, utilisables et maîtrisables par les utilisateurs ;
- une gestion stratégique et opérationnelle de la sécurité informatique (sécurité matérielle, logicielle, applicative, sécurité de l'information, cybersécurité) globale, intégrative et performante ;
- un usage cohérent et non abusif des TIC ;
- un comportement irréprochable et éthique de tous les acteurs de la chaîne numérique (utilisateurs, gestionnaires, fournisseurs).

La lutte contre la cybercriminalité passe par une volonté politique et économique forte, par des partenariats publics/privés, par l'existence et le respect d'accords internationaux, le respect des droits humains fondamentaux, par une collaboration et une entraide internationales, par une prise en compte des besoins de justice, de paix et de stabilité dans le cyberespace et dans la vie réelle.

Résumé

L'adoption universelle des technologies Internet, la dépendance des organisations et des États à ces mêmes technologies et l'interdépendance des infrastructures, introduisent un degré de vulnérabilité non négligeable dans le fonctionnement normal des institutions. La cybercriminalité est devenue un fléau de société qui touche tous les acteurs tant sur un plan national qu'international. Concomitante au cyberespace, elle reflète l'évolution des pratiques criminelles qui ont su s'adapter en tirant parti des technologies de l'information et de la communication. En matière de cybercriminalité, Internet contribue largement à rendre opaque et à masquer les actions relevant de la criminalité, tout en contribuant à rendre invisible leurs auteurs. En effet, la nature transnationale du cybercrime, les capacités du réseau permettant d'agir à distance et caché derrière un écran, de passer par de multiples intermédiaires techniques et infrastructures informatiques et de télécommunication de différents pays, l'anonymisation, la possibilité d'user de fausses identités numériques ou d'identités usurpées, la dimension transnationale de la cybercriminalité rendent difficile l'obtention d'une vue globale et complète de la réalité de la cybercriminalité.

Les dérives et l'insécurité générée par un usage abusif des technologies de l'information, qu'elles soient d'origine criminelle ou non, ne peuvent plus être ignorées. Cette composante doit être prise en compte lors de la conception, de la mise en place, de la gestion et de l'utilisation des solutions de sécurité.

Il est important de sensibiliser l'ensemble des acteurs d'Internet aux enjeux de la maîtrise de la sécurité et de la criminalité et aux mesures élémentaires qui, si elles sont clairement énoncées, définies et mises en œuvre intelligemment, renforceront la confiance des utilisateurs envers le monde numérique et diminueront les opportunités criminelles.

Face à la synergie et à la convergence du crime organisé, du crime économique et du cybercrime, une réponse complète est à apporter pour satisfaire aux besoins de sécurité des infrastructures informationnelles desquelles dépendent la sécurité des personnes, des biens matériels, des valeurs immatérielles et la sécurité publique et nationale.

Comme toute action de sécurité, la lutte contre la cybercriminalité, les cyberabus et les cyberdéfenses est complexe. Elle doit s'inscrire dans une optique de protection des personnes, des biens matériels et immatériels, et défendre les valeurs des sociétés démocratiques. Il convient alors de disposer d'une posture efficace et efficiente de cybersécurité et de cyberdéfense qui respecte les droits fondamentaux. Il ne suffit pas de sensibiliser la population aux dangers d'Internet et aux précautions élémentaires ou de la tenir pour seule responsable d'une situation qu'elle n'a, dans l'écrasante majorité des cas, pas les moyens de maîtriser. En effet, il serait injuste de faire porter par le consommateur final et le citoyen le coût du risque non assumé par les acteurs qui l'ont généré et ainsi de transférer un problème de société sur des personnes qui n'ont pas les moyens d'y faire face seules.

Une approche globale, interdisciplinaire et intégrative de cybersécurité permet de prendre les mesures préventives et réactives appropriées, dont l'efficacité dépendra de leur complétude et de leur cohérence tant au niveau national qu'international.

Exercices

2.1 Pourquoi l'ouverture des systèmes d'information des organisations par les réseaux de télécommunication pose-t-elle des problèmes de sécurité ?

2.2 Qu'est-ce qui a changé avec les attaques réalisées contre des infrastructures informatiques ?

2.3 Qu'est-ce qu'un crime informatique ? Que recouvre le terme de cybercriminalité ? Quelles sont les principales caractéristiques d'un crime informatique ?

2.4 Quelles sont les caractéristiques d'Internet qui peuvent être exploitées à des fins criminelles ?

2.5 Quels sont les événements qui ont contribué à l'évolution de la perception de la menace cybercriminelle ?

2.6 Quels sont les principaux types d'attaques réalisables via Internet ?

2.7 Quels sont les principaux dangers liés à la messagerie électronique en matière de cybercriminalité ?

2.8 Quelles sortes de délits sont favorisées par Internet ?

2.9 Quels sont les facteurs de succès de réalisation d'une attaque ?

2.10 Pourquoi un responsable sécurité a tout avantage à connaître les différentes phases de réalisation d'une attaque informatique ?

2.11 Qu'est-ce que la cybercriminalité ?

2.12 Identifier les principaux facteurs qui contribuent au développement de la cybercriminalité ?

2.13 Comment peut-on expliquer la proximité criminelle sur Internet ?

2.14 Quelles peuvent-être les cibles de cybermenaces ?

2.15 Pourquoi l'interdépendance des infrastructures pose-t-elle un problème de sécurité ?

Solutions

2.1 La mise en réseaux et l'ouverture *via* Internet des systèmes informatiques transforment ces derniers en ressources accessibles à distance et en **cibles** pour des cyberattaques potentielles. Cela accroît leur exposition aux risques (risques d'intrusion, de prise de contrôle à distance, d'infection, etc.). De plus, l'interdépendance des systèmes favorise la propagation des incidents.

2.2 Les attaques à main armée dans une banque, par exemple, ont pour objectif l'obtention d'une marchandise, d'un bien tangible. La sécurité à mettre en place est alors fonction de la valeur à protéger et son coût y est proportionnel.

Les attaques portant sur des valeurs immatérielles (sites web, données, etc.), réalisées à distance, sont plus difficiles à identifier et à contrer. La sécurité qu'il faut mettre en place dépend alors du **contexte** qui est *a priori* hostile et non pas de la **valeur directe** du bien. L'objectif de la sécurité est de permettre une protection par anticipation et de pouvoir réagir aux incidents.

2.3 Avec le **crime informatique**, l'ordinateur peut être la finalité d'un délit (vol de données, destruction, etc.) mais peut également servir d'intermédiaire pour perpétrer des activités délictueuses (délit financier par exemple).

Le **cybercrime** est une forme du crime informatique lié au cyberspace qui fait appel aux technologies Internet pour sa réalisation.

La **cybercriminalité** constitue le prolongement naturel de la criminalité classique. Non seulement Internet offre des conditions exceptionnelles pour de nouvelles entreprises et activités illicites, mais il autorise également la réalisation de fraudes ou de délits habituels. Une exploitation efficace des technologies du numérique permet des crimes économiques classiques avec une prise de risque minimale et une profitabilité maximale.

Le **crime informatique** est un crime lié aux technologies du numérique qui fait partie de la **criminalité en col blanc** et qui constitue un danger réel menaçant l'économie et la vie quotidienne.

Il s'agit d'un crime sophistiqué qui est souvent difficile à détecter, à investiguer, à poursuivre, qui possède le plus souvent des effets secondaires et un caractère international. Il est commis caché derrière un écran et peut être automatisé — ce qui autorise une commission à grande échelle (cyberépidémie).

2.4 Parmi les **caractéristiques d'Internet** qui peuvent être exploitées à des fins criminelles et qui offrent un contexte favorable à la réalisation de la criminalité, citons par exemple :

- la multiplicité des éléments, matériels, logiciels, réseaux et acteurs impliqués ;
- l'inexpérience, l'inconscience, les comportements à risque des utilisateurs ;
- les possibilités d'anonymat ou de pseudo-anonymat ;
- le caractère virtuel, immatériel de certaines opérations (caché derrière un écran et à distance au travers du réseau) ;
- l'existence de vulnérabilités techniques et organisationnelles ;
- la disponibilité sur Internet d'outils d'exploitation des failles, de bibliothèques d'attaques, de logiciels à paramétrier ;
- les capacités à capitaliser et à embarquer le savoir-faire criminel dans un logiciel ;
- la mobilité internationale rapide des données ou des services délictueux ;
- la juridiction multiple dans laquelle s'inscrivent les activités d'Internet, l'existence de paradis digitaux ;
- la nature de la trace informatique (immatérielle), qui est difficile à collecter et à sauvegarder ;
- la disponibilité d'outils de chiffrement, de stéganographie, qui rend confidentielles les communications des criminels.

2.5 Outre le bug de l'an 2000, qui a fait prendre conscience de la fragilité des logiciels et de notre dépendance vis-à-vis de l'informatique, souvenons-nous des attaques de **déni de service** contre des sites tels que Yahoo! (10 février 2000) et du fameux **virus** « *I love you* » (4 mai 2000). Depuis, associé à la médiatisation d'infections virales, de fraudes, d'escroquerie, de vols d'identité, d'informations confidentielles, ou personnelles, le grand public prend plus ou moins conscience de la réalité des menaces s'effectuant à travers Internet.

2.6 Les **attaques passives** n'altèrent pas la cible de l'attaque (écoutes non autorisées, interception de flux sans modification, collecte d'informations à l'insu du propriétaire par exemple), tandis que les **attaques actives** portent atteintes à l'environnement ciblé (perte d'intégrité, de disponibilité, vol, destruction, déni de services, etc.).

On distingue également les attaques fondées sur :

- l'usurpation d'identité, de paramètres de connexion, de mots de passe ;

- le leurre, l'exploitation des vulnérabilités (organisationnelles, humaines, technologiques) ;
- le détournement des technologies (déni de service par exemple) ;
- la manipulation de l'information ou attaque sémantique (défiguration de site web, propagation de fausses informations, manipulation d'opinion, infoguerre, diffusion de contenus illégaux, etc.) ;
- la prise de contrôle à distance des systèmes ;
- la diffusion de programmes malveillants (virus par exemple).

2.7 Le **spamming**, ou pourriel, désigne une communication électronique, non sollicitée par les destinataires, expédiée en masse à des fins publicitaires ou malveillantes. Il s'agit d'un envoi du même message électronique à un très grand nombre de destinataires. Très souvent cela concerne des publicités déloyales de produits pornographiques, de médicaments (produits de « dopage sexuel », hormones utilisées dans la lutte contre le vieillissement, etc.), de crédit financier, par exemple. Avec une augmentation des activités de *e-banking*, la messagerie électronique est devenue un bon moyen pour générer du **phishing**, qui consiste à tromper le destinataire en faisant passer un courriel pour un message de la banque ou d'un quelconque service protégé par mot de passe afin de récupérer les données personnelles de l'utilisateur (paramètres de connexion, numéro de compte, de carte de crédit, etc.).

Le **bombing** est défini comme l'envoi d'une grande quantité de messages à un destinataire unique dans une intention malveillante ». Le *mailbombing* consiste à envoyer de façon massive des courriels à un ou des destinataires.

L'objectif est de :

- saturer le serveur de mails ;
- saturer la bande passante du serveur et du ou des destinataires ;
- rendre impossible aux destinataires de continuer à utiliser l'adresse électronique.

Le **scamming** est un type de leurre pour abuser, mystifier une victime afin de lui faire réaliser des actions illégales. Ainsi, par exemple, un internaute peut se faire piéger et recevoir de l'argent sur son compte provenant soit d'un compte piraté (*via* une technique de phishing) soit d'un chèque (volé voire faux). L'astuce réside dans le fait que la victime effectue un virement vers le criminel (qui s'enrichit) au détriment de l'utilisateur abusé.

La messagerie électronique est un des moyens largement utilisés par le monde criminel pour diffuser des logiciels malveillants (*malware* – virus, chevaux de Troie, vers, logiciels espions, etc.) pour infecter les ressources informatiques, en prendre le contrôle, les modifier ou les détruire.

2.8 Le cyberspace constitue un champ d'action et une source additionnelle d'opportunités en matière de crime. Internet facilite la réalisation des **délits traditionnels** suivants : enrichissement illégitime, blanchiment d'argent, harcèlement,

incitation à la haine raciale, escroqueries diverses, espionnage, diffusion de contenus illicites, etc.

De plus, il a donné lieu à de **nouveaux délits** comme l'intrusion dans des systèmes informatiques, le vol, la détérioration de données numériques, l'utilisation frauduleuse d'un ordinateur, le vol de temps machine, l'obtention frauduleuse d'une prestation, etc.

2.9 Les principaux **facteurs de succès** de réalisation d'une attaque sont liés essentiellement à la connaissance de la cible et de ses vulnérabilités (récolte d'information sur la cible, *scan* des ports de communication, détection des failles, etc.), à la capacité de rendre l'attaque non détectable, à la capacité de ne pas laisser de traces et à la célérité de réalisation de l'attaque.

2.10 La mission principale du **responsable de la sécurité** est la protection des actifs. Protéger les actifs comprend entre autres la maîtrise de l'environnement pour qu'une attaque n'aboutisse pas. L'attaquant potentiel est rationnel, il va utiliser la manière la plus facile et la plus efficace pour atteindre sa cible. Pour diminuer la probabilité que le risque d'attaque se réalise, le responsable sécurité doit connaître la manière dont l'attaquant va se comporter et la démarche utilisée pour mener l'attaque. Il a tout intérêt, s'il a su détecter une attaque, à en connaître la phase afin d'activer les mesures de protection et de réaction nécessaires pour la contrer le plus efficacement possible ou en limiter les impacts.

2.11 La **cybercriminalité** se définit comme étant toute activité criminelle contraire à la loi, réalisée à travers le cyberspace, *via* le réseau Internet. Par extension, cela intègre toute forme de malveillance électronique effectuée à l'aide des technologies informatique et de télécommunication (téléphonie, cartes à puce, etc.). La criminalité classique étend son emprise sur Internet par une large gamme de forfaits (cyberescroquerie, cyberfraude, cyberextorsion, cyberabus, cyberespionnage, cybervandalisme, cyberconflit, cyberharcèlement...) qui traduisent l'apparition de comportements délinquants ou malveillants tirant parti de l'existence et des caractéristiques d'Internet.

2.12 Les technologies de traitement de l'information et de la communication (TIC) sont devenues des cibles de la malveillance (vol d'ordinateurs, de données, prise en otage de ressources informatiques...) et/ou des moyens pour commettre des actions illicites (chantage, détournement, blanchiment d'argent...). Le réseau Internet fait désormais partie des outils de performance et de réalisation de toute **stratégie criminelle**. Il facilite la réalisation de délits classiques, notamment ceux relevant de la criminalité économique, et permet de nouvelles formes d'expression de la criminalité (fraude informatique, piratage de logiciels...). La dématérialisation des services et des transactions, les outils de mise en relation et de communication, la capacité d'agir à distance et caché derrière un écran, le fait de pouvoir utiliser de fausses identités ou des identités usurpées, de passer par un grand nombre d'intermédiaires techniques (serveurs, fournisseurs d'accès...) et de pays différents, autorisent des formes d'organisation, d'échanges et d'activités criminelles très profitables.

au regard de l'investissement nécessaire et de la prise de risque, qui restent faibles par rapport aux gains générés par des actions cybercriminelles.

2.13 Internet et la téléphonie mobile ont créé un nouveau paradigme de communication qui peut se résumer par « *communiquer partout, n'importe quand voire tout le temps, avec n'importe qui* ». Ce n'importe qui est relatif aux enfants, aux personnes âgées ou à M. et M^{me} Tout-le-Monde, et également aux acteurs malveillants de toute sorte (pédophiles, terroristes, criminels, délinquants, professionnels de l'arnaque, etc.). Cela expose chaque personne physique ou morale, présente sur Internet, à une cyberproximité criminelle potentielle, mais bien réelle. Le réseau des réseaux peut dès lors être considéré comme étant une zone criminalisée où les individus comme les institutions privées et publiques, de par leur présence sur Internet, contribuent à l'extension de la criminalité sur Internet. Désormais, le risque informatique d'origine criminelle est un risque structurel, omniprésent et permanent.

2.14 Les infrastructures informatiques et télécoms sont des ressources stratégiques de grande importance tant pour les individus que pour les organisations ou les Etats. Tout en constituant la cible de **cybermenaces** qui pourraient les affecter dans leur disponibilité, leur intégrité ou leur confidentialité, elles peuvent également être un instrument de manipulation d'opinion, (endoctrinement, diffusion de rumeurs...), un instrument au service du renseignement, de l'espionnage, de la surveillance, du contrôle social, ou encore celui de déstabilisation économique et étatique. Ainsi, Internet est certes un fabuleux outil de communication, il doit néanmoins aussi être considéré comme un outil de pouvoir et une arme de guerre qui contribue à la guerre de l'information, par l'information, pour l'information et parfois contre l'information !

2.15 Les infrastructures informatiques sont largement distribuées, interconnectées et interdépendantes, mais sont également dépendantes d'infrastructures énergétiques (électricité, climatisation). Leurs caractéristiques, leurs limites, comme l'existence de failles dans leur conception, leur implantation, leur gestion ou leur utilisation sont exploitées par les criminels. Néanmoins, tous les incidents liés à un défaut de sécurité informatique ne sont pas intentionnels et ne relèvent pas forcément de la criminalité mais peuvent parfois être imputés à l'incompétence, à des erreurs ou à la survenue d'événements naturels comme une inondation par exemple.

GOUVERNANCE ET STRATÉGIE DE SÉCURITÉ

3

PLAN

- 3.1 Gouverner la sécurité
- 3.2 Gérer le risque informationnel
- 3.3 Connaître les risques pour les maîtriser
- 3.4 Vision stratégique de la sécurité
- 3.5 Définir une stratégie de sécurité
- 3.6 Organiser et diriger
- 3.7 Prise en compte des besoins juridiques
- 3.8 Principes d'intelligence économique
- 3.9 Prise en compte des risques cachés

OBJECTIFS

- Comprendre les notions de gouvernance et de stratégie de la sécurité.
- Posséder les fondamentaux de la maîtrise des risques et les principes généraux de la stratégie.
- Découvrir les métiers, les responsabilités et les compétences relevant de la sécurité.
- Appréhender les dimensions organisationnelle, économique, légale et réglementaire.
- Développer une vision de l'intelligence économique.
- Considérer la cybersécurité au service des droits fondamentaux et des libertés civiles.
- Penser la sécurité en termes de cyberrésilience et de cyberdéfense.

3.1 GOUVERNER LA SÉCURITÉ

3.1.1 Contexte

La sécurité ne doit pas être une juxtaposition de technologies mais doit être appréhendée et traitée comme un **processus continu**. La vision « processus » met en avant la **dimension managériale** de la sécurité, qui vise à l'optimisation et à la rationalisation des investissements tout en assurant la pérennité et l'efficacité des solutions de sécurité dans le temps.

L'importance d'une gestion rigoureuse de la sécurité des systèmes d'information, de son appréhension globale et intégrée, est reflétée par la notion de **gouvernance de la sécurité**.

La gouvernance de la sécurité traduit la volonté de diriger et de piloter la sécurité afin de dominer les risques liés au numérique. Cette connotation au pouvoir politique positionne le problème de la sécurité des systèmes d'information au plus haut niveau stratégique des organisations et sous-entend une mise en œuvre opérationnelle répondant à une vision politique.

La dépendance accrue des processus métiers envers les technologies de l'information et de la communication implique, entre autres, que la **stratégie de sécurité** corresponde à la stratégie de l'entreprise afin que cette dernière la supporte. Ainsi, la gouvernance de la sécurité de l'information fait partie de la gouvernance d'entreprise, système par lequel les organisations sont dirigées, contrôlées et évaluées. La gouvernance de la sécurité de l'information peut être vue comme un **processus** pour établir et maintenir un cadre supportant la structure de gestion qui permet de réaliser la stratégie de sécurité et de s'assurer que les objectifs stratégiques de sécurité sont alignés avec ceux du *business*. Il s'agit d'assurer la protection des actifs informationnels contre les risques d'indisponibilité (perte, vol, erreur, accident), d'usage abusif ou détourné, de divulgation ou de modification non autorisée, ou encore de maîtriser les risques juridiques liés à la responsabilité légale des acteurs et aux contraintes réglementaires (protection des données personnelles par exemple).

Il est parfois possible de distinguer la gouvernance de la sécurité de l'information de celle des technologies de l'information. La gouvernance de la sécurité de l'information reflète les exigences de sécurité au regard des besoins business et stratégique (niveau exécutif et vision managériale) et s'appuie sur la sécurité des technologies qui l'appréhendent (vision technologique et opérationnelle). En pratique, ces deux dimensions de la gouvernance sont le plus souvent associées du fait de leur nécessaire complémentarité et cohérence pour offrir le niveau de sécurité requis.

La gouvernance de la sécurité vise à s'assurer que les mesures stratégiques et opérationnelles de la sécurité sont optimales et proportionnelles aux risques encourus. Elle permet de pouvoir répondre de manière précise aux questions simples : Qui fait quoi ? Comment et quand ? Cela se décline, en particulier, par l'identification des acteurs qui élaborent, qui définissent, qui valident, qui mettent en œuvre, qui contrôlent, qui utilisent les mesures de sécurité.

3.1.2 Principes de base de la gouvernance de la sécurité de l'information

La mise en place d'un système gouvernant la sécurité de l'information presuppose l'existence des éléments suivants :

- des stratégies d'affaires et sécuritaires ;
- une politique de gestion des risques ;
- une politique de sécurité ;
- une structure organisationnelle de la sécurité ;

- des compétences ;
- des processus formels de surveillance (*monitoring*), de contrôle et d'évaluation de la sécurité (audit).

Puisque la gouvernance est une activité qui implique la **gestion** et le **contrôle** (évaluation de la satisfaction des objectifs stratégiques), la fonction de gouvernance doit être située au niveau le plus haut de la direction de l'entreprise. Impliquer les hautes instances donne de la crédibilité à la démarche de gouvernance et va ainsi la rendre plus efficace.

Un comité de direction réunit tous les responsables concernés par des besoins spécifiques de sécurité dans leurs tâches quotidiennes et leurs métiers. Leurs retours d'expérience aident à la définition correcte des exigences afin que l'implémentation de la sécurité puisse répondre au mieux à leurs besoins. Le comité de direction est un canal de communication privilégié promouvant une culture de sécurité proche des utilisateurs finaux.

Le responsable de la sécurité de l'information réalise l'implémentation opérationnelle de la sécurité qui découle des stratégies et objectifs exprimés par les instances supérieures.

Les principes généraux d'une démarche de gouvernance de la sécurité peuvent s'articuler autour des mots clés suivants :

1. **Responsabilité** – Chaque instance assurant la gouvernance doit être responsable de la tâche qui lui incombe.
2. **Proportionnalité** – Les investissements doivent être proportionnels au risque informationnel encouru par l'entreprise.
3. **Conscience** – Les instances directrices sont conscientes du rôle et de l'importance des actifs informationnels de l'entreprise et, par conséquent, du rôle et des besoins de sécurité.
4. **Conformité** – Les stratégies et les mesures sécuritaires doivent être conçues, mises en place et gérées en conformité avec les exigences légales et réglementaires.
5. **Efficacité et efficience** – Les mesures répondent aux exigences de sécurité de manière optimale et satisfaisante y compris sur le plan financier.
6. **Inclusion** – Les exigences de toutes les parties intéressées par la démarche (*stakeholders*) doivent être prises en considération.
7. **Transparence** – Le devoir d'informer les parties intéressées sur l'état courant de la sécurité incombe aux instances directrices.
8. **Éthique** – La démarche de sécurité doit respecter les valeurs d'éthique communément admises, en particulier les droits humains fondamentaux.
9. **Équité** – Les instances directrices implantent les solutions sécuritaires basées sur la perception et les règles démocratiques telles que perçues dans l'environnement où l'entreprise agit.
10. **Suivi** – Des évaluations doivent être réalisées périodiquement afin de s'assurer de la pertinence des réponses apportées au regard de l'évolution des risques.

11. **Gestion du risque** – Les instances directrices s’assurent que le processus d’appréciation des risques se fait d’une manière continue et formalisée et est en cohérence avec la gestion de la sécurité.
12. **Culture de la sécurité** – Une culture de la sécurité doit être développée afin que tous les acteurs développent des comportements cohérents et soient acteurs de la sécurité.

3.2 GÉRER LE RISQUE INFORMATIONNEL

3.2.1 Définitions

Un **risque** est un danger éventuel plus ou moins prévisible. Il se mesure à la probabilité qu'il se produise et aux impacts et dommages consécutifs à sa réalisation. Deux notions interviennent dans la variable de risque : celle de menace, qui est la cause potentielle d'un incident indésirable, et celle de vulnérabilité.

Un risque exprime la probabilité qu'une valeur soit perdue en fonction d'une **vulnérabilité** liée à une **menace**, à un danger ou à événement non sollicité.

$$\text{Risque} = (\text{vulnérabilité}, \text{menace}, \text{impact})$$

La terminologie associée au risque distingue l’analyse, l’évaluation, l’appréciation et le traitement de la gestion du risque, à savoir :

- **Analyse du risque** – Utilisation systématique d’informations pour identifier les facteurs de risque afin de pouvoir estimer ce dernier.
- **Évaluation du risque** – Processus de comparaison du risque estimé avec des critères de risque donnés pour déterminer l’importance du risque.
- **Appréciation du risque** – Ensemble des processus d’analyse et d’évaluation du risque.
- **Traitement du risque** – Processus de sélection et de mise en œuvre des mesures visant à modifier le risque.
- **Gestion du risque** – Activités coordonnées visant à diriger et à piloter une organisation vis-à-vis des risques et à maintenir les risques sous contrôle.

3.2.2 Principes de gestion

Les éléments constitutifs d’une **démarche de gestion** du risque informationnel sont :

- identification et classification des actifs ;
- évaluation des vulnérabilités liées aux actifs à protéger ;
- appréciation des menaces (origine, finalité, capacité à se réaliser, identification des facteurs inhibiteurs, amplificateurs ou catalyseurs des menaces) ;
- appréciation du risque et représentation par une matrice des probabilités et des impacts ;
- définition des contre-mesures (mesures procédurales, techniques, humaines).

3.2.3 Projet d'entreprise orienté vers la gestion des risques

La démarche sécurité est un **projet d'entreprise** dans la mesure où chacun est concerné par sa réalisation. Sa validité sera renforcée si l'organisation développe une **culture sécuritaire** et si elle stipule ses exigences de sécurité envers ses acteurs internes et ses partenaires externes.

La prise en compte de l'analyse des risques liés au système d'information dans un processus de gestion de risques globaux (*risk management*) guide toute la démarche de sécurité d'une organisation.

Le risque informatique, informationnel, ou lié au cyberspace (notion de **cyber-risque**) quel que soit le nom retenu, doit être identifié au même titre que tous les autres risques de l'organisation (risques financiers, métier, social, environnemental, etc.) auxquels doit faire face une organisation. Le risque informatique est un **risque opérationnel, un risque structurel et permanent** qui doit être maîtrisé.

Au-delà de l'analyse des risques opérationnels, les institutions doivent également s'assurer qu'elles respectent les réglementations, qu'elles satisfont aux exigences sécuritaires de leurs divers partenaires et qu'elles maîtrisent les risques réglementaires, organisationnels et stratégiques.

3.3 CONNAÎTRE LES RISQUES POUR LES MAÎTRISER

Pour une organisation, l'objet de sa sécurité est de contribuer à préserver ses valeurs, ses forces et ses moyens organisationnels, humains, financiers, technologiques et informationnels, dont elle s'est dotée pour réaliser ses objectifs. La sécurité de l'information, des processus et des systèmes est désormais un facteur de **productivité** et de **compétitivité** des organisations.



L'Organisation internationale de standardisation a défini une norme, l'ISO 27005, largement acceptée comme guide pour améliorer l'appréhension et la gestion des risques.

La finalité de la sécurité informatique est de contrecarrer les incidents, les erreurs ou les malveillances qui pourraient mettre en péril la **pérennité** d'une organisation, limiter sa productivité ou restreindre sa compétitivité. Cela consiste à diminuer la probabilité de voir des menaces se concrétiser, à limiter les atteintes ou dysfonctionnements induits, et à autoriser le retour à un fonctionnement normal à des coûts et dans des délais acceptables en cas de sinistre (figure 3.1).

Une **stratégie de sécurité** consiste donc à concevoir une conduite générale de protection, de prévention, d'organisation de la défense, d'élaboration de plans de réaction, de gestion de crises, de gestion de la continuité et de la reprise des activités, de gestion des poursuites pénales s'il y a lieu. Cela s'inscrit dans une **démarche proactive et réactive** qui permet d'anticiper et d'être préparé à prévenir et à gérer les incidents de sécurité.

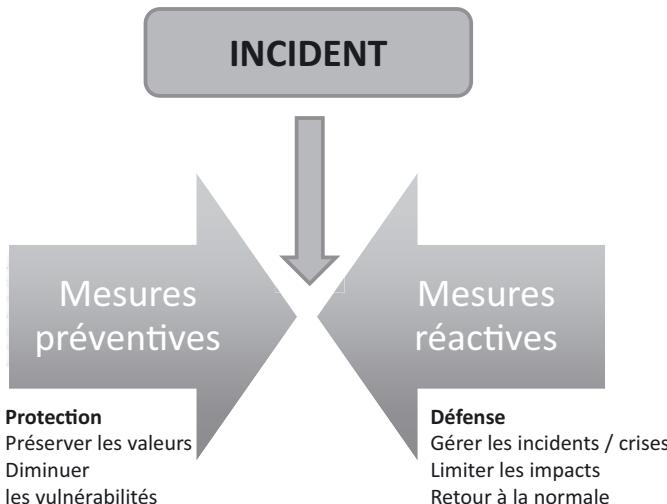


Figure 3.1 – Objectifs de la sécurité.



Pour une organisation, la maîtrise des risques informatiques consiste à les réduire à un niveau acceptable, voire assurable. La frontière entre le risque acceptable et celui qui ne l'est pas est parfois difficile à déterminer objectivement et dépend fortement des objectifs de l'organisation et du contexte dans lequel elle évolue. Les risques sont alors acceptés parce que connus et n'impactant pas de façon grave l'information et les systèmes qui la traitent.

Pour une organisation, la maîtrise des risques informatiques passe par la conception d'une stratégie, la définition d'une politique de sécurité et de sa réalisation opérationnelle. Certaines organisations peuvent également identifier un **plan d'action sécurité** qui constitue une **feuille de route** facilitant la mise en œuvre des mesures.

Une **démarche sécuritaire** est constituée de trois phases principales (figure 3.2).

La première étape (1) consiste à **identifier les valeurs** à protéger, et à faire **une analyse des risques** encourus en fonction notamment du niveau de vulnérabilité de ces valeurs et des menaces potentielles dont elles peuvent être la cible, afin de connaître les impacts consécutifs à leur perte totale ou partielle et de déterminer le niveau de gravité de ces pertes. C'est à l'organisation de décider du nombre de niveaux, de leur signification et de la catégorisation de ses risques (faible, important, grave, majeur par exemple). À chaque niveau de risque et critère de gravité, on devrait pourvoir associer un niveau d'occurrence (rare, vraisemblable, fort, maximal) afin d'obtenir une **matrice de criticité du risque** et de déterminer quels sont les risques à couvrir en priorité. À l'issue de cette analyse des risques, une vision de ce qui doit être protégé, contre qui et pourquoi, peut alors être formulée en fonction des priorités de sécurisation.

Il s'agit de définir une stratégie de protection et de gestion de la sécurité en fonction des besoins de sécurité, des valeurs et des menaces identifiées qu'encourent

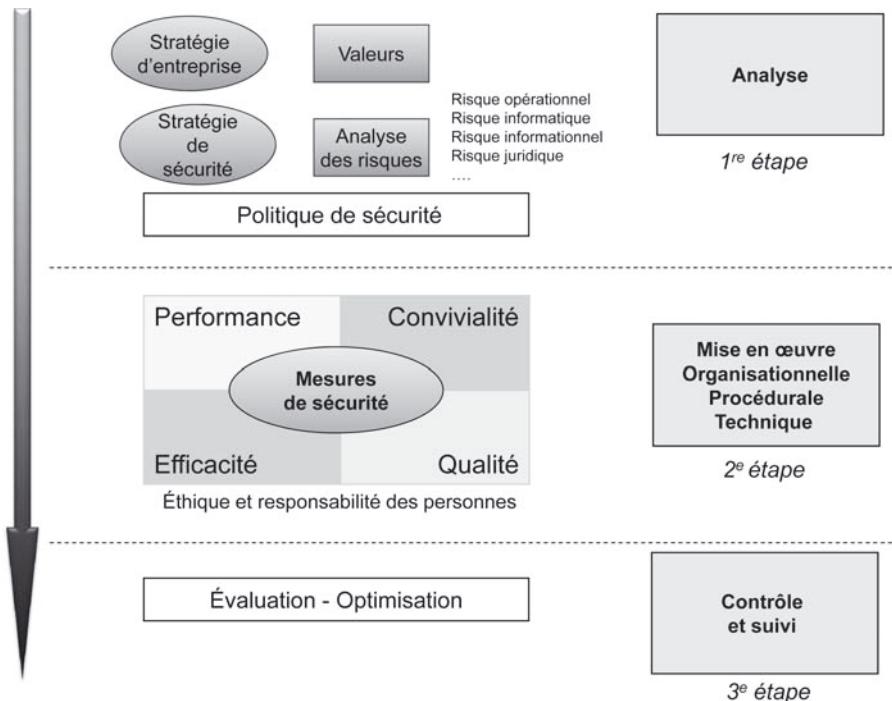


Figure 3.2 - Étapes de réalisation d'une démarche sécuritaire.

l'organisation. Cette stratégie fait l'objet d'un document général qu'est la politique de sécurité : véritable référentiel permettant de mettre en place un programme, une démarche de sécurité cohérente au sein de l'organisation.

De la pertinence de l'analyse des risques dépendra l'**identification** correcte des **exigences de sécurité**, des **moyens** à dégager et des **mesures** à mettre en œuvre pour sécuriser efficacement les ressources.

L'étape suivante (2) consiste à choisir puis à **mettre en place les mesures organisationnelles, techniques et procédurales** nécessaires à la gestion des risques et à la sécurité des systèmes, services et données.

L'optimisation de la démarche sécuritaire passe par la validation de :

- la pertinence de la vision stratégique de la sécurité ;
- la qualité de la politique de sécurité pour satisfaire aux impératifs de la maîtrise des risques ;
- l'adéquation des solutions de sécurité aux besoins en fonction des moyens financiers et humains à disposition ;
- la **cohérence** des mesures les unes par rapport aux autres dans le cadre d'une approche globale ;
- la capacité à gérer correctement la sécurité ;
- l'**intégrité des personnes** en charge de la sécurité.

Une **évaluation périodique** (étape 3) voire constante des mesures (outils et procédures) de sécurité en vue de leur **optimisation** et de leur **rationalisation** permet de répondre au mieux à l'évolution de l'environnement dans lequel ces mesures s'inscrivent.

Élaborer une stratégie de sécurité consiste à effectuer le **compromis** le plus judicieux possible entre le coût des mesures de sécurité à supporter pour pallier les risques qui pourraient affecter une organisation, et le coût des impacts de la concrétisation de ces risques s'il n'y avait pas de mesures (gestion de l'incertain).

Il n'existe pas de stratégie prédéterminée ou unique, ni de recette pour définir une stratégie. Chaque contexte d'organisation, d'environnement informationnel, de scénario de risques est particulier et évolutif. On ne peut définir de règles générales qui déterminent quelles sont les stratégies ou solutions de sécurité à planter pour maîtriser un risque donné. En revanche, il existe des invariants méthodologiques qui facilitent l'appréhension d'une démarche sécuritaire.

Une entreprise peut ainsi renoncer à mettre en œuvre un dispositif de secours (*back-up*) de son centre informatique au regard de son coût. En effet, ce coût peut s'avérer très élevé en termes de ressources et de procédures à utiliser si l'on tient compte :

- de la probabilité du risque de destruction physique totale des infrastructures ;
- du coût des mesures de surveillance et de détection (d'incendie, d'inondation, d'intrusion, etc.) ;
- de partitionnement des salles machines ignifugées à deux heures garanties, sur lesquelles sont réparties les applications critiques ;
- du fait que le **risque résiduel** est le plus souvent jugé comme acceptable par la direction générale.

La figure 3.3 résume les liens entre une vision stratégique des risques et un plan d'action de sécurité.

3.4 VISION STRATÉGIQUE DE LA SÉCURITÉ

3.4.1 Fondamentaux

Les solutions de la sécurité informatique et des télécommunications doivent permettre d'assurer tout ou partie des propriétés suivantes, qui ont valeur de critères de sécurité à satisfaire pour chaque ressource à sécuriser :

- la **disponibilité** (aucun retard) : maintien de l'accessibilité en continu sans interruption ni dégradation ;
- l'**intégrité** et l'**exactitude** (aucune falsification, aucune erreur) : maintien intégral et sans altération des données et des programmes (véracité des contenus) ;
- la **confidentialité** (aucune écoute illicite) : maintien du secret de l'information et accès aux seules entités autorisées.
- la **pérennité** (aucune destruction) : les ressources existent, elles sont conservées le temps nécessaire ;

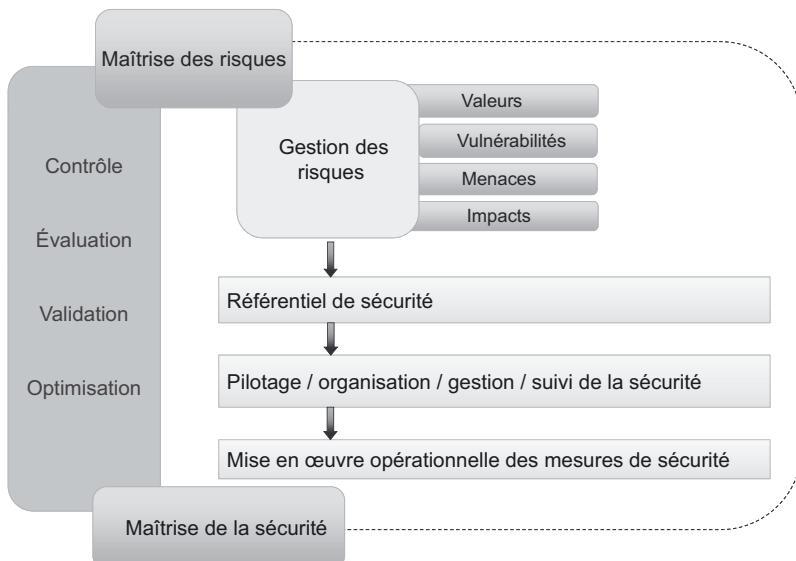


Figure 3.3 – Risques et plan d'action de sécurité.

- la **non-répudiation** et l'**imputabilité** (aucune contestation) : garantie de l'origine, de la source, de la destination, de la véracité d'une action et identification des entités responsables ;
- l'**authentification** (aucun doute sur l'identité d'une ressource, sur l'origine ou la destination d'une transaction) ;
- le respect de l'**intimité numérique** (*privacy*, aucune mise à défaut de la protection de la sphère privée de l'utilisateur, protection des données personnelles) et le respect des **contraintes légales** ou réglementaires (aucun risque juridique).

Pour réaliser ces propriétés, des mesures organisationnelles, techniques, managériales et humaines doivent exister, être opérationnelles, validées et contrôlées. Pour cela, il faut connaître les valeurs à protéger et exprimer leur besoin en termes de critères de sécurité afin de permettre d'identifier l'ensemble des mesures de sécurité à mettre en œuvre au travers, par exemple :

- d'outils technologiques comme des pare-feu, des protocoles cryptographiques, des antivirus, etc. ;
- de procédures (gestion des identifications et des habilitations, mises à jour d'antivirus, surveillance...) ;
- de personnes (recrutement, sensibilisation, formation...).

Les mesures de sécurité sont déterminées, gérées et optimisées par des **procédures de gestion**.



Au-delà de la nécessaire dimension d'ingénierie de la sécurité, la sécurité relève avant tout d'un acte de management (dimension managériale). La qualité de la sécurité dépend le plus souvent de la qualité de sa gestion et des personnes qui en sont responsables.

Réduire la sécurité à sa dimension technologique, c'est assurer son échec. Par ailleurs, se retrancher derrière des règles de sécurité prédéterminées, des réglementations ou des produits « leaders » du marché, sans valider leur adéquation aux besoins de l'organisation, peut mettre en péril la mission de sécurité.

3.4.2 Mission de sécurité

Chaque organisation doit spécifier sa propre **mission de sécurité** pour réaliser sa stratégie de sécurité telle que définie en accord avec la direction générale. Les activités d'une mission de sécurité peuvent se décliner de la manière suivante :

- effectuer une appréciation des risques ;
- concevoir une stratégie, une politique et un plan d'action de sécurité ;
- aligner les besoins de sécurité avec les risques et les coûts ;
- définir le périmètre de vulnérabilité des ressources ;
- offrir de manière continue un niveau de protection adapté aux risques encourus ;
- mettre en œuvre et valider l'organisation, les mesures, les outils et les procédures de sécurité ;
- effectuer un suivi, contrôler et faire évoluer les mesures stratégiques et opérationnelles ;
- optimiser la performance du système d'information en fonction du niveau de sécurité requis.

3.4.3 Principes de base

La mise en place d'une démarche sécurité repose sur des principes de base qui, s'ils sont adoptés par l'ensemble de l'organisation, facilitent la mise en place et la gestion de la sécurité. Il s'agit des principes de base suivants :

- **Principe de vocabulaire** — Nécessité de s'accorder, au niveau de l'entreprise, sur un langage commun de définition de la sécurité.
- **Principe de volonté directoriale** — Ce principe résulte directement de la considération de l'information comme ressource stratégique de l'entreprise. Il est de la responsabilité de ses dirigeants de libérer les moyens nécessaires à la mise en œuvre et à la gestion de la sécurité informatique.
- **Principe financier** — Le coût de la sécurité doit être en rapport avec les risques encourus. Le budget consacré à la sécurité doit être cohérent vis-à-vis des objectifs de sécurité fixés (notion d'**efficience**).
- **Principe de cohérence** — Une accumulation d'outils sécuritaires n'est pas suffisante pour réaliser un niveau global, cohérent et satisfaisant de sécurité.
- **Principe de séparation des pouvoirs** — Afin de ne pas concentrer les pouvoirs sur une seule entité et de minimiser le risque d'abus.
- **Principe de simplicité et d'universalité** — Les mesures de sécurité doivent être simples, compréhensibles pour les utilisateurs et doivent s'appliquer à l'ensemble du personnel.
- **Principe de précaution** — Ne pas se mettre en situation dangereuse.

- **Principe de dynamicité** — La sécurité doit être dynamique pour intégrer la dimension temporelle de la vie des systèmes et l'évolution des besoins et des risques.
- **Principe de *continuum*** — L'organisation doit continuer à fonctionner même après la survenue d'un sinistre. Pour cela, il faut disposer de procédures de gestion de crise, d'urgence, de reprise et de retour à la normale.
- **Principe d'évaluation, de contrôle et d'adaptation** — Il est impératif de pouvoir évaluer régulièrement l'adéquation des mesures de sécurité au regard des besoins effectifs et évolutifs de la sécurité (notion d'**efficacité**). Cela permet de contrôler et de vérifier que les risques sont maîtrisés de manière optimale dans un environnement dynamique, et d'adapter si nécessaire les solutions de sécurité. Des outils de type « tableau de bord de la sécurité » favorisent le suivi de la sécurité en offrant une meilleure appréciation de la variabilité des critères de sécurité. L'adéquation du niveau de sécurité par rapport aux besoins de sécurité de l'entreprise, qui sont par nature évolutifs, est un souci constant du responsable sécurité.

3.4.4 Conditions de succès

Les **conditions de succès** de la réalisation d'une démarche sécuritaire sont :

- une volonté directoriale, déjà inscrite comme un des principes fondamentaux de la sécurité ;
- une vision stratégique de la sécurité ;
- une politique de sécurité, reflétant la stratégie de sécurité de l'organisation, simple, juste, précise, compréhensible et applicable ;
- la publication de la politique de sécurité ;
- une gestion centralisée de la sécurité et une certaine automatisation des processus de sécurité ;
- un niveau de confiance déterminé envers les personnes, systèmes, outils impliqués ;
- du personnel compétent, sensibilisé et formé à la sécurité et possédant une haute valeur morale ;
- une certaine éthique des acteurs qui adhèrent à une **charte de sécurité** ;
- des procédures d'enregistrement, de surveillance et d'audit ;
- la volonté d'éviter de mettre les ressources, les valeurs (systèmes, réseaux et données) en situation dangereuse ;
- l'expression, le contrôle et le respect des clauses de sécurité dans les différents contrats ;
- le respect des contraintes légales.

L'**efficacité** des mesures de sécurité d'un système d'information ne repose pas uniquement sur les outils de sécurité, ni sur le budget investi. La performance de la sécurité, qui peut se mesurer par le nombre d'incidents survenus et maîtrisés, dépend de :

- la qualité de la stratégie de sécurité ;

- la spécification et la réalisation de la politique de sécurité qui en découle ;
- l'organisation mise en place et les moyens dégagés pour la réaliser ;
- la qualité de la gestion des incidents (détection, réaction) ;
- la capacité d'évaluation et d'évolution de la sécurité en fonction des besoins.

Cela nécessite une structure de gestion adéquate, des procédures bien définies et des personnes compétentes, pour concevoir la stratégie, définir une politique de sécurité, gérer, spécifier, mettre en œuvre et faire vivre des procédures et des mesures cohérentes.

La stratégie relève de la **direction générale**. Il faut donc comprendre que les prérogatives de la **structure organisationnelle** s'inscrivent dans un degré de délégation appropriée.

Cette structure détermine en outre le comportement, les priviléges et les responsabilités de chacun. Elle contribue à faire comprendre à l'ensemble des acteurs de l'organisation l'importance de la sécurité et du respect des règles de sécurité. Elle spécifie — en fonction de facteurs critiques de succès qui permettent d'atteindre les objectifs de l'entreprise — les mesures et les directives sécuritaires appropriées. Ces dernières doivent être rationnelles par rapport aux plans d'entreprise et d'information. Disposer d'une vision stratégique de la sécurité globale de l'organisation est donc primordial à la réalisation de la sécurité.



La sécurité d'un système d'information résulte de l'intégration harmonieuse des outils, mécanismes et procédures liés à la prévention, à la détection, à la protection et à la correction des problèmes relatifs à des fautes, à de la malveillance ou à des catastrophes naturelles.

3.4.5 Approche pragmatique

L'aspect multidimensionnel de la sécurité ne peut s'appréhender que d'une manière globale. À partir des directives générales de la stratégie de sécurité spécifiées par une politique de sécurité (**axe stratégique**), on décline les mesures (**axe tactique**) et on identifie les solutions (**axe opérationnel**) à mettre en œuvre en fonction du contexte d'utilisation des technologies et de leur nature (figure 3.4).



Seule une **approche pragmatique**, inscrite dans une démarche qualité qui définit précisément des objectifs de sécurité cohérents ainsi que des moyens concrets pour les atteindre, permet de sécuriser rationnellement des environnements.

3.4.6 Bénéfices

La sécurité informatique, si elle est bien appréhendée, doit être un facteur d'amélioration des processus métiers de l'entreprise, d'accroissement des performances et de la productivité globale d'une organisation quelle que soit sa taille. Elle est à considérer comme un **facteur critique de succès** et de **productivité**. La sécurité informatique ne doit plus être appréhendée comme une source de coût ni comme un frein à la réalisation de la stratégie d'entreprise, mais comme un levier de sa performance.

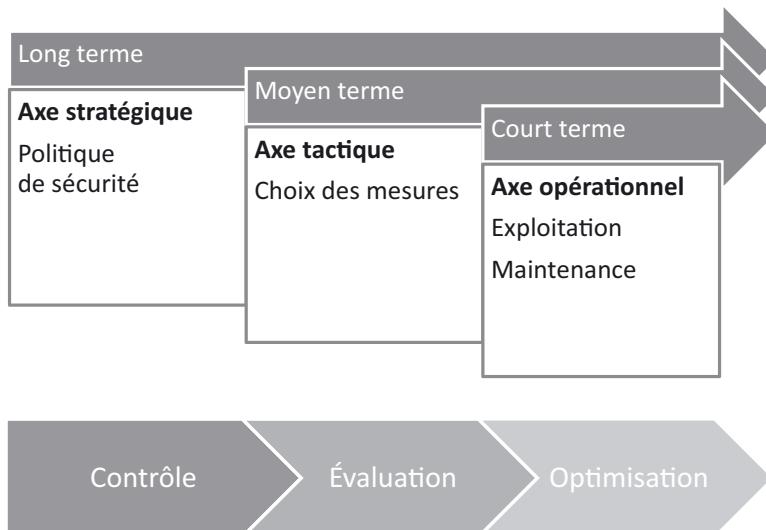


Figure 3.4 - Axes stratégique, tactique et opérationnel de la sécurité.

Ne pas être au même niveau d'insécurité que ses concurrents permet de ne pas être une cible privilégiée de la cybercriminalité, qui, de manière rationnelle, s'attaque aux acteurs les plus faibles.



La sécurité informatique ne doit plus être perçue comme une contrainte supplémentaire à intégrer dans la stratégie des organisations, mais elle doit constituer un **outil de production** qui fait partie des éléments fondamentaux de la stratégie de toutes les organisations et un élément de différenciation.

Comme la qualité, la sécurité est, pour une entreprise, un **facteur de compétitivité** contribuant à une meilleure rentabilité. La sécurité est un **facteur de qualité** qui pose, comme la qualité d'ailleurs, le problème de sa mesure et donc de la détermination des indicateurs et métriques associés. En effet, il est difficile de quantifier les apports directs et indirects d'une bonne maîtrise des risques du fait de l'intangibilité des économies réalisées. En fait, la sécurité permet aussi d'instaurer la confiance (confiance des employés, des clients et des administrés).

3.4.7 Aspects économiques

La mise en place d'un niveau de sécurité particulier est fonction du contexte et des besoins, qui eux-mêmes dépendent :

- des valeurs, de leur degré d'exposition aux risques ;
- du niveau de vulnérabilité des ressources lié à l'existence de failles organisationnelles, procédurales, techniques ou humaines ;
- des impératifs réglementaires et des exigences de sécurité.



Il est important de pouvoir déterminer le **coût de la sécurité** en regard des coûts engendrés par les conséquences directes ou indirectes de la perte de valeurs suite à des accidents, à des erreurs ou à de la malveillance.

Les questions « *Que peut rapporter la sécurité pour l'organisation qui la met en œuvre ? Comment exprimer la rentabilité de la sécurité ?* » suscitent d'autres interrogations, comme par exemple :

- Quelle est la valeur économique de la sécurité ?
- Quel est le retour sur investissement de la sécurité ?

Les réponses à ces questions sont difficiles à formuler et dépendent de la possibilité de quantifier la valeur des actifs informationnels et le coût des impacts et des préjudices consécutifs à la survenue d'un sinistre. Or il est extrêmement difficile d'estimer correctement l'exposition de l'organisation à tous les risques, notamment aux risques sériels dus à l'interconnexion avec des infrastructures tierces. De plus, il est parfois complexe d'évaluer précisément les coûts notamment ceux, indirects, résultant d'une perte d'image, de confiance ou de l'espionnage par exemple.

S'il peut paraître relativement aisé d'estimer ce que coûte la sécurité (budgets associés, rémunération du responsable sécurité et de son équipe, coût des produits de sécurité, des formations, de la veille technologique en matière de sécurité, etc.), il est plus délicat d'évaluer la rentabilité de la sécurité. De manière subjective, on peut penser que les mesures de sécurité possèdent intrinsèquement une **efficacité « passive »** et évitent certaines pertes à l'entreprise.

 La sécurité ne permet pas directement de gagner de l'argent, mais d'éviter d'en perdre !

Le **rapport coût/bénéfice** est ardu à établir car il n'existe pas de critère objectivement mesurable du rendement du capital investi et du retour sur investissement en sécurité. Les approches mathématiques quantitatives sont le plus souvent réservées aux outils de sécurité alors que les approches normatives qualitatives correspondent mieux à l'évaluation du coût d'une politique de sécurité.

Relativiser la notion de retour sur investissement passe par l'appréhension de la stratégie sécuritaire comme un élément de la stratégie globale de l'entreprise. De plus, si la stratégie de sécurité n'est pas disproportionnée et est cohérente par rapport aux risques réels, la nécessité de démontrer le retour sur investissement est moins importante.

Lorsque cela est nécessaire, la prise en considération, par exemple, des coûts suivants contribue à estimer de manière approximative le **retour sur investissement** de la sécurité :

- pertes, baisses de productivité consécutives aux dysfonctionnements et à l'indisponibilité, pertes de parts de marché, pénalités de retard, etc. ;
- coûts induits par des pertes d'image, impacts au niveau des clients, partenaires, sous-traitants, fournisseurs, etc. ;
- coûts de gestion, d'assurance, d'investigation, salaires des experts, etc. ;

- coûts consécutifs à des actions pénales, responsabilité civile, dommage et intérêts, etc. ;
- coûts de la gestion de crise, de reprise après incidents, de restitution, de reconstitution des données, de remise en état, de remplacement des systèmes, etc.

3.5 DÉFINIR UNE STRATÉGIE DE SÉCURITÉ

3.5.1 Stratégie générale

En raison du caractère évolutif du contexte de la sécurité informatique (évolution des besoins, des risques, des technologies, des savoir-faire des délinquants, etc.), les solutions de sécurité ne sont jamais ni absolues, ni figées, ni définitives. Cela pose le problème de la **pérennité des solutions** mises en place et de leur évolution. De plus, la diversité et le nombre de solutions peuvent créer un problème de **cohérence** globale de l'approche sécuritaire. La sécurité d'un système d'information ne doit en aucun cas être un empilement de solutions de sécurité.

Ainsi, la technologie sécuritaire doit être au service d'une vision stratégique de la sécurité. Seule la dimension managériale de la sécurité permet de faire face au caractère dynamique du risque. C'est la qualité de la gestion qui permet de tirer le meilleur parti des outils existants et qui apporte une réelle plus-value au service de la sécurité. Dans cette perspective, la sécurité du système d'information n'est qu'une composante de la **sécurité globale de l'organisation**. Il est donc extrêmement important que les orientations stratégiques en matière de sécurité soient déterminées au niveau de l'état-major de l'institution concernée.

Inscrire la définition des objectifs de sécurité dans une **vision stratégique** de l'appréhension de la sécurité informatique et des télécommunications permet à une organisation de définir sa politique de sécurité. De ce fait, la définition d'une stratégie sécuritaire est spécifique à la structure qui la conçoit et dépend directement de son organisation et de sa stratégie générale (figure 3.5). Il existe donc autant de stratégies de sécurité, de politiques de sécurité, de mesures, de procédures ou de solutions de sécurité que d'organisations et de besoins sécuritaires à satisfaire dans un contexte donné.

La **direction générale** de l'organisation est responsable de l'établissement de la stratégie de sécurité, de l'appréciation des risques, et de la mise en place de la structure organisationnelle qui mettra cette stratégie en œuvre. Risques et politique font l'objet d'une évaluation et d'une actualisation permanentes.

3.5.2 Compromis et bon sens

Le choix des mesures de sécurité résulte généralement d'un **compromis** entre le coût des attaques quand le risque accepté se concrétise et celui de la réduction des

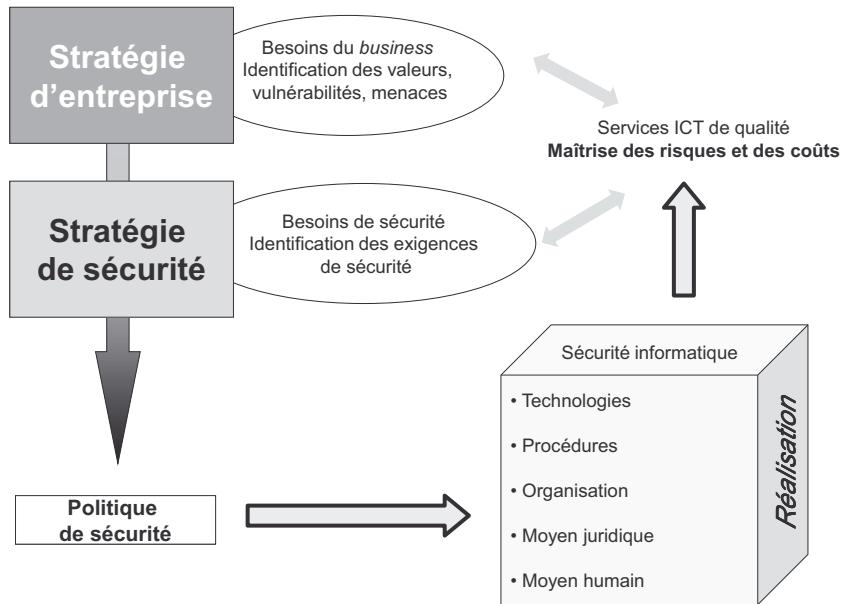


Figure 3.5 - De la stratégie d'entreprise à la stratégie sécuritaire.

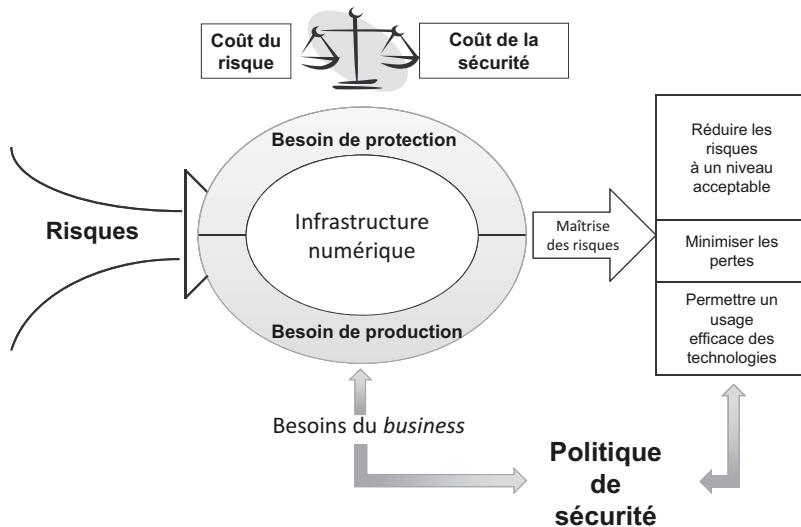


Figure 3.6 - La sécurité : une question de compromis.

risques. Il dérive de l'analyse à long, moyen et court termes des besoins et des moyens sécuritaires dépendant de la politique de l'organisation (figure 3.6).

La politique de sécurité, qui reflétera ce compromis, doit offrir une réponse graduée à un problème sécuritaire spécifique, en fonction de l'analyse des risques qui en est faite. Elle doit exprimer l'équilibre entre les besoins de production et de protection.

La définition d'une stratégie de sécurité est une affaire de bon sens, de vision, d'analyse, de compromis et de choix. Elle pourrait se résumer à une suite de questions simples auxquelles le gestionnaire doit apporter des réponses précises (figure 3.7) :

- Quelles sont les valeurs de l'organisation ?
- Quel est leur niveau de sensibilité ou de criticité ?
- De qui, de quoi, pourquoi doit-on se protéger ?
- Quels sont les risques réellement encourus ?
- Ces risques sont-ils supportables ?
- Quel est le niveau actuel de la sécurité ?
- Quel est le niveau de sécurité que l'on désire atteindre ?
- Quel est l'écart entre la protection à atteindre et celle que l'on a réellement ?
- Comment passer du niveau actuel au niveau désiré ?
- Quelles sont les contraintes effectives ?
- Quels sont les moyens disponibles ?

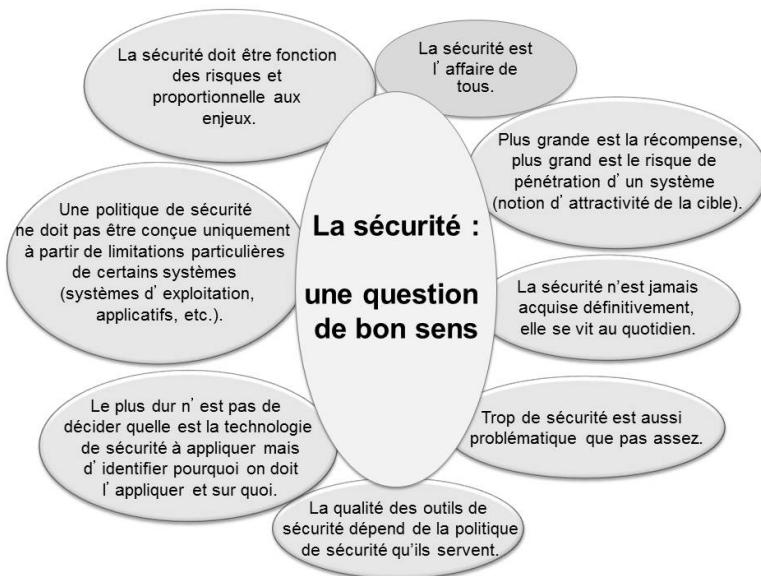


Figure 3.7 - La sécurité : une question de bon sens.

3.5.3 Responsabilité

Les responsables de systèmes d'information, de sécurité, les administrateurs systèmes ou les informaticiens sont des prestataires de service pour la partie de la sécurité qui les concerne, au même titre que les responsables des autres branches de l'organisation.

Leur capacité à accéder aux ressources informatiques implique en plus d'une **intégrité sans faille**, des procédures de surveillance et de contrôle de leurs actions particulièrement strictes, à la mesure des risques qu'ils font potentiellement courir aux systèmes qu'ils gèrent et à l'organisation qui les emploie.

Si les années de forte croissance des technologies de l'information ont permis à certains d'effectuer un **chantage** à leur direction en raison du faible nombre de personnel spécialisé, la multiplication des affaires criminelles ayant une origine interne, impliquant la complicité d'informaticiens, doit inciter les organisations à traiter la question de **responsabilité** et de dépendance avec **vigilance**.

3.5.4 Nouveaux risques, nouveaux métiers

Les **métiers de la sécurité informatique** et de l'information évoluent et se développent pour répondre aux nouveaux risques perçus.

Nouveau contexte, nouveaux besoins, nouvelle industrie de la sécurité. Force est de constater que le marché de la sécurité n'apporte pas de réponse totalement satisfaisante aux besoins de sécurité, la preuve en est le nombre d'incidents techniques, de défaillances technologiques ou humaines ou d'actes malveillants qui ne cessent de croître. Ainsi, tout potentiel dysfonctionnement informatique, quelle que soit son origine (accident, erreur ou malveillance), constitue un risque opérationnel dans la mesure où il en résultera un « *risque de pertes dû à l'inadéquation ou à l'échec de processus internes, du personnel et de systèmes ou provenant d'événements externes* » comme nous le rappellent les **accords de Bâle II**¹.

La gestion des risques est inhérente aux institutions économiques. À l'heure d'Internet, de la dématérialisation des données, des services, de la monnaie, la maîtrise du risque informationnel prend une dimension prépondérante dans la stratégie des organisations. Pour être pérennes, les institutions ont dû faire évoluer leur fonction sécurité. Évolution des fonctions, des tâches, des structures organisationnelles, des budgets, des mesures, des procédures, des contrôles, des outils et des formations consacrés à la sécurité informatique, tout cela reflète un certain niveau de maturité du **management** et de l'**ingénierie de la sécurité informatique**.

Bien que les métiers de la sécurité informatique et les cahiers des charges corrélés possèdent des périmètres variables plus ou moins bien définis par les organisations, les métiers suivants sont couramment identifiés :

- *Chief Information Officer (CIO)* – Associé au *top management* d'une institution, ce dirigeant est responsable de la stratégie et du management liés aux technologies de l'information ou du système d'information.
- *Chief Technology Officer (CTO)* – La personne est le plus souvent responsable de la recherche, du développement ou de l'innovation liés aux technologies de l'information.

1. Le Comité de Bâle sur le Contrôle bancaire (<http://www.cssf.lu/>) émet des recommandations afin d'accroître la stabilité du système financier international. Les accords de Bâle II concernent la maîtrise des risques bancaires (les risques de crédits, de marché et les risques opérationnels).

- *Chief Data Officer* (CDO) – C'est le responsable des gisements de données de l'entreprise, fonction de plus en plus nécessaire quand l'utilisation du *Big Data* fait partie de la stratégie de l'organisation.
- Pour ce qui concerne plus spécifiquement les métiers de la sécurité, retenons :
- *Chief Security Officer* (CSO) – Il s'agit d'un responsable en charge de toute la sécurité et de la sûreté de l'organisation.
- *Chief Information Security Officer* (CISO) – La personne assume pour son organisation la responsabilité de la sécurité de l'information.
- Un nouveau métier existe en France depuis 2005, celui de **Correspondant Informatique et Libertés** (CIL) dont la tâche est de contribuer à s'assurer du respect des obligations juridiques en matière de protection des données personnelles.

Selon la taille, les besoins ou la culture de l'organisation, diverses fonctions ou missions spécifiques existent comme par exemple : responsable de la sécurité des systèmes d'information, de la sécurité des réseaux, des systèmes, de la veille technologique en matière de sécurité, auditeur ou encore architecte de la sécurité des systèmes d'information. Ce dernier par exemple pourra être amené à formaliser les besoins de sécurité, à identifier les mesures de sécurité appropriées, à évaluer le niveau de sécurité, à gérer en fait la sécurité².

La prise en compte des contraintes légales et des besoins de conformité à des réglementations ou à des politiques internes a, par ailleurs, conduit à la définition de la fonction de *Chief Compliance Officer* ou de *Corporate Compliance Officer* (CCO).

La DRH (direction des ressources humaines) est aussi impactée par la sécurité de l'information de l'organisation et doit contribuer en particulier à la définition de la politique de sécurité et au développement de la sensibilisation de tous les employés.

3.6 ORGANISER ET DIRIGER

3.6.1 Organisation structurelle

Une politique de sécurité ainsi qu'une structure organisationnelle particulière pour la supporter doivent être définies.

 La mise en place d'une structure dédiée à la mise en œuvre et à la maintenance d'une politique de sécurité dépend de l'organisation et de la stratégie de l'entreprise.

2. L'ANSSI a publié en 2013 un référentiel métier concernant les compétences d'un architecte référent de la sécurité des systèmes d'information <http://www.ssi.gouv.fr/fr/anssi/publications/autres-publications-233/l-anssi-publie-un-referentiel-metier-de-l-architecte-referent-en-securite-des.html>

Selon une approche fonctionnelle, on distinguera le plus souvent le comité de direction générale, l'entité chargée de la réalisation de la mission de sécurité et l'organe de révision.

Le **comité de direction générale** est chargé du pilotage et du management de la sécurité. À ce titre, il doit :

- définir la stratégie, même si pour cela il recourt à la mission sécurité qu'il a mise en place ;
- valider la politique de sécurité : cela comprend la définition de la mission sécurité, l'identification des lois, des règlements et des pratiques relatifs à la manière de « gouverner » la sécurité afin de gérer, de protéger et de diffuser les informations sensibles ;
- désigner les acteurs de la sécurité et leur assigner leurs responsabilités³ ;
- s'impliquer activement à la sensibilisation des cadres et des collaborateurs ;
- défendre le budget sécurité au conseil d'administration.
- Les tâches de la **mission sécurité** (de nature transverse et pérenne) sont :
- aligner les objectifs de la mission elle-même avec la politique de sécurité de l'organisation ;
- identifier les cibles de la sécurité et s'assurer qu'elles font l'objet d'un suivi opérationnel ;
- élaborer et documenter la politique de sécurité ;
- créer et maintenir le plan de formation et de sensibilisation des collaborateurs, conforme au niveau de sécurité requis par la stratégie ;
- évaluer et sélectionner les composants externes (produits ou solutions) dédiés à la sécurité ;
- demander une étude d'impact sur la sécurité au service concerné lors de l'installation d'un nouvel élément informatique ;
- organiser et maintenir, avec le comité de direction générale, une cellule de gestion de crise dans le but de prendre des décisions pertinentes lors de sinistres majeurs ;
- instruire le budget sécurité ;
- suivre l'évolution des risques, des vulnérabilités, des normes de sécurité, des besoins, des mesures (notion de veille technologique en matière de sécurité et de vulnérabilité) ;
- établir en collaboration avec les organes de révision les plans d'audit.

Afin d'évaluer le niveau de sécurité de l'existant, les différentes cibles de sécurité font l'objet d'une **évaluation** spécifique qui sera confiée à l'**organe de révision**. Ce dernier doit être externe et pourra être mandaté par le conseil d'administration. Selon la cible, et sur la base d'un référentiel préalablement établi et validé par les commanditaires, on distinguera différents types d'**audit** :

3. À la responsabilité des personnes est associée le fait qu'elles doivent rendre des comptes et qu'elles seront tenues responsables du succès ou de l'échec de leur mission (notion d'imputabilité).

- **Audit financier et organisationnel :**
 - ◊ contrôler l'alignement de la stratégie de la sécurité avec le plan informatique et le budget ;
 - ◊ analyser les structures de coûts ;
 - ◊ contrôler l'organisation et l'adéquation de l'organisation ;
 - ◊ vérifier la conformité légale.
- **Audit de la sécurité :**
 - ◊ contrôler le niveau de la sécurité physique ;
 - ◊ contrôler le niveau de la sécurité logique (étanchéité du système d'information, contrôle d'accès, etc.) ;
 - ◊ contrôler en particulier la sécurité des réseaux et des sites web, cibles visibles et sensibles pour d'éventuelles cyberattaques ;
 - ◊ contrôler la documentation, la formation et la sensibilisation des utilisateurs en matière de sécurité ;
 - ◊ contrôler, le cas échéant, la couverture de l'assurance « risque informatique » ;
 - ◊ contrôler le dispositif associé au plan de secours (service minimal) ;
 - ◊ éventuellement, contrôler la mise en application ou la maintenance de la politique de sécurité si l'organisation a obtenu la certification ISO 27001.
- **Audit des centres d'exploitation** : analyser leur fonctionnement, c'est-à-dire entre autres les procédures, la documentation, l'organisation, les configurations des systèmes, les performances, les priorités des traitements, les plans de continuité d'activité et de secours, les procédures de sauvegarde et de reprise.
- **Audit des centres de développement** :
 - ◊ vérifier l'organisation et le contrôle interne ;
 - ◊ contrôler le niveau de prise en compte de la sécurité dans la gestion de projets (coordination, méthodes de développement, jeux de tests) ;
 - ◊ analyser le niveau de sécurité intégré dans le contrôle qualité.
- **Audit de la réception des applications** (ceci s'applique tant aux développements qu'à l'exploitation) : analyse des procédures de réception et de la maintenance des applications.
- **Audit de l'ensemble des acteurs du système d'information** : fiabilité des équipements, disponibilité des ressources, modes opératoires, etc.

3.6.2 Acteurs et compétences

Responsable sécurité

Un **responsable sécurité**, quel que soit son titre exact (directeur ou responsable de la mission sécurité, administrateur...), qui est fonction de la taille et de la culture de l'entreprise, est une personne qui porte la responsabilité du maintien de la sécurité en condition d'exploitation. Sa fonction est transversale et plus organisationnelle que technique. Il peut être amené à effectuer, entre autres, les tâches suivantes :

- contrôler la gestion et l'administration des moyens et des mesures de sécurité mis en œuvre sur les différentes cibles de la sécurité ;

Chapitre 3 • Gouvernance et stratégie de sécurité

- définir les priviléges d'accès aux ressources de manière à ce que l'utilisateur final ne puisse pas s'autoriser des accès ou interférer avec les ressources d'un autre utilisateur ;
- réévaluer régulièrement les priviléges d'accès ;
- élaborer et maintenir la documentation utilisateur et administrateur ;
- s'assurer que les cibles de sécurité sont sous surveillance, participer à l'analyse d'incidents éventuels et décider avec les acteurs concernés des actions nécessaires pour remédier aux défaillances constatées.

La question du rattachement du responsable sécurité à la hiérarchie de l'entreprise est d'importance. Si celui-ci est rattaché à la DSI (direction du système d'information), il lui sera difficile de mener les négociations nécessaires avec la direction de l'organisation, et son budget risque d'être une variable d'ajustement... à la baisse. Le responsable sécurité doit être le plus proche possible de la direction générale. Un bon niveau pour lui permettre d'exercer pleinement ses responsabilités est de le rattacher à la direction qualité, quand elle existe, ou directement au plus haut niveau de l'organisation.

Responsable des ressources humaines

Le **responsable des ressources humaines** (RRH), dans un contexte de gestion de la sécurité, est chargé notamment :

- d'effectuer les contrôles nécessaires avant l'engagement de nouveaux collaborateurs (intégrité des personnes et valeurs morales) ;
- de sensibiliser les nouveaux collaborateurs face à leur responsabilité en matière de sécurité. Sans être exhaustif, le RRH devra ainsi leur transmettre les directives de sécurité, les inciter à adopter un comportement éthique vis-à-vis de l'usage des nouvelles technologies, leur communiquer et leur faire signer une charte d'utilisation des ressources et les engager à la respecter, les rendre attentifs aux différentes clauses de non-divulgation et de confidentialité ;
- de faire signer la déclaration de respect du secret professionnel, de non-reproduction des informations et leur approbation de la politique de sécurité ;
- de coordonner les activités avec le responsable de sécurité lors d'une rupture de contrat d'un collaborateur.

Chefs de service

En tant que managers avertis, les **chefs de service** doivent notamment :

- veiller à ce que leurs collaborateurs ou consultants soient informés de la politique de sécurité afin qu'ils en respectent les directives ;
- informer les administrateurs de la sécurité concernés de toutes les modifications ayant un impact potentiel sur le niveau de sécurité ou sa gestion ;
- analyser, valider et prendre position par rapport aux demandes d'accès aux ressources émanant de leurs collaborateurs ;
- recenser et récupérer les informations sensibles détenues par un collaborateur qui quitte sa position dans l'organisation.

Ils ont ainsi un rôle majeur à assumer, tout spécialement lors du départ de collaborateurs. Ils doivent s'assurer qu'ils n'auront plus accès aux ressources dès la cessation de leur fonction afin qu'ils n'aient pas l'occasion de mettre à mal l'infrastructure informatique, spécialement lors de conflits révélés. Pour certains, l'employé est l'ennemi de la sécurité (le maillon faible), pour d'autres un facteur de sécurité.

Utilisateurs

Les **utilisateurs** constituent par excellence les points faibles de l'architecture de sécurité surtout lors d'usage mobile, ou par le biais de leur environnement informatique personnel et aussi parfois de solutions *cloud* privées (cas du **BYOD**, *Bring Your Own Device*). Ils ont l'obligation d'informer le responsable sécurité de tout élément ayant un impact potentiel sur la sécurité. Pour cela, la constitution de « fiches d'étonnement », quand ils remarquent un évènement pouvant impacter sur la sécurité de l'information, est une action nécessaire. Ce dernier point est particulièrement important car certains risques se concrétisent de manière progressive, et la notification de dysfonctionnements apparemment minimes (**signaux faibles**) permet parfois aux responsables concernés de mettre en œuvre des mesures palliatives avant la survenue d'un désastre.

3.7 PRISE EN COMPTE DES BESOINS JURIDIQUES

3.7.1 Infractions, responsabilités et obligations de moyens

De nouvelles législations, nées de la nécessité de définir un **cadre juridique** approprié à l'usage des technologies du numérique, viennent compléter la plupart des législations existantes. Renforcer la législation n'est pas forcément suffisant si les moyens de l'appliquer manquent. Une loi est de peu d'utilité si la justice n'est pas en mesure de traiter les preuves immatérielles, d'identifier, de localiser, d'appréhender et de sanctionner les auteurs de comportements cybercriminels. Elle n'est pas efficace si les malveillants ont le sentiment d'agir en toute impunité. Il est de la responsabilité des États de se doter de moyens nécessaires et suffisants pour poursuivre un crime informatique, et, parce que le cyberspace ne connaît pas de frontières, y compris au niveau de l'entraide judiciaire internationale.

Par ailleurs, il est également important que les responsables sécurité des organisations soient sensibilisés aux **contraintes d'une enquête policière** (documentation minimale relative à l'incident, conservation des traces, isolement des systèmes compromis, etc.). Cette mesure n'a de sens que lorsque les délits sont effectivement rapportés à la justice. L'État doit alors favoriser le signalement des cybercrimes et instaurer la confiance entre les différents acteurs du monde économique et les services de justice et de police.

Le seul instrument juridique à portée internationale existant est la **Convention sur la cybercriminalité⁴** – Budapest 23 novembre 2001 du **Conseil de l'Europe**.

Cette convention aborde les points suivants :

- Disposition de **droit pénal matériel** concernant :
 - ◊ les infractions contre la confidentialité, l'intégrité et la disponibilité des données et systèmes informatiques ;
 - ◊ les infractions informatiques ;
 - ◊ les infractions liées aux atteintes à la propriété intellectuelle et aux droits connexes.
- Disposition de **droit procédural** concernant :
 - ◊ la conservation rapide des données informatiques, de données relatives au trafic et à sa divulgation rapide à l'autorité compétente ;
 - ◊ la conservation et la protection de l'intégrité des données pendant une durée aussi longue que nécessaire pour permettre aux autorités compétentes d'obtenir leur divulgation ;
 - ◊ l'injonction de produire ;
 - ◊ la perquisition et la saisie des données stockées ;
 - ◊ la collecte en temps réel des données ;
 - ◊ la protection adéquate des droits de l'homme et des libertés.
- Chaque état doit adopter des **mesures législatives** et autres, qui se révèlent nécessaires pour ériger en infraction pénale, dans le respect de son droit interne :
 - ◊ l'accès intentionnel et sans droit à tout ou partie d'un système ;
 - ◊ l'interception intentionnelle et sans droit de données lors de transmissions non publiques, à destination, en provenance ou à l'intérieur d'un système ;
 - ◊ le fait intentionnel et sans droit d'endommager, d'effacer, de détériorer, d'altérer ou de supprimer des données ;
 - ◊ l'entrave grave intentionnelle et sans droit au fonctionnement d'un système ;
 - ◊ la production, la vente, l'obtention pour l'utilisation, l'importation, la diffusion ou d'autres formes de mise à disposition d'un dispositif conçu ou adapté pour réaliser une des infractions mentionnées ;
 - ◊ l'introduction, l'altération, l'effacement ou la suppression intentionnelle et sans droit de données, engendrant des données non authentiques, dans l'intention qu'elles soient prises en compte ou utilisées à des fins légales, comme si elles étaient authentiques ;
 - ◊ le fait intentionnel et sans droit de causer un préjudice patrimonial à autrui par l'introduction, l'altération, l'effacement ou la suppression de données, toute forme d'atteinte au fonctionnement d'un système, dans l'intention, frauduleuse ou délictueuse, d'obtenir sans droit un bénéfice économique pour soi-même ou pour autrui ;
 - ◊ « la complicité en vue de... » est érigée en infraction pénale ainsi que « la tentative intentionnelle de... ».

4. <http://conventions.coe.int/Treaty/FR/Treaties/Html/185.html>

- Les **états** doivent établir leurs compétences à l'égard de toute infraction pénale lorsque cette dernière est commise :
 - ◊ sur son territoire ;
 - ◊ à bord d'un navire battant pavillon de cet État ;
 - ◊ par un de ses ressortissants, si l'infraction est punissable pénalement là où elle a été commise ou si l'infraction ne relève de la compétence territoriale d'aucun État.
- Règles concernant la **coopération internationale** en matière :
 - ◊ d'extradition ;
 - ◊ d'entraide aux fins d'investigation ;
 - ◊ de procédures concernant les infractions pénales liées à des systèmes et données informatiques ;
 - ◊ de recueil de preuves sous forme électronique d'une infraction pénale.
- Création d'un réseau d'entraide :
 - ◊ 24h/24, 7j/7 ;
 - ◊ point de contact national ;
 - ◊ assistance immédiate pour les infractions.

Tableau 3.1 – Lignes directrices de l'OCDE en matière de sécurité informatique (juillet 2002).

Sensibilisation	Les parties prenantes doivent être sensibilisées au besoin d'assurer la sécurité des systèmes et réseaux d'information et aux actions qu'elles peuvent entreprendre pour renforcer la sécurité.
Responsabilité	Les parties prenantes sont responsables de la sécurité des systèmes et des réseaux d'information.
Réaction	Les parties prenantes doivent agir avec promptitude et dans un esprit de coopération pour prévenir, détecter et répondre aux incidents de sécurité.
Éthique	Les parties prenantes doivent respecter les intérêts légitimes des autres parties prenantes.
Démocratie	La sécurité des systèmes et des réseaux d'information doit être compatible avec les valeurs fondamentales d'une société démocratique.
Évaluation des risques	Les parties prenantes doivent procéder à des évaluations des risques.
Conception et mise en œuvre de la sécurité	Les parties prenantes doivent intégrer la sécurité en tant qu'un élément essentiel des systèmes et réseaux d'information.
Gestion de la sécurité	Les parties prenantes doivent adopter une approche globale de la gestion de la sécurité.
Réévaluation	Les parties prenantes doivent examiner et réévaluer les sécurités des systèmes et réseaux d'information et introduire les modifications appropriées dans leur politique, pratiques, mesures et procédures de sécurité.

Bien que des lois, ou des principes directeurs comme ceux énoncés par l'OCDE (Organisation de coopération et de développement économiques) : « *Lignes directrices de l'OCDE régissant la sécurité des systèmes et des réseaux – vers une culture de la sécurité – 2002⁵* » (tableau 3.1) existent depuis longtemps, leur application reste faible. Ce sont la difficulté et la complexité du chantier à mettre en œuvre et l'importance des moyens nécessaires pour atteindre les objectifs de lutte contre la cybercriminalité qui font qu'Internet est un vecteur de la criminalité.

3.7.2 Prendre en compte la sécurité en regard de la législation

Certaines législations ou réglementations doivent impérativement être respectées par les organisations, qui doivent alors se doter, dans une démarche de **maîtrise du risque juridique**, de mesures de sécurité de leur système d'information, leur assurant la **conformité juridique** requise.



La responsabilité d'une personne morale ou physique mise en défaut de sécurité lors d'une infraction informatique établie peut être pénale, civile ou administrative. Les dirigeants d'une organisation ont le plus souvent une **obligation de moyens de la sécurité** (mais non une obligation de résultat).

La **législation** est de plus en plus un facteur endogène de prise en compte de la sécurité. La valeur économique des investissements nécessaires à assurer le seuil minimal de sécurité (protection des infrastructures et protection juridique) est fonction des pertes matérielles et aussi des risques encourus par l'organisation.

La législation en matière de **traitement des données à caractère personnel** et de **protection de la sphère privée** est également un facteur qui pousse les entreprises à bien gérer leur sécurité, notamment en ce qui concerne la gestion des données utilisateurs, la surveillance des communications et des employés, la gestion des sauvegardes et le traitement automatisé de données à caractère personnel. Plusieurs directives du Parlement européen et du Conseil de l'Europe depuis 1981 abordent ces questions et mettent en avant le respect des droits fondamentaux.

L'usage abusif d'Internet hors du cadre professionnel par des employés (**cybers-lacking**) pose des problèmes de productivité. Cela peut induire des problèmes de sécurité (introduction de virus, divulgation d'informations sur des réseaux sociaux par exemple...) et potentiellement mettre en cause la responsabilité civile ou pénale de l'organisation et de l'employé. Pour tenter de maîtriser l'usage non professionnel des outils de communication mis à disposition par les organisations pour ses employés, ces dernières peuvent être tentées d'utiliser des outils de surveillance pour contrôler l'usage fait des ressources informatiques et télécoms (notion de **cybersurveillance** des employés).

5. <http://www.oecd.org/dataoecd/16/22/15582260.pdf>. En 2013, l'OCDE procède à la réactualisation de ces lignes directrices, qui restent des principes fondamentaux toujours d'actualité.



L'organisation doit être vigilante au respect de la **protection des données à caractère personnel** de ses employés comme de celles de ses clients, fournisseurs ou partenaires. Lors de la mise en place de procédures de **cybersurveillance**, elle doit éviter l'abus de contrôle et se conformer aux lois en vigueur dans ce domaine.

La prérogative patronale du pouvoir de contrôle de l'employeur, aussi légitime soit-elle, ne doit pas s'exercer en violation des droits et des libertés des employés. Dans la plupart des pays, la législation ou la doctrine et la jurisprudence recommandent que la mise en œuvre de la cybersurveillance soit préalablement accompagnée d'une **charte d'utilisation** des ressources, d'une information aux employés et à leurs représentants et d'une proportionnalité des moyens de surveillance mis en œuvre.

Dans la plupart des pays, il existe des contradictions majeures entre le fait que les organisations sont responsables des actes illégaux de leurs employés (ce qui les conduit à mettre en place des outils de surveillance, suivant l'état de l'art) et l'obligation faite aux organisations de respecter l'intimité numérique de ces derniers.

Il est constaté que la démarche sécuritaire est souvent limitée à la mise en place des mesures de réduction des risques pour les valeurs informationnelles des organisations. Or, l'approche sécuritaire doit également répondre aux besoins de **sécurité des individus**, notamment en ce qui concerne la protection de leur vie privée et le respect de leurs **droits fondamentaux** dans le cadre de leur activité professionnelle.

3.7.3 La confiance passe par le droit, la conformité et la sécurité

Depuis le scandale financier Enron⁶, en 2001, la **conformité à des réglementations** est en passe de devenir une préoccupation majeure des dirigeants des grandes organisations. La preuve en est l'apparition d'un nouveau métier, celui de *Chief Compliance Officer* : personne possédant une grande compréhension des technologies de l'information tout en étant compétent en droit et dans le domaine d'activité de l'entreprise. Déplaçant ainsi les frontières traditionnelles d'une approche verticale des problématiques business, l'organisation recourt aux réglementations comme celles de Sarbanes-Oxley (SOX⁷) par exemple, pour démontrer que des pratiques frauduleuses n'ont pas cours. Ainsi, l'importance est mise sur le respect des **contraintes réglementaires** pour établir la **confiance**, au travers de la mise en place d'un certain nombre de contrôles internes, répondant aux exigences spécifiées par le « Sarbanes-Oxley Act⁸ », qui concernent notamment le type d'information à conserver et leur durée de conservation.

6. « En décembre 2001 la faillite frauduleuse du courtier en énergie Enron fut le résultat de manipulations comptables. La faillite d'Enron a entraîné le licenciement de 5 600 personnes et fait s'évaporer 68 milliards de dollars de capitalisation. » Source : <http://www.monde-diplomatique.fr/2004/02/RAMONET/10686>. Voir également <http://www.monde-diplomatique.fr/dossiers/enron/>.

L'enjeu pour les organisations est alors de pouvoir s'appuyer sur des technologies de l'information afin de conserver, traiter et restituer, en toute sécurité et à un coût optimal, les données nécessaires à la validation de la **conformité** à une loi. Au regard des **responsabilités** civile et pénale engagées par les dirigeants, ces derniers ont tout intérêt à s'associer les compétences nécessaires à la maîtrise de ce nouveau type de risque réglementaire et à s'appuyer sur des solutions de sécurité informatique, pour avoir confiance dans les informations à partir desquelles les décisions sont prises. Cela déplace le problème de la responsabilité des pratiques frauduleuses sur la qualité des informations et pose le problème de la confiance envers les technologies de l'information. Ce sentiment de « **sûreté** » se bâtit notamment au travers de la sécurité informationnelle. La confiance est alors liée à la fiabilité des solutions et des mesures de sécurité. Même si des lois favorisent l'adoption de comportements sécuritaires, la sécurité est avant tout du ressort de la **gestion des risques**. Peu d'études ont été conduites pour connaître l'impact des réglementations sur le niveau de sécurité des organisations. De plus, être en conformité réglementaire n'est pas forcément synonyme d'être en sécurité. Est-ce que le fait d'être en conformité avec des lois permet d'augmenter la qualité, l'efficacité et la sécurité des technologies de l'information ?

Pour les organisations, l'**intelligence juridique** devient le facteur clé de succès de la réalisation de la sécurité informatique. La responsabilité pénale des acteurs, — du responsable sécurité ou du directeur de systèmes d'information par exemple — est de plus en plus invoquée lorsque les ressources informatiques qu'ils gèrent, sont l'objet ou le moyen d'une fraude.

Il est nécessaire que les responsables puissent alors démontrer que des mesures suffisantes de protection du système d'information et des données ont été implantées afin de se protéger contre un délit de manquement à la sécurité (notion d'**obligation de moyens**). Les responsables d'entreprises doivent donc être extrêmement attentifs à l'égard du droit, et leur système d'information doit être en **conformité juridique**.

Les enjeux juridiques liés à la sécurité informatique sont désormais devenus prépondérants. Ils peuvent concerner, par exemple, la conservation des données, la responsabilité des prestataires techniques ou des hébergeurs, la gestion des données

7. Votée par le Congrès américain en juillet 2002 et ratifiée par le président Bush le 30 du même mois suite aux scandales des affaires Enron et Worldcom, la **loi Sarbanes-Oxley** implique que les présidents des entreprises cotées aux États-Unis certifient leurs comptes auprès de la *Securities and Exchanges Commission* (SEC), l'organisme de régulation des marchés financiers US. Guidée par trois grands principes soit l'exactitude et l'accessibilité de l'information, la responsabilité des gestionnaires et l'indépendance des vérificateurs/auditeurs, la loi vise à augmenter « *la responsabilité corporative et à mieux protéger les investisseurs pour rétablir leur confiance dans le marché.* » Source : http://www.lexposia.com/pages/dossiers/lex04_dossiers_sarbanesoxley.html . Voir également *Sarbanes-Oxley, Financial and Accounting Disclosure Information*, <http://www.sarbanes-oxley.com/>.

8. Législation émanant des États-Unis, adoptée en juillet 2002 et gérée par la *Securities and Exchange Commission*, qui impose des règles de conformité aux organisations. Voir <http://www.sec.gov/>.

personnelles des clients, la cybersurveillance des employés, la propriété intellectuelle, les contrats informatiques, ou la signature électronique. Ils constituent maintenant autant de points à prendre en considération lors de la mise en place de solutions de sécurité.

La sécurité est souvent la résultante d'un compromis, du choix consistant à privilégier un facteur aux détriments d'autres. Toutefois, l'application des **principes de précaution**, de coopération, d'économie, de décentralisation et de séparation des pouvoirs en matière de sécurité informatique serait de peu d'utilité si elle ne desservait pas une politique de sécurité résultant d'une gestion efficace des besoins et des risques. Ainsi, le droit dans le domaine du numérique peut devenir un atout stratégique pour les organisations qui le maîtrisent.

3.8 PRINCIPES D'INTELLIGENCE ÉCONOMIQUE

Une organisation qui maîtrise la sécurité de ses infrastructures informationnelles peut être encore plus performante si elle s'appuie également sur une démarche d'**intelligence économique (IE)** pour tirer parti au mieux des informations stratégiques la concernant et de celles relatives à son environnement pour assurer sa compétitivité dans un contexte de mondialisation, d'hyperconnectivité et de guerre économique (notion de sécurité économique).

La protection du **patrimoine numérique** peut être considérée comme faisant partie d'une démarche d'intelligence économique, mais celle-ci à un champ d'application plus large. Elle englobe la protection des savoir-faire et de la connaissance, devrait permettre d'être proactif, d'influencer son environnement, de rechercher des informations spécifiques (se renseigner et non pas espionner – notion de veille stratégique) et de protéger et défendre son entreprise contre des menées malveillantes. Dans sa dimension sécuritaire, l'intelligence économique doit contribuer à **éviter la fuite de données sensibles** (*Data Leak Prevention [DLP]*), le vol de celles-ci, et les atteintes à l'image et à la réputation. Il s'agit de rechercher activement des informations stratégiques et utiles à la compétitivité de l'entreprise, de les analyser, de les valoriser, de les protéger, de les diffuser (de manière sélective) et de les exploiter (décision, action). L'intelligence économique peut être vue comme un outil d'aide à la décision, à l'innovation, à l'identification d'opportunités économiques ou encore d'aide à la gestion des risques.

La **collecte informationnelle** peut être fortuite ou ciblée, active et/ou passive, et se réalise à partir d'une multitude de sources comme par exemple les espaces publics, les transports, les clubs, les manifestations professionnelles (salons, conférences, etc.), Internet (réseaux sociaux,...), les médias, les sous-traitants, les stagiaires, les partenaires, etc. Une information peut être distinguée en fonction de sa source et de son mode d'accès. Elle est qualifiée de blanche si elle est ouverte et facilement accessible, de noire si son accès et son usage sont spécialement protégés et restreints, et de grise si son accès est licite mais demande une connaissance et un effort particuliers pour y accéder.



L'intelligence économique ne peut s'intéresser qu'à l'information blanche ou grise. S'intéresser à l'information noire est du domaine de l'espionnage.

3.9 PRISE EN COMPTE DES RISQUES CACHÉS

3.9.1 Externalisation et *cloud computing*

Les risques « cyber » s'inscrivent dans une problématique plus large des risques liés à la dépendance des infrastructures numériques et à des fournisseurs d'infrastructures matérielles et logicielles, de capacités de traitement, de télécommunication, de stockage, de services ou encore d'informatique en nuage (*cloud computing*). Certains fournisseurs (notamment les GAFA – Google, Amazon, Facebook et Apple – et les NATU – Netflix, Airbnb, Tesla, Uber) sont devenus des géants incontournables d'Internet ou de la téléphonie mobile, et sont de véritables empires à la volonté hégémonique affichée. La montée en puissance de certains groupes mondialisés induit de nouveaux risques notamment liés à l'espionnage industriel et à la capacité de ces groupes de réaliser un « fichage » des utilisateurs, voire un « filtrage » des échanges, et cela à l'échelle mondiale.

Avant **d'externaliser** (*outsourcing*), de sous-traiter tout ou partie de son informatique, et avant de devenir dépendant d'un fournisseur, surtout s'il est étranger, il est nécessaire de se poser la question de savoir si les économies à court terme, induites par une telle sous-traitance, sont justifiées en regard de la perte de la maîtrise des technologies, des savoir-faire et du risque de détournement d'information ou d'exploitation abusive des données. Il s'agit de choix qui impactent durablement les développements futurs des entités qui s'allient à des fournisseurs tiers, et qui s'accompagnent généralement de la perte de maîtrise des données et des infrastructures, des pertes de capacités de recherche et développement (R & D), mais aussi de délocalisation ou de chômage pour les employés de la structure cliente. De plus, le retour en arrière est souvent impossible et les préjudices subis sont irrémédiables. Par ailleurs, lors de l'externalisation de ses données et traitements, l'utilisateur comme l'organisation s'exposent à différents risques de perte de maîtrise.

Cela peut concerter :

- la localisation des données ;
- la sous-traitance de sous-traitants ;
- l'impossibilité de pouvoir effectuer des audits ;
- l'indisponibilité des ressources suite à des problèmes réseaux ou techniques du prestataire ;
- des risques liés au partage du *cloud* avec d'autres acteurs (risques liés au co-hébergement et à la mutualisation des ressources).



Sous certaines conditions, externaliser ses données et la gestion de sa sécurité vers une entreprise dont la sécurité est le métier n'est pas forcément une mauvaise solution, si l'on n'investit pas le budget nécessaire pour que la sécurité de l'information de son organisation soit gérée en interne.

3.9.2 Droits fondamentaux et libertés civiles

Internet, la surveillance électronique, la traçabilité des activités, la collecte de données, leur exploitation à l'insu des personnes, les modèles d'affaires basés sur les données personnelles ou encore l'informatique en nuage par exemple ne sont pas forcément compatibles avec le respect des droits fondamentaux et des libertés civiles des citoyens.

Par ailleurs, les fournisseurs de services peuvent profiter des données livrées de plein gré par des internautes et de celles collectées à leur insu. Les géants d'Internet sont des puissances économiques qui imposent leurs conditions générales, sans les expliquer clairement. Ils peuvent stocker, traiter, exploiter les données du consommateur (publicité ciblée, profilage comportemental, etc.), généralement dans un pays étranger où la loi l'autorise mais où le droit national dont l'internaute est le ressortissant ne s'applique pas nécessairement. La plupart du temps, l'utilisateur a accepté ces conditions en ayant cliqué sur le bouton « J'accepte » pour créer son compte, sans avoir vraiment lu ou compris ce qu'il a accepté. De nos jours, il existe un réel accroissement de la surveillance informatisée et à grande échelle, réalisable par l'exploitation des traces numériques laissées par l'utilisation de l'informatique ou des télécoms (cartes à puce, téléphonie, GPS, Internet, RFID, etc.). En contrepartie, un niveau de sécurité adapté aux besoins des individus et des organisations n'est pas garanti mais peut contribuer notamment à une mise en danger de la compétitivité économique, de la liberté d'expression, d'association, de se déplacer (liberté de mouvement, de naviguer sur Internet), du droit à la connaissance, du droit au secret de la correspondance ou du droit à la protection de la vie privée.

La culture des **droits humains** et des **libertés civiles** chère aux pays démocratiques peut être perçue et mise en œuvre fort différemment de par le monde.

En 1948, la Déclaration universelle des droits de l'homme était adoptée. Cette même année, George Orwell rédigeait son roman « 1984 » rendant célèbre l'expression « *Big Brother is watching you.* » **Big Brother** est le dictateur invisible qui exerce un contrôle totalitaire au travers d'un système de surveillance asymétrique. Le terme de Big Brother s'est imposé pour évoquer des procédés de surveillance liberticides, l'abus de pouvoir et les atteintes à la sphère privée des individus.

Connecté, l'internaute participe à sa propre surveillance, l'accepte, la trouve éventuellement normale ou s'y résigne en échange d'un service dont il ne peut plus se passer.

Internet est aussi omniprésent qu'invisible et intrusif. Associé à un faux sentiment de confiance et de fraternité mis en exergue par certains services, il peut être comparable au système de surveillance décrit par Orwell. Il existe un rapport de force inégalitaire entre surveillants et surveillés, car si l'internaute peut voir l'autre (le surveillé peut être aussi surveillant), il ne voit pas ceux qui maîtrisent les infrastructures et les contenus d'Internet, ni ce que les acteurs licites et illicites voient de lui ou la manière dont ses données sont utilisées.

En ne voyant que le service rendu par la technologie et non la capacité de surveillance qu'elle autorise, l'internaute ne peut saisir les enjeux globaux de la

protection de ses données à caractère personnel. Il ne peut donc remettre en question ni ses choix, ni certains acteurs d'Internet qui pourraient être considérés comme de nouveaux dictateurs qui se seraient appropriés le slogan propagandiste de Big Brother : « *L'ignorance c'est la force* ». L'utilisateur a accepté ces conditions quand il a créé son compte pour bénéficier des services de ces « Big Brothers ». Pourtant, la protection des données personnelles est une condition préalable de l'autodétermination et de la protection de la liberté d'expression et de la dignité humaine.

3.9.3 Cyberrésilience, risque écologique et écosystème numérique

Que ce soit dans le domaine de l'écologie, de la psychologie, du management, de l'informatique ou de l'économie par exemple, la **résilience** est relative à la capacité d'un « système » à pouvoir continuer à opérer si possible normalement, ou au moins en mode dégradé, après un incident, un choc, une perturbation, une panne. Parler de **cyberrésilience** aujourd'hui revient à admettre qu'il est impossible d'empêcher des cyberincidents d'avvenir, que le cyberspace est un monde fragile, instable et potentiellement hostile. Pour autant, faire de la cyberrésilience ne revient pas à accepter une relative impuissance à protéger correctement les infrastructures informationnelles, même si parfois il peut exister une certaine insuffisance de mesures de sécurité préventives efficaces.

La **cybersécurité** ne doit pas s'inscrire uniquement dans une logique de réactivité qui permet d'être préparé à « survivre » à un cyberincident, d'origine intentionnelle ou non. Bien que cette capacité à résister soit fondamentale et absolument nécessaire, elle ne peut suppléer à un défaut d'une approche globale multiacteur aux niveaux national et international, de l'appréhension du phénomène relevant pour l'essentiel de la cybercriminalité et de la réalité des cyberattaques. Chacun peut devenir un acteur actif ou passif de la cybercriminalité, et un équipement familier comme un smartphone ou un ordinateur peut devenir une arme. Cela change considérablement le paradigme de la protection car contrairement au passé, il n'est plus possible de sécuriser un périmètre particulier. De plus, la notion de coffre-fort électronique, représentée par la mise en œuvre de mécanismes cryptographiques, pour mettre à l'abri des données sensibles, ne permet pas de garantir la protection absolue de ces dernières.

Parmi les risques indirects induits par l'informatique et ayant des impacts sur notre planète, retenons principalement les risques relatifs :

- à l'élimination et au recyclage des déchets électroniques ;
- à la consommation énergétique (besoins en électricité accrus et permanents) ;
- au réchauffement climatique (dégagement de chaleur et besoin de refroidissement des ordinateurs et des fermes de serveurs) ;
- à l'exploitation des terres rares et des métaux nécessaires à la construction des équipements électroniques ;
- aux conséquences environnementales d'incidents provoqués par des cyberattaques sur des systèmes contrôlant des stations d'épuration, la production et la distribution de produits toxiques, des alarmes incendies, etc.

Le **cyberespace** est un nouvel espace où se déploient toutes sortes d'activités. Il permet entre autres d'influencer, de déstabiliser ou encore de réaliser des profits. C'est un instrument au service de la profitabilité économique et un lieu d'expression du pouvoir : c'est en fait un territoire stratégique. Dès lors, il est à protéger et à défendre. De plus, comme dans tous les secteurs d'activité, les activités militaires sont elles aussi tributaires de l'informatique et des systèmes d'information pour être opérationnelles et performantes. L'efficacité des moyens de défense traditionnels dépend désormais des capacités informatiques.

Aujourd'hui, l'**écosystème numérique** construit autour d'Internet constitue également un théâtre, un champ de bataille où le secteur de la défense est présent. Toute doctrine militaire se doit impérativement de prendre en compte ce nouveau champ de bataille et de développer des axes stratégique, tactique et opérationnel dans les domaines de la défense active, de l'informatique offensive et défensive ainsi que dans celui de la **gestion de crise informatique**. Certains pays l'ont bien compris et sont très actifs dans ce domaine et dans la conquête et la domination du cyberespace. Rappelons que le département de la Défense américain (DoD) est à l'origine d'Internet, que depuis toujours l'informatique et la cryptographie sont au service des forces armées. L'ignorer ou accuser un retard en matière de **doctrine informatique offensive et défensive**, sous prétexte de ne pas vouloir alimenter un discours sur « la militarisation » d'Internet, serait faire preuve de naïveté et d'angélisme et desservirait la société en laissant d'autres entités imposer leur suprématie dans le cyberespace et dans le monde réel.



La lutte informatique défensive (LID) doit être encouragée, mais la **lutte informatique offensive** (LIO) ne peut être utilisée que par des organismes légalement mandatés pour la pratiquer, ce qui exclut en particulier les entreprises.

Doctrine et posture de **cyberdéfense** se développent, notamment dans les pays les plus connectés. Elles reposent sur des acteurs formés à la cybersécurité et à la cyberdéfense, ce qui suppose que de telles filières de formation existent. Par ailleurs, un réservoir de miliciens ou de réservistes éventuellement civilo-militaires dûment accrédités et compétents en cybersécurité peut contribuer à la cyberdéfense d'un pays et à faire entrer **l'esprit de cyberdéfense** auprès du citoyen. Une connaissance approfondie des systèmes, des vulnérabilités, une attitude vigilante, une fonction de renseignement, une veille active et dynamique de l'environnement cyber, ancrées dans la réalité politique du moment, contribue à avoir une approche prospective pour mieux anticiper les menaces, maîtriser les risques cybernétiques, détecter les anomalies pour en limiter les impacts et développer la cyberrésilience. Résister aux cyberattaques est désormais une **responsabilité collective**. La cybersécurité ne peut s'appréhender que de manière interdisciplinaire et intégrative. Cela se traduit au niveau de l'État par une vision partagée et transversale de la problématique, par une collaboration interministérielle (interdépartementale, interoffice) renforcée et par une capacité à travailler ensemble (secteur public et secteur privé).

Agir ensemble, en toute connaissance des risques pour saisir les opportunités technologiques afin de construire une société de l'information inclusive, bâtir un cyberspace et un écosystème numérique de confiance et durable, donner du sens aux changements induits par le numérique, devrait nous mobiliser autour d'un objectif commun et des valeurs de société partagées. Cela pourrait peut-être être résumé par la volonté de vivre ensemble en toute sécurité et stabilité dans un monde *on line* et *offline*.

Résumé

Les principales préoccupations des acteurs de la sécurité sont relatives à l'appréhension globale de la maîtrise des risques technologique et informationnel *via* une approche managériale intégrative et évolutive, tenant compte des facteurs d'ordres humain, technologique, économique, juridique et politique des questions de sécurité.

Il n'y a pas de règle pour définir une stratégie de sécurité mais celle-ci repose sur le bon équilibre à trouver entre les différentes exigences et les facteurs parfois contradictoires, à prendre en considération, comme par exemple :

- risques et menaces ;
- besoins et solutions (niveaux de sécurité et coûts des solutions) de sécurité ;
- facilité d'utilisation et efficacité des solutions de sécurité ;
- délais de disponibilité des solutions efficaces et conviviales ;
- coûts de développement et d'intégration des mesures de sécurité.

Un équilibre est à obtenir entre les besoins de sécurité et les dimensions financières et humaines de la mise en œuvre opérationnelle des solutions de sécurité viables. Le niveau de sécurité des infrastructures résulte donc d'un compromis entre trois facteurs : le coût, le niveau de service de sécurité et le temps de livraison (notion de priorisation des actions et des mesures de sécurité à réaliser). Il est illusoire de croire que ces trois facteurs pourraient être satisfaits simultanément. Des choix doivent être effectués pour déterminer quel sera le facteur à privilégier et à partir duquel les autres devront être adaptés.

L'État possède des responsabilités importantes pour la réalisation d'une sûreté numérique. Ceci est particulièrement vrai pour la définition des lois, pour la spécification et la réalisation d'une stratégie de sécurité informatique pour les infrastructures vitales du pays, pour conserver sa souveraineté, pour assurer la sécurité dans le cyberspace et renforcer la lutte contre la cybercriminalité. De plus, il doit favoriser et encourager la recherche et le développement de solutions en matière de sécurité mais aussi promouvoir une **culture de la sécurité et du respect de l'intimité numérique**, imposer le respect d'un minimum de normes de sécurité, et faire entrer l'esprit de cyberdéfense auprès du citoyen.

Bien que le marché tente de développer des mécanismes pour réduire, transférer ou partager le risque informatique, le secteur privé comme les pouvoirs publics d'ailleurs ne peuvent résoudre seuls la question de maîtrise des cyberrisques. Se posent alors des questions relatives aux modèles économiques sous-jacents à la réalisation d'une infrastructure informatique et télécom fiable et sécurisée et aux **partenariats publics-privés (PPP – Public Private Partnerships)**.

Replacer l'**humain** et les **valeurs démocratiques** au cœur du développement des technologies de l'information et des solutions de sécurité est nécessaire pour donner les moyens aux internautes de devenir des **cybercitoyens** avertis et non pas des consommateurs vulnérables et dépendants ou des proies faciles de la cybercriminalité. Cela devrait contribuer à ce que le cyberspace ne devienne un lieu à risques, un espace policé à outrance ou contrôlé par des entités commerciales superpuissantes ou des agences de sécurité.

Il est de ce fait de la responsabilité des États de définir une véritable **politique de développement de la société de l'information** en fonction de ses valeurs propres, de sa culture, et de mettre à disposition les ressources nécessaires à cette réalisation.

Exercices

- 3.1** Que recouvre la notion de stratégie de sécurité ?
- 3.2** Pourquoi la sécurité doit-elle être gérée selon un processus continu ?
- 3.3** Faites un schéma des principales étapes de réalisation d'une démarche sécuritaire.
- 3.4** Dans quelles mesures la sécurité informatique est-elle la résultante d'un compromis ?
- 3.5** Pourquoi considère-t-on le principe de vocabulaire comme un principe de base de la sécurité ?
- 3.6** Qu'est-ce que la confiance en matière de sécurité informatique ?
- 3.7** Dans quelle mesure la conformité réglementaire se décline-t-elle comme un besoin de sécurité ?
- 3.8** Expliquez la notion de risque juridique en matière de sécurité informatique.
- 3.9** Pourquoi la compréhension du risque juridique par des responsables de la sécurité informatique est-elle importante ?
- 3.10** À quels besoins répond la Convention européenne sur la cybercriminalité ?
- 3.11** Pourquoi est-il nécessaire d'optimiser une démarche sécuritaire ?
- 3.12** À quoi correspond la notion de structure organisationnelle de la sécurité ?
- 3.13** Qu'apporte la notion de gouvernance de la sécurité à celle de gestion de la sécurité ?
- 3.14** Quelles sont les relations entre une approche de gestion de risques et de gestion de la sécurité ?

3.15 Quels sont les éléments de la maîtrise des risques ?

3.16 Pourquoi faut-il tenir compte du rôle du facteur humain dans une démarche sécuritaire ?

3.17 À quoi correspond la notion de société de l'information inclusive ?

3.18 Qu'est-ce que l'intelligence économique ? Quelle est sa relation avec la sécurité de l'information ?

Solutions

3.1 La **stratégie de sécurité** est une réponse d'ordre stratégique aux besoins de sécurité particuliers d'une organisation (notion de plan stratégique). Mettre en œuvre la sécurité consiste à rendre opérationnelle une stratégie de sécurité spécifiée dans une politique de sécurité en implantant les mesures adaptées (figure 3.8).

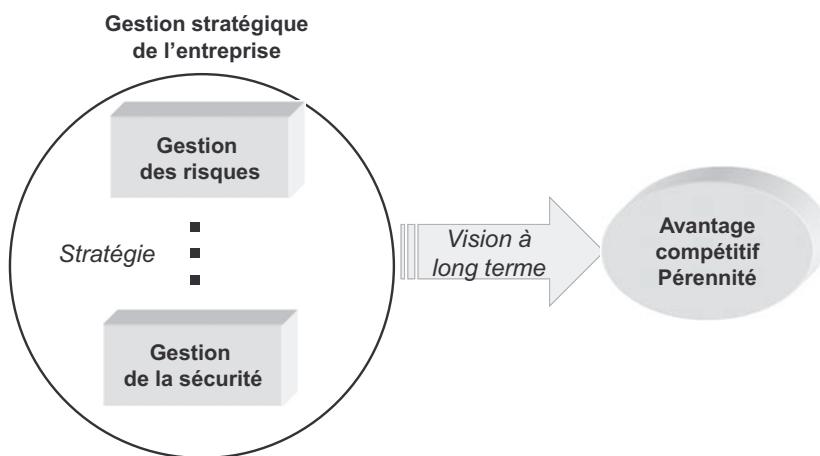


Figure 3.8 – La stratégie de sécurité : une vision à long terme.

3.2 Les solutions de sécurité doivent toujours répondre de manière efficace aux besoins de protection des ressources qui évoluent sans cesse (apparition de nouvelles vulnérabilités et menaces, le savoir-faire des attaquants évolue, les personnes et l'environnement informatique changent). Cela impose la réalisation d'un **processus de gestion continu** pour faire face au contexte dynamique de l'environnement à sécuriser. La sécurité n'est jamais acquise définitivement (figure 3.9).

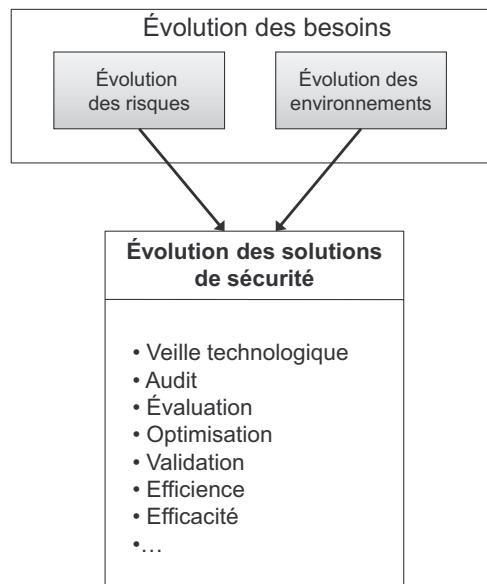


Figure 3.9 – Prise en compte de la dimension dynamique de la sécurité.

3.3

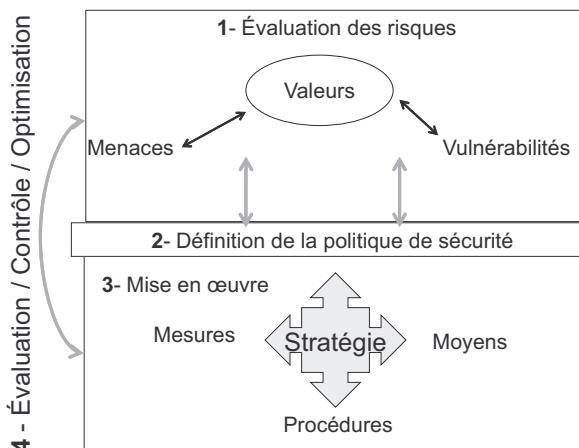


Figure 3.10 – Étapes de réalisation d'une démarche sécuritaire.

3.4 La sécurité informatique ne peut être que la résultante d'un compromis dans la mesure où un équilibre est à trouver entre le coût du risque (des impacts), celui de sa réduction, et le niveau de sécurité.

3.5 Le **principe de vocabulaire** se définit comme la nécessité de s'accorder, au niveau de l'entreprise, sur un langage commun de définition de la sécurité. Ceci est très important dans la mesure où la sécurité informatique est une tâche transversale qui nécessite la collaboration de plusieurs acteurs aux compétences diverses, provenant de domaines et de secteurs différents (techniques, économiques, juridiques, processus métiers, etc.). Un vocabulaire uniifié permet d'effectuer un travail basé sur des principes traités et compris de la même façon. Un bon document sur ces définitions, qui est de plus une norme, est donné par l'ISO 27000.

De plus, la sécurité informatique qui sera déployée en entreprise fera objet de documents spécifiques tels que des stratégies de sécurité ou politiques de sécurité. Le vocabulaire commun est un facteur de succès non seulement pour leur rédaction mais surtout pour la compréhension de la part des employés des notions, principes, obligations et actions à mettre en œuvre pour satisfaire les exigences de sécurité.

3.6 La notion de **confiance** relève d'un sentiment perçu à partir d'un contexte donné. Ce sentiment ne s'appuie pas sur une recherche approfondie d'indicateurs ou de preuves formelles. Il existe une ambiguïté quant à l'implémentation de ce concept dans le domaine très concret et pragmatique de la sécurité de l'information. Relevons que la sécurité sous-entend en quelque sorte une **non-confiance**. Ces notions sont indépendantes et non bijectives. La sécurité peut amener un certain sentiment de confiance, cependant **la confiance ne garantit pas un niveau de sécurité effectif**. Construire la sécurité et établir une confiance entre les différents acteurs – utilisateurs des technologies de l'information – ne peut se réaliser qu'en ne faisant pas confiance aux différents acteurs ! La confiance n'excluant pas le contrôle, il faudrait permettre aux utilisateurs de pouvoir effectuer le contrôle des dispositifs de sécurité auxquels ils sont soumis. En tout état de cause, c'est en sachant qui contrôle la sécurité et en toute connaissance des risques encourus que la confiance peut s'établir entre les différents acteurs et clients des infrastructures informatiques et télécoms.

3.7 Le fait de ne pas être conforme à des **réglementations** particulières met en danger la pérennité de l'entreprise et son existence. Aux dommages induits par un incident affectant les critères de sécurité et par conséquence les valeurs de l'entreprise, s'ajoutent ceux liés au fait de ne pas avoir agi en conformité avec les lois et réglementations en vigueur. Ainsi, toute démarche sécuritaire doit prendre en considération le risque juridique comme le risque technologique, et les besoins de conformité réglementaire.

3.8 Le **risque juridique** est le fait de ne pas être en accord avec la législation en vigueur concernant les domaines liés aux technologies de l'information. Cela peut relever du droit civil ou pénal. Ce risque peut avoir des impacts financiers importants et porter atteinte à l'image et à la réputation des personnes et des organisations. Les entreprises ont une obligation de moyen ; ainsi, par exemple, elles doivent mettre en place les mesures de protection et de contrôle suffisantes pour sécuriser les données personnelles lors de leur traitement, de leur stockage et de leur transmission.

3.9 Le **risque juridique** est une composante des risques qu'encourt l'organisation, et de ce fait il doit faire partie intégrante de l'analyse des risques et de la gestion de la sécurité, d'où l'importance de la compréhension de ce type de risque par un **responsable sécurité** puisqu'il doit diminuer la probabilité du risque ainsi que son impact. La connaissance des risques juridiques va permettre leur prise en compte au niveau de la stratégie de l'entreprise et de la politique de sécurité, qui sera alignée aux exigences légales en vigueur.

Pour ce faire, le responsable de sécurité doit focaliser son intention sur l'identification des ressources (financières, humaines, corporelles, fournisseurs, partenaires, clients, environnementales, immatérielles), sur le droit applicable, sur les normes « les plus sensibles », sur l'identification des comportements transgressifs, sur les choix stratégiques de l'entreprise, sur les pratiques opérationnelles (matière de la responsabilité sans faute) et effectuer (ou faire effectuer) une veille juridique.

3.10 La **Convention européenne sur la cybercriminalité** répond au besoin de disposer d'un cadre de référence international concernant les mesures légales qui doivent exister au niveau national tout en étant compatibles au niveau international. La Convention définit, entre autres, les types d'infractions possibles *via* Internet, le droit applicable et les besoins de coopération internationale des instances de justice et de police pour poursuivre un délit commis *via* les technologies Internet.

3.11 Il est impératif que toute **démarche sécuritaire** soit efficace et efficiente, et donc optimisée en fonction des objectifs poursuivis et de la manière de les atteindre. Cela sous-entend la pertinence de la stratégie, la satisfaction des exigences de maîtrise de risques selon des priorités fixées en fonction du niveau de criticité des valeurs à protéger, l'adéquation des solutions et la cohérence des mesures.

De plus, les ressources (financières et humaines) sont toujours limitées. Elles doivent être utilisées à bon escient et couvrir en priorité les risques dont les impacts seraient les plus graves.

La sécurité doit être proportionnée et optimisée en fonction des risques réels et des impacts.

3.12 Au sein des institutions, la **structure organisationnelle de la sécurité** reflète les choix d'organisation et de management de la sécurité. Elle contribue à indiquer par exemple le comportement, les droits, les devoirs et les responsabilités de chaque acteur, au travers notamment de la politique, des mesures et des directives sécuritaires appropriées dans le cadre des objectifs et des stratégies de l'organisation.

3.13 La **gouvernance de la sécurité** est une activité située au niveau le plus haut de la direction de l'entreprise, qui concerne le processus par lequel la sécurité de l'information est traitée par rapport aux visions stratégiques du business. Elle vise donc à s'assurer que les mesures de sécurité en place sont optimales et appropriées. La gestion de la sécurité est un des éléments constitutifs et de réalisation de la gouvernance de la sécurité. Elle concerne principalement l'identification des valeurs

à protéger et les risques encourus, la mise en place de mesures organisationnelles, techniques et procédurales, et l'évaluation périodique des mesures en vue de leur efficacité, optimisation et rationalisation afin de répondre aux besoins stratégiques de l'organisation.

3.14 Les deux approches sont liées. La **gestion de risques** concerne l'identification des actifs, l'appréciation des vulnérabilités, des menaces et des facteurs relatifs, et l'évaluation des risques afin de les maîtriser. La **gestion de la sécurité** peut commencer dès lors qu'il est possible de spécifier une politique de sécurité en fonction des risques encourus. La gestion de la sécurité répond donc aux besoins de la maîtrise des risques.

3.15 La **maîtrise des risques** nécessite une analyse des risques (identification des valeurs, analyse des menaces, estimation des impacts) afin de permettre la spécification et la réalisation d'une politique de sécurité avec les moyens (financiers, organisationnels, humains, technologiques) nécessaires à la mise en place de mesures efficaces et appropriées, à un processus continu d'évaluation, de contrôle, validation et optimisation.

Pour une entreprise, les principaux éléments de la maîtrise des risques sont liés à sa capacité à pouvoir identifier ses valeurs et les scénarios de perte de celles-ci. Cela comprend une bonne compréhension de l'entreprise, de son environnement et de ses vulnérabilités et des menaces qui pourraient les exploiter.

3.16 La sécurité n'est pas une activité technologique. Le **facteur humain** est très important pour plusieurs raisons : les décisions stratégiques et les priorités en matière de sécurité sont prises sur la base d'une réflexion humaine. La sécurité est un acte de management qui nécessite plusieurs qualités humaines (compréhension, communication, gestion, motivation...) et la sécurité est mise en œuvre et utilisée par des hommes et des femmes.

De plus, les personnes même les plus performantes ne sont pas à l'abri d'une erreur (erreur d'appréciation, de discernement, d'inattention, de gestion...). Elles peuvent commettre des erreurs stratégiques ou opérationnelles. Enfin, elles peuvent également être malveillantes ou encore être les cibles de chantage et de toute sorte de pressions (besoins financiers...) et donc être à l'origine d'un problème de sécurité.

3.17 La notion de **société de l'information inclusive** correspond au fait que tout un chacun puisse tirer parti de la révolution informationnelle, s'approprier les technologies de traitement et de communication de l'information et devenir un acteur à part entière de la société de l'information et un cybercitoyen averti et non un consommateur vulnérable et dépendant.

Ainsi, la sécurité informatique au sens large devrait pouvoir contribuer à la protection de l'intégrité physique et morale de chaque utilisateur, à la protection de sa sphère privée et au respect de ses droits fondamentaux afin de mettre l'humain et les valeurs démocratiques au cœur du développement technologique.

3.18 L'**intelligence économique** est relative à la maîtrise de l'information stratégique qui permet à une organisation d'être compétitive. Cette dernière s'appuie également sur des mesures de sécurité de ses infrastructures numériques et de ses informations pour assumer sa performance économique. Aussi l'intelligence économique peut être perçue comme une extension du champ de la sécurité de l'information qui englobe, outre la protection du patrimoine numérique des organisations, des phases actives de recherche, de collecte et de traitement de l'information.

POLITIQUE DE SÉCURITÉ

4

PLAN

- 4.1 De la stratégie à la politique de sécurité
- 4.2 Propriétés d'une politique de sécurité
- 4.3 Méthodes et normes contribuant à la définition d'une politique de sécurité
- 4.4 De la politique aux mesures de sécurité
- 4.5 Continuité et gestion de crises
- 4.6 Place de l'audit des systèmes d'information en matière de sécurité
- 4.7 Mesurer l'efficacité de la sécurité
- 4.8 Certification des produits de sécurité

OBJECTIFS

- Définir ce qu'est une politique de sécurité et la manière de la spécifier.
- Mettre en évidence le rôle pivot d'une politique de sécurité pour la maîtrise des risques et la gestion de la sécurité.
- Offrir un panorama des principales normes et mesures de sécurité.
- Traiter les problématiques de gestion des plans de secours et de la continuité des activités.

4.1 DE LA STRATÉGIE À LA POLITIQUE DE SÉCURITÉ

Une **politique de sécurité** exprime la volonté managériale de protéger les valeurs informationnelles et les ressources technologiques de l'organisation. Une politique de sécurité concrétise une stratégie sécuritaire et est un outil indispensable à la gouvernance de la sécurité (figure 4.1). Elle spécifie les moyens (ressources, procédures, outils, etc.) qui répondent de façon complète et cohérente aux objectifs stratégiques de sécurité.



La politique de sécurité fait le lien entre la stratégie de sécurité de l'entreprise et la réalisation opérationnelle de la sécurité. La **gestion des risques** constitue le point de départ de l'analyse des besoins sécuritaires qui permet la définition de la politique de sécurité (figure 4.2).

Chapitre 4 • Politique de sécurité

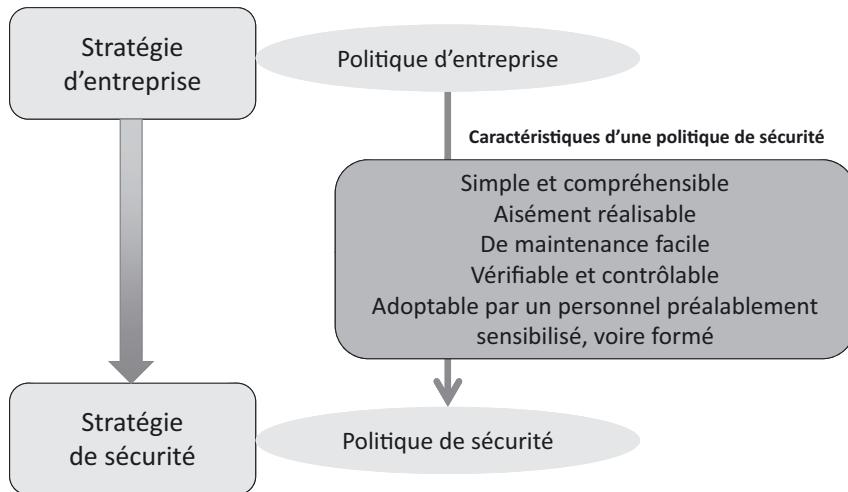


Figure 4.1 – Stratégie et politique de sécurité.

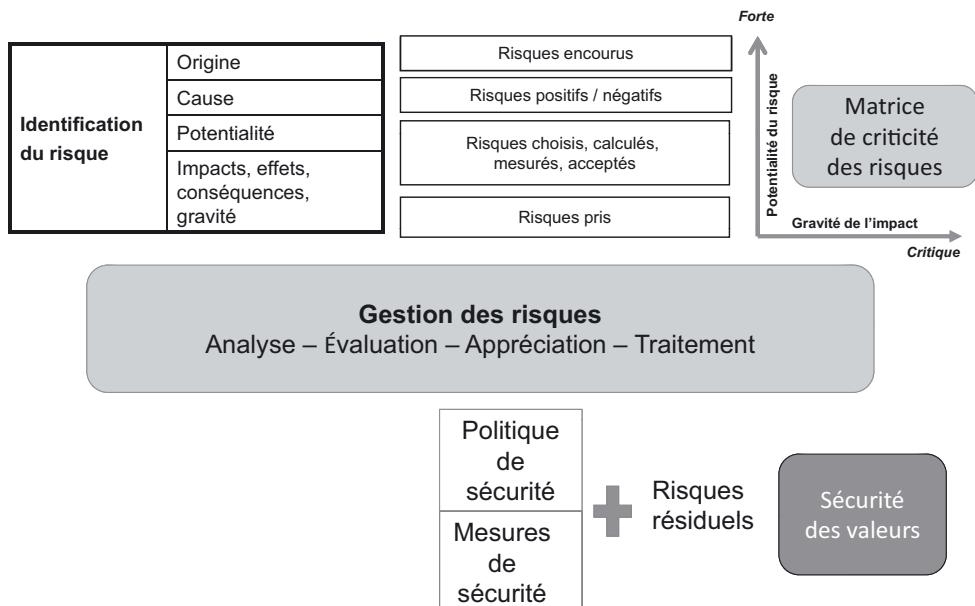


Figure 4.2 – De l'analyse des risques à la politique de sécurité.



La politique de sécurité permet de transcrire le travail effectué pour comprendre les risques et leurs impacts, en des **mesures opérationnelles de sécurité**. Sa spécification facilite le choix et la mise en œuvre des mesures de sécurité. Elle donne de la cohérence à la gestion et contribue à adopter, vis-à-vis des risques, une attitude proactive et réactive.

Une politique de sécurité contribue à la **maîtrise des risques**, tout en réduisant la probabilité d'occurrence d'attaques qui concrétisent les risques et en diminuant leurs impacts. Même un bon gestionnaire de la sécurité, tout en anticipant et prévenant certains incidents, volontaires ou non, n'est pas devin. Ne pouvant anticiper toutes les nouvelles menaces, mais sachant qu'elles exploitent les vulnérabilités et les failles des systèmes en place, le gestionnaire s'emploiera à **réduire les vulnérabilités** de l'environnement à protéger afin de minimiser la probabilité de réalisation des menaces.

4.2 PROPRIÉTÉS D'UNE POLITIQUE DE SÉCURITÉ

Une politique de sécurité résulte d'une **analyse des risques** et est définie pour répondre aux exigences de sécurité, dans un contexte donné (figure 4.3). Elle se traduira par la réalisation de mesures, de fonctions, de procédures, de services, comme par exemple :

- des règles de classification de l'information, d'utilisation des ressources ;
- des outils : contrôle d'accès, chiffrement des données, authentification, systèmes pare-feu, sondes de détection d'incidents, de surveillance et d'enregistrement, journalisation, traçabilité ;
- des contrats de services : clauses de responsabilité, devoirs et obligations ;
- des plans gestion de crise, de secours, de continuité et de reprise d'activité ;
- des plans d'actions de poursuite en justice ;
- des mesures d'assurance, de gestion de la performance.

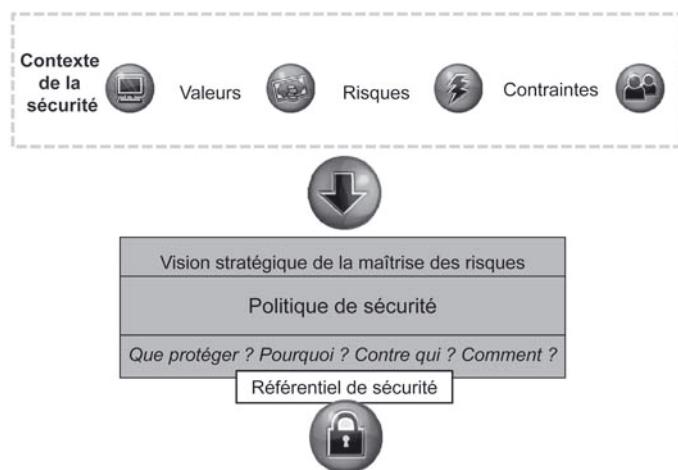


Figure 4.3 - Contexte d'une politique de sécurité.

Une politique de sécurité est **périodiquement évaluée**, optimisée et adaptée à l'évolution des risques. Elle doit prendre en compte la variabilité **temporelle** et la variabilité **spatiale** des besoins de sécurité (tranche horaire, nomadisme des usagers) ce qui la rend complexe à spécifier et à mettre en œuvre.

Une politique de sécurité peut être structurée en sous-politiques correspondant au contexte particulier d'une organisation comme le montre la figure 4.4.



Figure 4.4 – Différentes composantes d'une politique de sécurité.

4.3 MÉTHODES ET NORMES CONTRIBUANT À LA DÉFINITION D'UNE POLITIQUE DE SÉCURITÉ

4.3.1 Principales méthodes françaises

Dans un premier temps, il faut pouvoir identifier les risques avant d'identifier les parades à mettre en place. On peut s'appuyer alors sur une méthode qui facilite l'identification des points principaux à sécuriser (notion de *check list*), ou sur des normes ou sur un **ensemble reconnu de bonnes pratiques** (*best practices*). Toutes peuvent servir de guide à l'élaboration d'une politique de sécurité. Elles sont utilisées plus ou moins complètement et le plus souvent adaptées à un contexte particulier en fonction de l'entité qui les met en œuvre.

4.3 • Méthodes et normes contribuant à la définition d'une politique de sécurité

Les méthodes préconisées par le **Clusif** sont historiquement **Marion** (méthode d'analyse des risques informatiques et optimisation par niveau) puis **Méhari** (méthode harmonisée d'analyse des risques)¹ (figure 4.5).

Méthode Méhari -- Méthode Harmonisée d'Analyse des Risques

-  Propose un cadre et une méthode qui garantissent la cohérence des décisions prises au niveau directorial.
-  Structure la sécurité de l'entreprise sur une base unique d'appréciation, dans la complexité des systèmes d'information.
-  Permet la recherche de solutions au niveau opérationnel de la sécurité en déléguant les décisions aux unités opérationnelles et autonomes.
-  Assure, au sein de l'entreprise, l'équilibre des moyens et la cohérence des contrôles.
-  Quelques applications de Méhari :
 - Plan Stratégique de Sécurité
 - Plan(s) Opérationnel(s) de Sécurité
 - Traitement d'une famille de scénarios
 - Traitement d'un risque spécifique
 - Traitement d'un critère de sécurité
 - Traitement d'un scénario particulier
 - Traitement d'une application opérationnelle
 - Traitement d'un projet...



Figure 4.5 – Méthode préconisée par le Clusif.

Au-delà de l'aide à l'analyse des vulnérabilités et des risques, Méhari permet d'avoir une vision globale et stratégique de la problématique de la sécurité des entreprises, par la définition d'un plan stratégique de sécurité à partir duquel des plans opérationnels pourront être définis. Méhari est une méthode adaptable, évolutive et compatible avec les normes internationales du domaine.

En France, l'Agence nationale de la sécurité des systèmes d'information (ANSSI) propose une méthode bien documentée, avec des exemples et des conseils, qui est mise à jour régulièrement². Dénommée **Ebios**, pour *Expression des besoins et identification des objectifs de sécurité*, cette méthode, largement utilisée entre autres par les administrations françaises, permet de spécifier les objectifs de la sécurité des organisations. Elle facilite largement l'appréhension du contexte de sécurité et constitue une véritable aide à la définition des objectifs et des politiques de sécurité. Cela peut conduire à remplir le document « Fiche d'expression rationnelle des objectifs de sécurité (Feros) » pour ce qui concerne toutes les ressources sensibles, afin de déterminer au mieux les mesures de sécurité nécessaires à leur protection.

Il existe par ailleurs diverses directives nationales : allemandes, issues du *Bundesamt für Sicherheit Informationstechnik*³, canadiennes, issues du CST (Centre de la

1. www.clusif.asso.fr
2. <http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html>
3. <http://www.bsi.de>

sécurité des télécommunications)⁴, américaines, issues du NSI (*National Standards Institute*)⁵, par exemple, qui traitent des politiques de sécurité.

4.3.2 Normes internationales ISO de la série 27000

Origine et évolution

À l'origine de la série de normes **ISO 27000**, se trouve la norme **ISO 17799** adoptée par l'ISO⁶ à la fin de l'année 2000 à partir de la norme BS 7799 élaborée par l'Association de normalisation britannique en 1995. Avant d'être reconnue comme une méthode de référence, la norme internationale ISO 17799 a tout d'abord été contestée du fait de sa procédure accélérée de normalisation : elle n'avait pas été révisée par les États membres avant d'être publiée et n'avait donc pas tenu compte des savoir-faire et autres méthodes existant dans d'autres pays.

Basée sur la **gestion des risques**, la norme propose un **code de pratiques** pour la gestion de la sécurité et identifie des exigences de sécurité, sans toutefois spécifier la manière de les réaliser. On peut ainsi considérer cette norme tour à tour comme un référentiel pour la définition d'une politique de sécurité, une liste de points de risques à analyser (*check list*), une aide à l'audit de sécurité, ou encore comme un support à la communication sur la sécurité.

L'intérêt de cette norme réside dans le fait qu'elle aborde les aspects organisationnels, humains, juridiques et technologiques de la sécurité informatique en rapport aux différentes étapes de conception, mise en œuvre et maintien de la sécurité d'un système d'information.

La version 2005 de la norme ISO 17799 a accordé plus d'importance à la **dimension managériale**. De nouveaux paragraphes concernant l'évaluation et l'analyse des risques, la gestion des valeurs et des biens ainsi que la gestion des incidents ont été intégrés.



La norme ISO 17799 : 2005 a été rebaptisée en 2007, norme **ISO 27002**. Elle définit la sécurité de l'information comme étant un processus visant à protéger l'information contre une large gamme de menaces, de manière à garantir la continuité des services, à réduire le risque et à optimiser le retour sur investissement. Elle permet de répondre aux questions : Que protéger ? De quoi ? Pourquoi se protéger ?

La première étape consiste à réaliser l'inventaire des valeurs à protéger en distinguant leur degré de criticité afin d'affecter des priorités à la réalisation de la sécurité. Cette tâche de « prioritisation » des actions de sécurité est souvent très difficile à réaliser. La compréhension des menaces, accompagnée d'une étude des vulnérabilités techniques et managériales liées aux technologies utilisées, est alors nécessaire

4. <http://www.cse-cst.gc.ca>

5. <http://www.ansi.org>

6. ISO : *International Organization for Standardization* (www.iso.org). Les normes de la série 27000 sont expliquées notamment sur le site <http://www.27000.org>.

4.3 • Méthodes et normes contribuant à la définition d'une politique de sécurité

pour contribuer à l'identification des risques pouvant porter atteinte aux actifs de l'entreprise. Des mesures de sécurité peuvent ensuite être mises en place pour contrer la survenance et les impacts des risques.

L'objectif de la norme est de contribuer à définir des recommandations autorisant la gestion, l'implémentation ou la maintenance de la sécurité de l'information d'une organisation. Elle constitue en quelque sorte un guide rassemblant des pratiques de gestion de la sécurité de l'information. Basée sur une approche de gestion des risques, la norme facilite l'identification des exigences fonctionnelles de sécurité. Elle permet de spécifier une politique de sécurité et de définir une architecture de sécurité.

La famille des normes ISO/IEC 27000/2016

La famille des normes ISO/IEC 27000/2016 traite des différents domaines du **management de la sécurité de l'information**, à savoir :

- Les notions fondamentales, une vue d'ensemble et une formalisation du vocabulaire sont données dans la norme **ISO 27000**.
- La norme **ISO 27001** définit les exigences de sécurité d'un système de management de la sécurité (SMSI).
- La norme **ISO 27002** propose un code de bonnes pratiques pour la gestion de la sécurité de l'information.
- Des lignes directrices (guide) pour la mise en œuvre et l'implémentation d'un **système de management de la sécurité de l'information** (SMSI) sont édictées dans la norme **ISO 27003**.
- Des métriques du management de la sécurité de l'information sont identifiées dans le document **ISO 27004**.
- La gestion du risque en matière de sécurité de l'information est traitée dans la norme **ISO 27005**.
- Les exigences pour les organismes auditant et certifiant un SMSI font l'objet de la norme **ISO 27006**.
- Les directives concernant le processus d'audit d'un SMSI se trouvent dans la norme **ISO 27007**.
- La norme **ISO 27008** traite des directives pour les auditeurs concernant les contrôles à effectuer dans un SMSI.
- La norme **ISO 27010** est relative à la gestion de la sécurité de l'information des communications intersectorielles et interorganisationnelles.
- La norme **ISO 27011** traite du management de la sécurité de l'information pour les organismes de télécommunications.
- La norme **ISO 27015** correspond à des lignes directrices pour le management de la sécurité de l'information pour les services financiers.
- La norme **ISO 27018** peut être considérée comme un guide pour la protection des données à caractère personnel dans les infrastructures de clouds publics.
- La norme **ISO 27019** se focalise sur le management de la sécurité de l'information des systèmes de contrôle des procédés spécifiques à l'industrie de l'énergie.

- Les normes **ISO 27031 à 27035** abordent respectivement les questions relatives au plan de continuité des affaires, à la cybersécurité, à la sécurité des réseaux, à la sécurité des applications et à la gestion des incidents.
- Les normes **ISO 27036 à 27039** concernent la sécurité de l'information dans un contexte de relation avec des fournisseurs.
- La norme **ISO 27037** quant à elle traite de l'identification, de la collecte et de la préservation des traces numériques.
- Les normes **ISO 27038 et 27039** sont respectivement relatives à des techniques de sécurité concernant l'élaboration de documents numériques, et la sélection, le déploiement et les opérations des systèmes de détection d'intrusion.
- La question du management de la sécurité de l'information relative à la santé fait l'objet de la norme **ISO 27799**, élaborée sur la base de l'ISO 27002.

Introduction à la norme ISO 27001

La norme ISO 27001 propose un modèle pour établir, implémenter, exploiter, surveiller, maintenir et améliorer le système de management de la sécurité de l'information **SMSI** (ou ISMS, *Information Security Management System*). La norme 27001 se focalise sur l'implémentation d'un système de management de la sécurité basé sur une structure formalisée et des contrôles à effectuer.

La norme se base sur un modèle dit **modèle PDCA** (*Plan, Do, Check, Act*) – Préparer (ou Planifier) – Développer – Contrôler ou Vérifier – Agir (ou Réagir) (figure 4.6) qui reprend le concept de la « roue de Deming »⁷. Telle cette roue qui remonte une pente en exécutant à chaque tour le « *Plan, Do, Check puis Act* », à chaque tour on met une cale pour empêcher la roue de redévaler la pente, le modèle PDCA implique qu'à chaque passage, arrivé au « *A de Act* », il faille caler le modèle et ne jamais s'arrêter de le poursuivre, pour ne pas risquer de perdre tous les atouts accumulés dans l'évolution de la sécurité du SMSI et se retrouver au bas de la pente. Le modèle PDCA implique un perfectionnement permanent de la sécurité du SMSI.

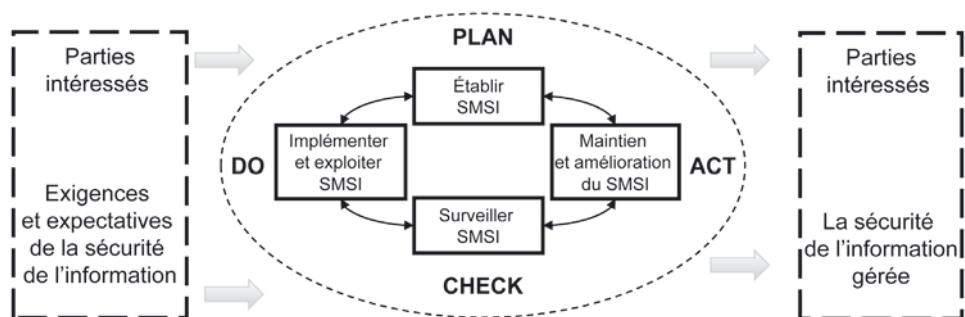


Figure 4.6 – Le modèle PDCA (adapté à partir de la norme ISO 27001).

7. La méthode comporte quatre étapes, chacune entraînant l'autre, et vise à établir un cercle vertueux qui permet d'améliorer sans cesse la qualité d'un produit, d'une œuvre, d'un service, etc.

4.3 • Méthodes et normes contribuant à la définition d'une politique de sécurité

Appréhender la sécurité sous la forme d'un modèle PDCA contribue à :

- **comprendre** les exigences de sécurité et les besoins de la politique de sécurité (PSSI, politique de sécurité du système d'information) ;
- **implémenter** et effectuer des contrôles pour gérer le risque informationnel ;
- **surveiller** et revoir la performance du SMSI ;
- **proposer** des améliorations basées sur des mesures d'efficacité du SMSI.
- Le fait de développer un modèle de gestion de sécurité satisfaisant les exigences de la norme implique trois étapes :
 - **Étape 1 – Création d'un cadre managérial** afin de fixer les directives, les intentions et les objectifs pour la sécurité de l'information et de définir la politique stratégique qui engage la responsabilité du management.
 - **Étape 2 – Identification et évaluation des risques** réalisées sur la base des exigences de sécurité définies par l'organisation pour déterminer les actions managériales appropriées à entreprendre et les priorités pour maîtriser les risques.
 - **Étape 3 – Développement du SMSI**, sélection et implémentation des contrôles à effectuer. Une fois que les exigences ont été identifiées, les contrôles appropriés peuvent être sélectionnés afin de s'assurer que les risques que le système d'information fait encourir à l'organisation sont réduits à un niveau acceptable conformément aux objectifs de sécurité de l'entreprise. Ces contrôles portent sur les politiques, pratiques ou procédures à suivre en tenant compte de la structure de l'organisation.

Établissement et gestion du SMSI

La première phase de conception et de mise en place du système de management de la sécurité informationnelle débute par l'établissement et la gestion du système, par l'appréciation de l'envergure et des limites du système d'information sur lequel le système de management sera calqué, conformément aux besoins de l'entreprise. Une fois le périmètre sur lequel va porter la sécurité identifié, l'appréciation du risque est effectuée. Il s'agit d'une analyse et d'une évaluation du risque (menaces génériques, circonstances particulières, vulnérabilités, scénarios de risques, de probabilités et de dommages) au regard des actifs de l'entreprise (information, matériels, logiciels, réseaux, processus, activités). Une fois le risque et ses composantes identifiés, l'entreprise peut décider de la manière dont ce risque va être traité. Les alternatives sont l'acceptation, l'évitement, la réduction ou le transfert du risque.

Toute cette démarche aura comme résultat l'obtention de l'autorisation d'implémenter le SMSI, ainsi que la préparation d'un document d'applicabilité. Faute de cela, le contrôle de la mise en œuvre en termes d'efficience et d'efficacité ne serait pas possible.

Responsabilité du management

Le management doit clairement mettre en évidence son engagement en ce qui concerne les étapes du SMSI. Pour se faire, il doit :

- **établir** une politique de SMSI ;

- **désigner** les rôles et les responsabilités ;
- **mettre en place** les moyens pour une communication la plus large possible ;
- **décider** des critères d'acceptation des risques (ou de non-acceptation) ;
- **assurer** que des audits du SMSI seront effectués d'une manière régulière ;
- **assurer** que tout le personnel assigné à définir le SMSI possède ou acquière les compétences nécessaires pour pouvoir effectuer la tâche.

Révision et amélioration du SMSI

La révision du SMSI se révèle nécessaire puisque l'environnement de travail est dynamique. Les changements technologiques et structurels sont assez fréquents et les composantes du risque sont dynamiques (augmentation exponentielle du savoir-faire des malveillants, nouvelles vulnérabilités ou menaces, etc.).

En ce qui concerne la **révision**, les données à prendre en considération pour éventuellement modifier les procédures et les contrôles en toute connaissance de cause et optimiser l'efficacité du SMSI, sont :

- les résultats d'audit ;
- les retours d'expérience des parties intéressées ;
- les résultats des mesures effectuées ;
- les données de surveillance continue (monitoring, veille active, etc.).

En ce qui concerne l'**amélioration** de SMSI, les actions à entreprendre sont relatives aux mesures correctives et préventives, à l'identification des non-conformités et de leurs causes pour y remédier.

Norme ISO 27001

La norme ISO 27001 propose des contrôles à personnaliser en fonction des besoins et des objectifs de sécurité pour faciliter le pilotage et l'amélioration de la sécurité. Ils concernent les domaines suivants :

- **La politique de sécurité** : les contrôles à mettre en place serviront à démontrer le support de la direction, à la sécurité informatique, conformément aux besoins de l'organisation, sont présents en approuvant, publiant, communiquant et revoyant la politique de sécurité du système d'information.
- **La sécurité informationnelle** de l'organisation : les contrôles à mettre en place montreront le fait que la sécurité informationnelle, dans et à l'extérieur de l'organisation, est assurée (preuves de l'existence de l'engagement du management, coordination des activités de la sécurité avec tous les responsables des différents départements de l'organisation, contact permanent avec les groupes d'intérêt, identification de toutes les exigences de sécurité concernant les données par exemple).
- **La gestion des actifs** : les contrôles à mettre en place montreront le fait qu'une protection appropriée des actifs de l'organisation est accomplie et maintenue (existence des inventaires des actifs à protéger, existence clairement définie et formalisée de l'assignation des responsabilités, etc.).

4.3 • Méthodes et normes contribuant à la définition d'une politique de sécurité

- La **sécurité des ressources humaines** : les contrôles à mettre en place montreront le fait que les employés, les contractants, et les tierces personnes comprennent leurs responsabilités, sont au courant des vulnérabilités existantes pour ainsi réduire l'impact du risque informationnel. Ceci peut être démontré par une documentation solide des responsabilités ainsi que par des mesures mises en place afin de respecter les politiques de sécurité en vigueur et les termes et conditions de leur engagement.
- La **sécurité physique et environnementale** : les contrôles à mettre en place montreront le fait que des mesures empêchant les accès non autorisés afin de prévenir les pertes, les dommages, les vols des actifs informationnels existent. Ceci se fait par la définition d'un périmètre de sécurité, des procédures de contrôle physique, et par les différentes mesures de protection contre le risque environnemental.
- Le **management des opérations et des communications** : les contrôles doivent montrer que l'exploitation des ressources est sûre et correcte. Les indicateurs le prouvant sont des documents concernant les procédures et les responsabilités ainsi que la fréquence des contrôles. D'autres contrôles à effectuer sont relatifs à la surveillance de l'utilisation des ressources, à l'existence d'un processus de sauvegarde ou de contrôle d'accès, par exemple. Les contrôles du mécanisme de **contrôle d'accès** doivent permettre de vérifier que les accès non autorisés aux informations sensibles sont bien maîtrisés (existence d'une politique de gestion des utilisateurs, des identités, des authentifications, des permissions, des priviléges ou des droits d'accès).
- La **maintenance et de développement du système de l'information** : les contrôles à mettre en place montreront le fait que la sécurité est une partie intégrante du système d'information et que les critères et les besoins en sécurité sont satisfaits. Ceci passe par des contrôles portant sur les données, les processus et sur les procédures notamment pour ce qui concerne les installations de logiciels, décourageant ainsi les modifications sans un consentement préalable des responsables de sécurité.
- La **gestion des incidents** : les contrôles à mettre en place montreront le fait que les problèmes de sécurité sont identifiés, enregistrés, communiqués et qu'une approche cohérente de gestion des incidents est mise en place. Les contrôles auront pour objet les comptes rendus des incidents, leurs causes et les failles les ayant permis, la mise en place des mécanismes et procédures, aptes à faire partager l'expérience acquise en termes d'incidents.
- La **continuité de l'activité** : les contrôles à mettre en place montreront que des mécanismes opérationnels sont présents afin de s'assurer qu'une interruption, due à un incident, aura un impact minimum. Ceci se fait par les contrôles concernant l'existence du plan de secours et du plan de continuité et de reprise des activités, des plans de tests, et de l'évaluation de l'existant au regard des besoins de conformité aux objectifs annoncés.
- La **conformité juridique** : les contrôles à mettre en place montreront le fait que les lois, les réglementations ou les obligations contractuelles mais aussi la politique

Chapitre 4 • Politique de sécurité

de sécurité et d'autres normes sont respectées. Ceci se fait en identifiant les textes auxquels l'organisation est soumise, en protégeant les différentes documentations et en informant les employés sur l'utilisation des ressources informatiques et ses conséquences.

Une organisation peut obtenir pour le niveau de sécurité de son SMSI la certification ISO 27001, mais un employé peut également obtenir une certification ISO 27001. Il existe deux labels pour un employé : « *ISO 27001 Auditor* » et « *ISO 27001 Implementor* ».

Norme ISO 27002

Cette norme révisée, en 2013, peut être vue comme une collection de bonnes pratiques concernant la sécurité de l'information sur lesquelles s'appuyer pour sécuriser un système d'information (figure 4.7).

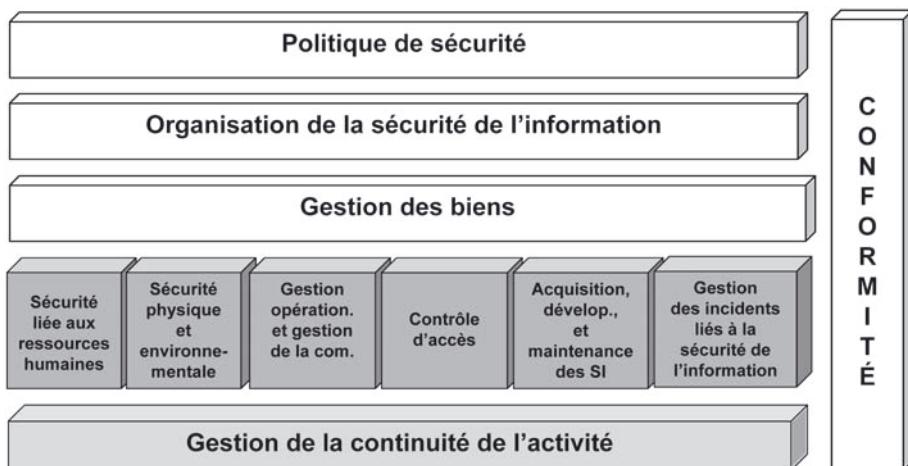


Figure 4.7 - Chapitres de la norme ISO 27002.

La norme ISO 27002 traite notamment des aspects suivants :

- **Appréciation et traitement du risque** : Qu'est-ce que la sécurité de l'information ? Pourquoi la sécurité de l'information est-elle nécessaire ? Comment établir les besoins de sécurité ?

Points forts – L'appréciation, en se basant sur une évaluation systématique de l'ampleur du risque, permet de définir de façon pertinente les actions à engager ainsi que les priorités en matière de gestion du risque. Le **traitement** permettra de décider du degré de l'acceptabilité du risque.

- **Politique de sécurité**, orientation et soutien de la direction et besoin de réexamen afin de garantir la pertinence, l'adéquation et l'efficacité de la sécurité.

4.3 • Méthodes et normes contribuant à la définition d'une politique de sécurité



Points forts - Apporter à la sécurité une orientation et un soutien de la part de la direction, conformément aux exigences métier et aux lois et règlements en vigueur. **Faire approuver** la politique de sécurité par la direction, puis la publier et la diffuser auprès de l'ensemble des salariés et des tiers concernés. **Réexaminer** régulièrement la politique de sécurité pour garantir sa pertinence, son adéquation aux besoins et son efficacité.

- **Organisation de la sécurité d'un point de vue interne et d'un point de vue externe.** Du point de vue interne, l'objectif reste la gestion de la sécurité au sein de l'organisation en établissant un cadre de gestion pour initialiser et contrôler la mise en œuvre de la sécurité. Des responsabilités doivent être assignées aux gestionnaires de l'organisation ainsi que des instances spécifiques liées à la sécurité doivent être mises en place. Du point de vue externe, l'organisation doit s'assurer que ses politiques sont respectées par les organisations externes mandatées des systèmes de l'information.



Points forts - Crédit d'une instance impliquant des représentants de tous les départements, et responsable de la sécurité des informations (le comité de sécurité) - **Définition** claire des responsabilités et des modalités d'accès aux ressources - **Externalisation** des fonctions de l'organisation.

- **Gestion des biens et des valeurs** pour mettre en place et maintenir une protection appropriée des valeurs. Ceci passe par un inventaire des biens à protéger, leur classification et leur utilisation acceptable ainsi que par l'identification des propriétaires pour chacun des biens et l'attribution des responsabilités qui leur incombent.



Points forts - Réalisation du travail d'inventaire pour indiquer les besoins, les priorités et le degré de protection requis - **Identifier** une procédure pour chaque classe d'information, un propriétaire pour chaque actif principal.

- **Aspects de sécurité liés aux ressources humaines** pour garantir que les salariés, contractants et utilisateurs connaissent leurs responsabilités, afin de réduire le risque de vol, de fraude ou de mauvais usage des ressources. Pour cela des mesures doivent être appliquées :
 - ◊ *avant le recrutement* : concernant la compréhension de la confidentialité et de la sécurité de l'information par les employés ;
 - ◊ *pendant la durée du contrat* : la politique de sécurité de l'organisation doit être enseignée aux employés et des sanctions qui pourront être prises en cas de violation doivent être explicitement présentées ;
 - ◊ *en cas de fin ou de modification de contrat* : tous les droits d'accès doivent être retirés lorsqu'une ressource humaine quitte l'organisation.



Points forts - Réalisation d'une culture de la sécurité - **Contribution** à la réduction du risque d'erreur et de mauvais usage des technologies - **Mise en place** des procédures pour le signalement des incidents et la gestion des connaissances associées.

Chapitre 4 • Politique de sécurité

- **Sécurité physique, environnementale** pour empêcher tout accès physique non autorisé, tout dommage aux locaux et systèmes de l'entreprise. Des zones sécurisées (contrôle d'accès physique et mécanismes de protection environnementale *i.e.* : feu, inondation, protection des sources énergétiques, etc.) peuvent être créées.



Points forts – Prévention des accès non autorisés – **Identification** des points de contrôle et recommandations pour la sécurité physique, la sécurité des serveurs et de leur environnement.

- **Sécurité de l'exploitation** afin d'assurer une exploitation correcte et sécurisée de l'infrastructure informatique. Cela passe entre autres par l'assignation de responsabilités, la séparation de tâches, la gestion du changement, la surveillance et le contrôle des services fournis par des tiers, la gestion des supports amovibles, la destruction des supports, le *back-up* des informations, la journalisation des événements, etc.



Points forts – Sécurisation de l'exploitation de l'information liée au réseau de télécommunication – **Assurance** d'une exploitation correcte des ressources.

- **Sécurité des communications et cryptographie** concernent les principes fondamentaux de la gestion de la sécurité des échanges et la mise en œuvre du chiffrement.



Points forts – Sécurisation des transactions et des infrastructures.



- **Contrôler les accès** à l'information en tenant compte notamment des exigences métier (besoins du business) en fonction des impératifs de l'organisation et de la politique définie.

Points forts – Gestion et contrôle de l'accès aux informations, prévention et détection des accès non autorisés, de la malveillance interne à l'organisation, des failles dues à l'interconnexion des réseaux.

- **Sécurité lors des phases d'acquisition, de développement et de maintenance** des systèmes d'information et relations avec les fournisseurs pour s'assurer que la sécurité est bien appréhendée de manière intégrée durant tout le cycle de vie des systèmes et des applications et que les divers acteurs concernés sont des vecteurs de la sécurité. Différentes facettes de sécurité y sont abordées telles que :

- ◊ l'exactitude des traitements applicatifs ;
- ◊ la validation des données saisies ;
- ◊ le contrôle du traitement interne ;
- ◊ l'intégrité des messages ;
- ◊ la politique de contrôle de l'usage de la cryptographie ;
- ◊ la gestion des clés ;

4.3 • Méthodes et normes contribuant à la définition d'une politique de sécurité

- ◊ la sécurité des fichiers systèmes ;
- ◊ le contrôle des logiciels opérationnels ;
- ◊ la gestion des vulnérabilités techniques.



Points forts – Déploiement d'infrastructures – **Validation** des données d'entrée – **Contrôle** du traitement interne – **Authentification** et validation des données de sortie – **Prise en compte** des besoins de sécurité dès la phase de conception du système d'information et des rôles des fournisseurs.

- **Gestion des incidents liés à la sécurité de l'information** pour garantir que le mode de notification des événements et des failles de sécurité permet la mise en œuvre des actions correctives dans les meilleurs délais. Cela s'appuie sur la mise en place de procédures formelles de remontée d'information et de signalement progressif. La norme préconise que des rapports précis et documentés, quant à la survenance des incidents, soient tenus à jour et que tous les problèmes soient signalés.



Points forts – Gestion des incidents et optimisation – **Documentation** pour tirer des leçons des erreurs ou des inattentions. La norme **ISO 27035 (Information Security Incident Management)**, de 2011, propose une approche structurée et des directives pour détecter, rapporter, gérer les incidents et les vulnérabilités de sécurité.

- **Gestion de la continuité** dont l'objectif est de neutraliser les interruptions des activités et de protéger les processus métiers cruciaux. Le plan de continuité doit contribuer à réduire le plus possible l'impact des risques et à récupérer les actifs organisationnels perdus à la suite d'événements majeurs. La norme spécifie quels sont les aspects sécuritaires de la gestion de la continuité et la manière de les inclure dans le processus de gestion des affaires. Les activités à entreprendre durant le cycle de vie du plan sont spécifiées en termes de développement, implémentation, planification, test, maintenance et réévaluation.



Points forts – Pérennité de l'entreprise – **Réponse rapide** aux interruptions, environnement de travail suffisant pour chaque collaborateur.

- **Appréhender les besoins de conformité.** L'objectif étant d'éviter toute violation des obligations légales, statutaires, réglementaires, contractuelles ou celle des exigences sécuritaires. Trois niveaux de conformité sont identifiés par la norme, à savoir :
 - ◊ Conformité avec les exigences légales découlant des exigences réglementaires et contractuelles qui doivent être explicitement définies pour chaque système d'information.
 - ◊ Conformité avec les politiques de sécurité et les standards garantissant que les procédures de sécurité, sous leurs responsabilités, sont en accord avec les politiques de sécurité de l'organisation.
 - ◊ Les procédures d'audit, avec la garantie que des audits réguliers sont entrepris pour assurer le respect des politiques de sécurité.



Points forts – Prise en compte de la législation nationale et le cas échéant internationale – Traçabilité et suivi des procédures.

La norme ISO 27002 constitue un véritable point de départ pour l'élaboration d'une politique de sécurité et des procédures de sa mise en œuvre, d'exploitation et de contrôle. Elle facilite l'identification et la définition des exigences de sécurité d'un environnement particulier.

Sans vouloir être exhaustif, diverses normes complètent la famille des normes ISO 27xxx, comme par exemple les suivantes :

- La norme **ISO 27010** (*Information security management for inter-sector and inter-organisational communications*) traite **du management du partage d'informations de sécurité ou sensibles entre des organisations**, par le biais de contrôles et de directives spécifiques. Cela concerne les organisations publiques ou privées, notamment celles relatives aux infrastructures critiques.
- La norme **ISO 27032** (*Guidelines for cybersecurity*) concerne principalement la cybersécurité d'un pays. Elle définit les principes de base de la cybersécurité en rappelant notamment les relations entre les différents domaines de la sécurité (sécurité de l'information, des réseaux, d'Internet, de la protection des infrastructures informationnelles critiques).
- La norme multipartie **ISO 27033** (*Network security*) couvre plusieurs domaines de la sécurité des réseaux : la partie 2 (*Guidelines for the design and implementation of network security - 2012*) concerne des directives pour la conception et l'implémentation de la sécurité réseau. Les différents documents constitutifs de la norme ISO 27033 sont :
 - ◊ *Part 1 : Overview and concepts* (2009).
 - ◊ *Part 3 : Reference networking scenarios. Threats, design techniques and control issues* (2010.)
 - ◊ *Part 4 : Securing communications between networks using security gateways* (2014).
 - ◊ *Part 5 : Securing communications across networks using Virtual Private Network (VPN)* (fin 2013).
 - ◊ *Part 6 : Securing IP network access using Wireless* (2015).

La première partie de norme **ISO 27034** existe depuis 2011 et concerne les principes généraux de la sécurité des applications et des processus de gestion de la sécurité des applications (*Application security – Part 1 : Overview and concepts*).

La norme **ISO 27037** (*Information security guidelines for identification, collection, acquisition and preservation of digital evidence*) est relative à l'**informatique forensique**, nécessaire lors de procédures et d'investigations notamment judiciaires. Elle définit le traitement de la preuve numérique par des directives pour l'identification, la collecte et la préservation des traces numériques afin que ces dernières puissent constituer des preuves recevables auprès d'un tribunal.

Les **normes ISO 13335** (lignes directrices pour la gestion de la sécurité des technologies de l'information) et **ISO 15408**, qui relèvent également de la dimension organisationnelle de la sécurité, sont des outils normatifs complémentaires à l'appréhension de la sécurité.



Il ne faut pas confondre les normes (telle l'ISO 27001) et les méthodes (comme Ebios. L'ISO 27001 ne préconise aucune méthode particulière. La méthode attachée à la norme peut être, indifféremment, par exemple Ebios ou Méhari ou une autre méthode.

4.3.3 Méthodes et bonnes pratiques

En ce qui concerne les **bonnes pratiques** qui peuvent également constituer des guides de référence permettant d'élaborer des politiques de sécurité, parmi les plus connues retenons par exemple celles éditées par :

- le CERT⁸ – *Guide to System and Network practices* ;
- le NCSA⁹ – *Guide to Enterprise Security*, qui concerne la dimension technique de l'implantation d'une politique de sécurité ;
- l'Internet Security Alliance¹⁰ – *Common Sense Guide for Senior Manager* ;
- l'Information Security Forum¹¹ – *The Standard of Good Practice for Information Security*.



Une norme ou une méthode peut contribuer à définir une politique de sécurité. Savoir en tirer parti en fonction d'un contexte d'entreprise particulier dépend de la compétence des personnes qui les appliquent.

Quelles que soient la norme et la méthode retenues, il est important de pouvoir les **adapter au contexte** auquel elles s'appliquent (tableau 4.1). En tout état de cause, ce doit être un soutien à l'appréhension et l'appréciation des risques encourus. La pertinence d'une politique de sécurité est fonction de la qualité de l'analyse des risques effectuée dans le cadre de l'analyse de l'existant. Les grands cabinets de conseils ont défini leur propre méthode en s'inspirant le plus souvent des normes et des méthodes existantes. La méthode **OCTAVE** (*Operationally Critical Threat, Asset and Vulnerability Evaluation*)¹², élaborée à l'université de Carnegie Mellon, est également adoptée voire adaptée par divers cabinets de consultants en politique de sécurité.

8. <http://www.cert.org>
9. <http://www.ncsa.edu>
10. <http://www.isalliance.org>
11. <http://isfsecuritystandard.com>
12. www.cert.org/octave/

Tableau 4.1 - Avantages et inconvénients de l'utilisation d'une méthode pour définir une politique de sécurité.

Avantages	Inconvénients
<p>Gain en termes d'efficacité en réutilisant le savoir-faire transmis par la méthode. Capitalisation des expériences.</p> <p>Langage commun, référentiel d'actions, structuration de la démarche, approche exhaustive.</p> <p>Être associé à des groupes d'intérêts. Partage d'expérience, de documentation, formation possible.</p>	<p>Bien qu'elles puissent faire l'objet de révision (nouvelles versions), les normes ou les méthodes n'évoluent pas au même rythme que les besoins ou les technologies.</p> <p>Une norme ou une méthode est générale. Il faut savoir la spécifier en fonction de besoins particuliers de l'organisation.</p> <p>Prolifération des méthodes : difficulté de choix.</p> <p>Disposer des compétences nécessaires. Efforts financiers, durée, coûts. Difficultés à maîtriser la démarche qui peut s'avérer lourde et nécessiter des compétences externes.</p>

4.3.4 Modèle formel de politique de sécurité

Différents modèles ont été proposés par la communauté scientifique pour spécifier et exprimer de manière formelle et non ambiguë des politiques de sécurité. Ils permettent une présentation abstraite des principes de sécurité à prendre en compte. Parmi les plus anciens, mentionnons :

- **le modèle de Bell-LaPadula¹³** : modèle des exigences de contrôle d'accès à des informations classifiées d'une politique de sécurité pour la confidentialité ;
- **le modèle de Clark et Wilson¹⁴** relatif à l'intégrité de l'information pour des environnements commerciaux ou industriels ;
- **le modèle de Brewer-Nash¹⁵** concernant l'exigence de contrôle d'accès visant à assurer la confidentialité pour le client.

4.4 DE LA POLITIQUE AUX MESURES DE SÉCURITÉ

4.4.1 Classification des ressources

La réalisation d'un inventaire complet et précis de tous les acteurs et intervenants de la chaîne sécuritaire contribue à une meilleure connaissance de l'environnement à

13. MITRE Technical Report 2547, Volume I “Secure Computer Systems: Mathematical Foundations” by D. Elliott Bell and Leonard J. LaPadula dated 1 March 1973.

14. Modèle de Clark et Wilson — D.D. Clark. and D.R. Wilson, « A comparison of commercial & military Security policies » Proc. of the IEEE Symposium on Security and Privacy, pages 184-194, April 1987.

15. Modèle de Brewer-Nash — Brewer, D.F.C and Nash, M.J., « The Chinese Wall Security Policy » IEEE Symposium on Security and Privacy, 215-228 (1989).

protéger – « *On ne peut sécuriser que ce que l'on connaît et que l'on gère !* ». C'est dans les phases d'analyse de l'existant et des risques que ces données d'inventaire prennent toute leur importance. Elles interviennent également dans la phase d'identification des valeurs et de classification des ressources pour déterminer leur **degré de sensibilité** (ou **degré de criticité**). Plus la ressource possède de la valeur, plus elle est sensible et plus les conséquences d'un défaut de sécurité sont graves pour l'organisation.

Chaque ressource peut être perçue comme une cible de sécurité pour laquelle il faut identifier les risques et des scénarios de risques combinés, les mécanismes de sécurité inhérents et applicables, ainsi que les contraintes techniques, financières et organisationnelles afin de déterminer la faisabilité de la politique de sécurité pour chaque cible de sécurité. La **classification** des ressources à protéger, selon leur degré d'importance, est nécessaire pour fixer les priorités des actions de sécurité à réaliser. Elle est donc indispensable à l'élaboration de la politique de sécurité et à la définition des mesures et des procédures. De plus, c'est en fonction du degré de sensibilité des données et du profil des utilisateurs que l'on attribuera à ces derniers, des permissions et droits d'accès, et qu'on chiffrera ou pas les données stockées ou transmises.

Déterminer le degré de sensibilité des données consiste tout d'abord à **identifier des classes génériques de données** auxquelles on associe des valeurs entières définissant leur degré de sensibilité. Cela permet de disposer d'une métrique, dont l'échelle des valeurs est déterminée par l'organisation et qui reflète le degré de sensibilité de la donnée pour celle-ci. Ainsi, par exemple, pour une entreprise les données peuvent être classées :

- **publiques** – non sensible : degré de sensibilité 0 ;
- **privées** – diffusion limitée : degré de sensibilité 1 ;
- **confidentielles** : degré de sensibilité 2 ;
- **secrètes** : degré de sensibilité 3.

La classification, qui doit être adaptée en fonction des besoins, étant effectuée, des règles de protection et d'usage doivent être assignées pour une durée précise.

4.4.2 Mesures de sécurité

Les **mesures de sécurité** se distinguent en fonction de ce sur quoi elles portent (sécurité physique, sécurité environnementale, sécurité logique, sécurité des systèmes, réseaux, données et programmes) et selon leur nature. Il peut s'agir :

- de mesures procédurales et managériales (procédures de gestion, de surveillance, d'évaluation, de mises à jour, de sauvegarde, de secours, d'exploitation, de gestion des ressources humaines, etc.) ;
- d'outils technologiques matériels ou logiciels (protocoles cryptographiques, système pare-feu, système de filtrage, de contrôle d'accès...) ;
- de compétences humaines.

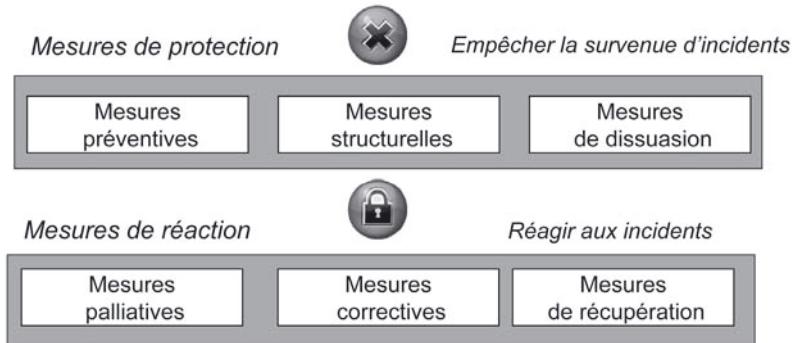


Figure 4.8 - Typologie des mesures de sécurité.

Comme le montre la figure 4.8, plusieurs types génériques de mesures de sécurité existent.

Les **mesures préventives** servent de barrière afin d’empêcher la réalisation d’incidents, d’une malveillance ou d’une erreur (procédures de contrôles d’accès physique et logique, détection de virus, etc.).

Les **mesures structurelles** agissent sur la structure, l’architecture, l’organisation du système d’information (cloisonnement d’environnements, redondances, fragmentation de l’information, par exemple afin de réduire la vulnérabilité des ressources par exemple).

Les **mesures de dissuasion** autorisent une prévention en décourageant les agresseurs de mettre à exécution une menace (procédures juridiques et administratives touchant à la sensibilisation et à la gestion des ressources humaines, aux conditions de travail ou aux moyens de détection et de traçage, etc.).

Les **mesures de protection** ont pour objectifs de renforcer la sécurité et la robustesse des ressources et de diminuer les détériorations consécutives à la réalisation d’une menace (*via* des contrôles de cohérence, des détecteurs d’intrusion, d’incendie, d’humidité, d’erreurs de transmission, et des structures coupe-feu pour se protéger des agressions ou en limiter l’ampleur par exemple).

Les **mesures palliatives** ou **correctives**, telles que les sauvegardes, les plans de continuité, les redondances, les réparations ou corrections par exemple, contribuent à pallier ou à réparer les dégâts engendrés par un incident et permettent la continuité des activités.

Les **mesures de récupération** autorisent un retour à un fonctionnement normal et limitent les pertes consécutives à un sinistre, et réduisent le préjudice subi par un transfert des pertes sur des tiers (assurance) ou par attribution de dommages et intérêts consécutifs à des actions en justice.

4.5 CONTINUITÉ DES SERVICES, DES ACTIVITÉS ET GESTION DE CRISES

4.5.1 Définitions et objectifs

Pour limiter les dommages consécutifs à un incident qui n'a pu être évité, malgré les mesures de prévention et de protection, il faut au préalable avoir planifié les différentes activités et procédures qui seront prises.

Le **plan de continuité** permet l'identification des activités et des fonctions critiques de l'organisation, pour définir les politiques et les mesures afin d'assurer la continuité des affaires.

Le **plan de continuité d'activité** a pour objet de minimiser l'impact des sinistres touchant les processus métiers de l'entreprise, assurer leur fonctionnement et permettre le retour dans la normalité. Il a pour objectif de neutraliser les interruptions des activités de l'organisme, de protéger les processus métiers cruciaux des effets causés par les principales défaillances des systèmes d'information ou par des sinistres pour garantir une reprise de ces processus dans les meilleurs délais.

Le **plan de reprise d'activité**, qui comprend la gestion de crise, va guider l'organisation après un sinistre afin de pouvoir rétablir les fonctions et activités critiques dans un laps de temps le plus court possible avec un minimum de perte.

Les objectifs de ces plans impliquent :

- la minimisation de la probabilité d'occurrence, des dommages après sinistre, celle de la responsabilité civile envers des tiers, des effets de l'interdépendance de quelque nature et des coûts d'assurance ;
- la conformité avec les règlements et lois en vigueur.

Pour atteindre ces objectifs, l'organisation doit connaître ses ressources, ainsi que leurs besoins en matière de délai de redémarrage des activités. Il faut pour cela par exemple connaître et déterminer notamment les points suivants :

- la durée maximale d'interruption admissible ;
- les pertes des données maximales admissibles ;
- les procédures de substitution et de rattrapage ;
- les montants des impacts financiers.



La norme ISO 22301 (*Societal Security Business Continuity Management System Requirements*), publiée en 2012, spécifie les exigences pour planifier, établir, implémenter, opérer, surveiller, évaluer, maintenir et optimiser un système de management de reprise après incident et de continuité.

4.5.2 Démarche de déploiement d'un plan de continuité

Les principaux éléments clés du **déploiement** d'un plan de continuité sont les suivants :

- identifier et hiérarchiser les risques et les processus métiers cruciaux, ainsi que les systèmes et applications qui supportent ces derniers ;

- analyser l'impact probable des interruptions (de l'impact le plus faible jusqu'au plus fort) ;
- souscrire éventuellement une assurance ;
- définir la mise en œuvre des mesures préventives ;
- identifier les ressources financières, organisationnelles, techniques et environnementales suffisantes pour satisfaire les exigences de sécurité ;
- assurer la sécurité du personnel et garantir la protection des moyens de traitement de l'information et des actifs matériels ;
- documenter les plans de continuité de l'activité satisfaisant aux exigences de sécurité ;
- tester et mettre à jour de façon régulière les plans et processus mis en place ;
- intégrer le plan de continuité aux processus et à la structure de l'organisation ;
- attribuer des responsabilités concernant le processus de gestion du plan de continuité.



C'est pendant les périodes de crises et de prise de décision rapide que les contrôles internes ont tendance à être contournés ou oubliés et que les critères de sécurité ne sont pas toujours respectés.

Dans un plan de continuité, les **impacts** sont considérés comme étant des pertes ou des modifications de l'état initial (ou prévu) des critères de sécurité liés aux actifs informationnels (disponibilité, confidentialité, intégrité, efficience, effectivité, fiabilité, conformité, etc.). Ces impacts peuvent être regroupés en :

- **impacts financiers** (baisse de la valeur des actions, perte de clients ou d'actifs financiers, coûts élevés de refinancement ou de remplacement, amendes contractuelles...) ;
- **impacts opérationnels** (interruption de la production, des ventes et/ou des livraisons, augmentation des délais de paiement ou d'achat, réduction de la qualité...) ;
- **impacts intangibles** (très difficiles à évaluer et à monnayer comme par exemple la baisse du niveau de satisfaction des clients, la perte de confiance et de réputation, la perte de motivation ou d'avantages concurrentiels...).

Pour pouvoir évaluer des incidents, il faut d'abord les catégoriser selon une échelle propre à l'entreprise, exprimant la satisfaction des exigences individuelles en matière de sécurité. Ainsi par exemple, une échelle de classification des incidents pourrait être de quatre niveaux : négligeable, mineur, majeur et critique.

4.5.3 Plans de continuité et de reprise

Après avoir identifié les **activités critiques de l'entreprise**, une analyse des impacts après sinistre sur les processus et les actifs les supportant est réalisée pour identifier les plans d'urgence pour la continuité, la reprise des activités et la remise en état des infrastructures les supportant (figure 4.9).

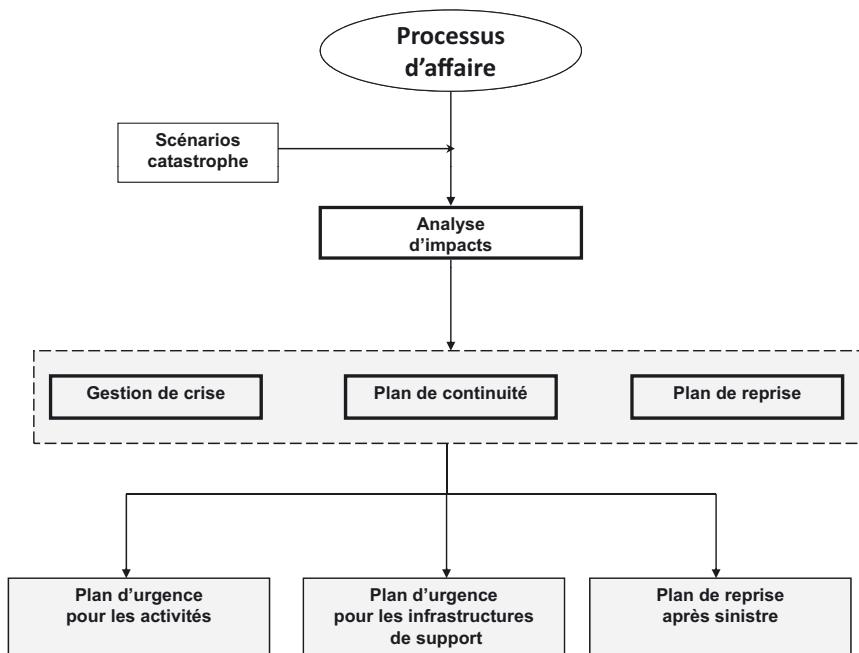


Figure 4.9 – Gestion de crise et plans de continuité, de reprise et d'urgence.

Cette analyse des impacts reprend les catégories précédemment énoncées, en prenant en compte les éléments suivants par ordre de priorité :

- les menaces contre les personnes ;
- la perte des données importantes ;
- l'interruption des opérations ;
- la non-conformité ;
- les dommages en termes de réputation.

L'établissement d'un plan de continuité requiert une planification rigoureuse du temps, des ressources à déployer et des objectifs à atteindre, et répond à trois principales questions :

- Quels sont les processus et les activités supportant les affaires ?
- Quelles sont les ressources critiques liées aux processus critiques ?
- Quel est le temps de dépannage critique à disposition ?

Le plan de continuité implique une priorisation des processus de la part des instances de gestion, mais aussi l'identification du **délai de fraîcheur** (figure 4.10).



Le **délai de fraîcheur** comprend la fréquence des sauvegardes en fonction des exigences en termes de perte de données maximale acceptable.

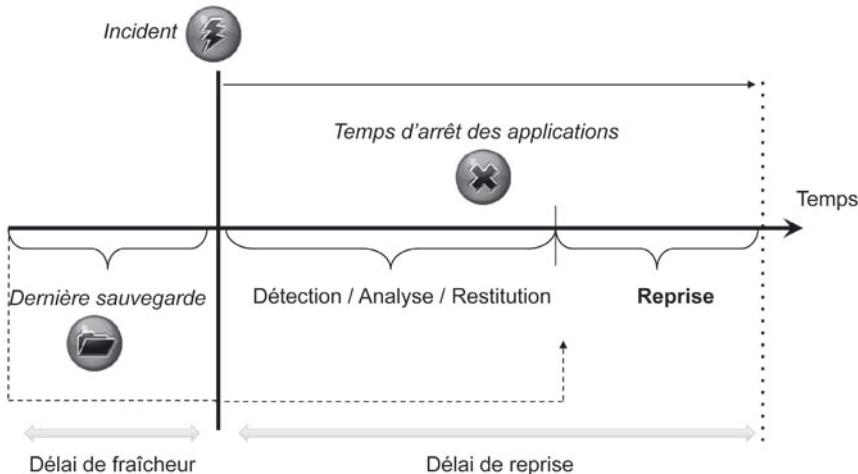


Figure 4.10 – Notions de délais de fraîcheur et de reprise.

Le délai de reprise est le temps maximal requis pour reprendre les activités à 100 % des capacités.



La stratégie de sauvegarde des données constitue la pierre angulaire d'un plan de continuité et de reprise car elle va permettre d'assurer le critère de disponibilité.



Différents types de sauvegarde existent, à savoir :

- la sauvegarde complète, qui est une copie exhaustive des données ;
- la sauvegarde incrémentale, qui est une sauvegarde de tous les éléments modifiés ;
- la sauvegarde différentielle, qui sauvegarde les fichiers modifiés après une sauvegarde complète ;
- la journalisation, qui crée un journal de toutes les modifications concernant un seul fichier.

Le choix du type de sauvegarde (ou d'une combinaison de types) est basé sur plusieurs facteurs relatifs à l'importance des données, à la quantité et aux taux de modifications des données, au volume de données à copier et à stocker à chaque reprise, et au temps nécessaire pour effectuer une sauvegarde.



Pour être valide, une stratégie de secours doit être testée régulièrement. Elle doit également être évolutive et robuste aux changements et répondre au principe « KISS – Keep It Short and Simple ».

Afin d'assurer que le plan de continuité et le plan de reprise en place sont conformes aux objectifs de l'organisation en termes de sécurité et de pérennité, un **audit** doit être prévu de manière régulière éclaircissant les points suivants :

- comprendre et évaluer la stratégie ;
- évaluer le plan en le comparant avec des standards et des régulations ;
- vérifier que le plan est effectif en analysant les résultats des tests ;
- évaluer l'adéquation des locaux d'archivage extra-entreprise ;
- évaluer la capacité de réponse de l'utilisateur final ;
- vérifier que la procédure du maintien des plans existe et est effective ;
- vérifier que les manuels sont rédigés d'une manière simple et conviviale.

4.5.4 Dispositifs de secours et plan de secours

Les **dispositifs de secours** nécessaires doivent être décidés lors de la phase de la conception du plan de continuité afin de garantir la **disponibilité des ressources critiques** au système d'information pour son bon fonctionnement, même en cas de sinistre. Les dispositifs de secours les plus courants comprennent :

- la mobilisation des ressources nécessaires ;
- le secours des équipements informatiques et télécoms ;
- le secours de la téléphonie ;
- la reprise des traitements ;
- la logistique ;
- le relogement ;
- la reprise des activités des services utilisateurs ;
- la communication de la crise ;
- les dispositifs de post-reprise.

Ces dispositifs doivent être conçus, utilisés et mis en œuvre en équilibrant les coûts engendrés par les solutions de reprise avec les coûts du sinistre (figure 4.11).

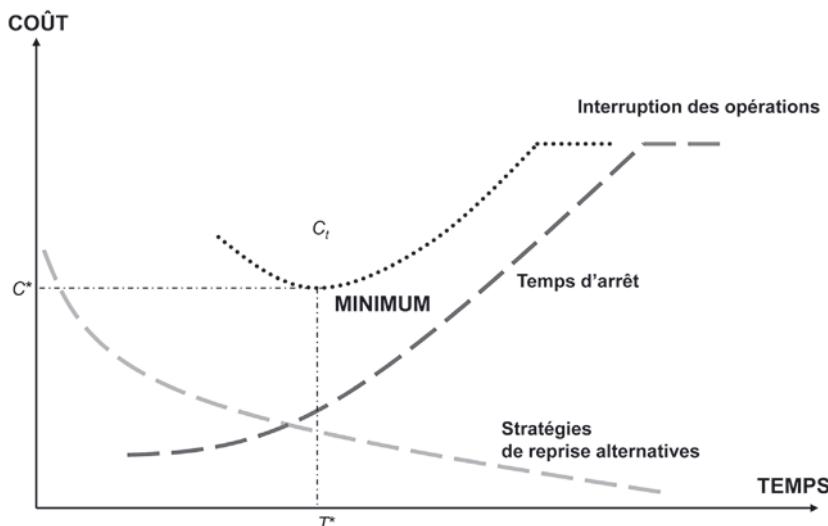


Figure 4.11 - Coût d'interruption et coût de reprise.

Le choix de la stratégie de secours dépendra des variables telles que les délais de fraîcheur et de reprise.

Les stratégies de moyens de secours comprennent des :

- **salle blanche (cold site)** – infrastructure distante équipée pour accueillir des installations informatiques ;
- **salle orange (warm site)** – salle pour accueillir des installations informatiques et qui est partiellement équipée de matériel informatique ;
- **salle rouge (hot site)** – salle dite *latente* qui abrite un ensemble d'équipements informatiques tenus en état de marche avec un personnel dédié en permanence ;
- **salle mobile (mobile site)** – salle réalisée *via* des camions ou des logements mobiles ;
- **salle miroir (mirrored site)** – salle assurant une redondance parfaite et fidèle de l'environnement opérationnel.

Des considérations budgétaires entrent toujours en jeu lors du choix de la stratégie. Il existe des écarts importants de coûts entre la location d'une salle blanche partagée et une salle miroir vers laquelle la production peut être commutée d'un moment à l'autre.



Un **plan de secours** est un dispositif organisationnel et technique qui permet d'assurer un fonctionnement minimal des applications critiques après la survenue d'un sinistre.

Le plan de secours définit une stratégie de reprise en identifiant notamment :

- le temps minimal écoulé entre un dommage et la reprise d'un fonctionnement normal (notion de durée critique) ;
- les événements et les actions pour mener à bien la reprise (synchronisation, répartition des actions, déclaration du sinistre auprès des assurances, identification des dépenses exceptionnelles).

Les éléments constitutifs d'un plan de secours sont résumés par la figure 4.12.

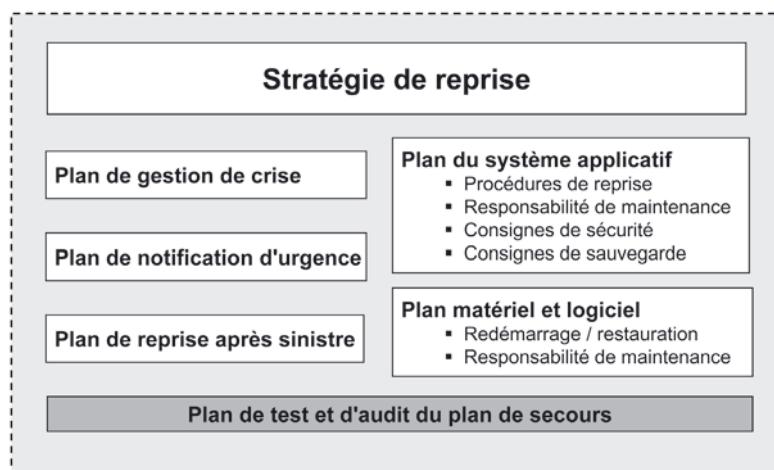


Figure 4.12 – Éléments constitutifs d'un plan de secours.

La définition et l'établissement d'un plan de secours doivent être gérés comme un **projet** à part entière et suivre une démarche courante de gestion de projet. Il est recommandé en outre de suivre une méthodologie de conception de plan de secours afin de systématiser et de mieux maîtriser les différentes étapes de la mise en place d'un tel projet.

La figure 4.13 identifie les quatre phases constitutives d'un plan de secours.

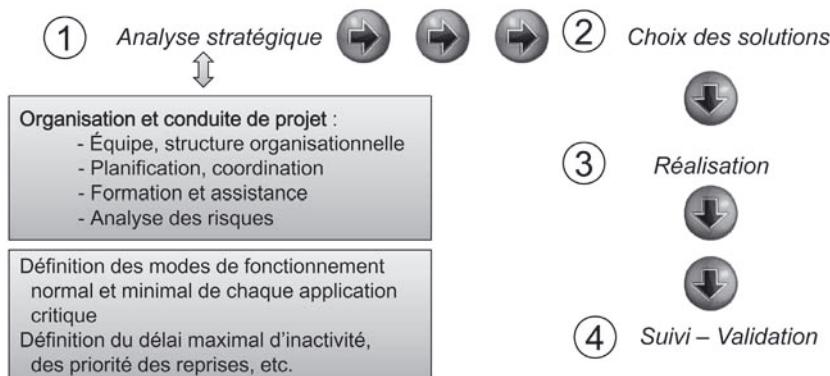


Figure 4.13 – Les quatre phases de réalisation d'un plan de secours.

Phase 1 – Analyse stratégique

L'**analyse stratégique** est le point de départ de la définition d'un plan de secours (phase 1). Elle se structure autour de quatre tâches principales :

- **Tâche 1 – Organisation et conduite de projet** dont les objectifs sont :
 - ◊ *identification d'une équipe et d'une structure organisationnelle* : le chef de projet doit avoir une responsabilité centralisée, une visibilité élargie, ainsi que l'autorité appropriée ; il rend compte à la direction ;
 - ◊ *planification* : coordination, organisation de la mise en œuvre, de la mise à jour du plan de secours ;
 - ◊ *formation et assistance* des personnes chargées du plan de secours.
- **Tâche 2 – Analyse des risques** pour :
 - ◊ *l'évaluation des risques* ;
 - ◊ *la définition des sinistres potentiels*.
- **Tâche 3 – Analyse d'impact** contribuant à :
 - ◊ *l'identification des critères de fragilité et de sensibilité* aux risques des applications ;
 - ◊ *l'analyse des conséquences* des différentes pannes, erreurs, dysfonctionnements sur les activités de l'entreprise ;
 - ◊ *l'évaluation des impacts stratégiques et tactiques*.
- **Tâche 4 – Définition des modes de fonctionnement normal et minimal de chaque application critique** afin de définir :
 - ◊ *le délai maximal d'inactivité toléré* ;

- ◊ les *consignes opérationnelles* ;
- ◊ les *priorités de restauration* des applications critiques ;
- ◊ les *procédures de reprise* ;
- ◊ les *exigences de planification*.

Phase 2 – Analyse des solutions

La phase 2, qui est l'étape méthodologique d'**analyse des solutions**, a pour objet d'identifier et d'évaluer les différentes solutions de reprise possibles et de choisir la meilleure en fonction des critères stratégiques de l'entreprise. C'est à ce stade que l'on procède à la rédaction des documents définitifs.

Phase 3 – Mise en œuvre opérationnelle

La phase 3 de **mise en œuvre opérationnelle** de la stratégie de secours passe par une attribution des responsabilités, la sensibilisation et la formation des personnes responsables de l'exécution des procédures de reprise. Une documentation complète du plan de secours doit être également établie.

Phase 4 – Validation et suivi

La phase 4 de **validation** et de **suivi** permet de tester le plan, son efficacité par des simulations d'alertes et la réalisation de tests de bascule programmés du site de production vers le site de secours, de documenter et d'analyser les résultats de ces tests afin d'obtenir un certain niveau de fiabilité et de sûreté de fonctionnement du plan de secours. Il doit également être mis à jour en fonction des événements, du changement de personnel, des modifications des applications et fait partie ainsi de la gestion opérationnelle quotidienne du site de production.

L'**audit d'un plan de secours**, qui peut ou non faire partie de la phase de validation et de suivi, a pour objet de déterminer la qualité du plan établi. Pour cela, on identifie les domaines sensibles de l'entreprise pour lesquels le plan de secours doit s'appliquer et on évalue les dispositions, procédures, tâches et actions prévues par le plan en cas de sinistre puis on élabore des recommandations.

4.5.5 Plan d'action

Un **plan d'action proactif** et **réactif** pour se protéger et contrer les incidents doit être défini dans la politique de sécurité. Il s'appuie le plus souvent sur la mise en œuvre d'un **plan de secours**. Ce plan d'action-réaction se décline en :

- **mesures préventives** (mesures de sauvegarde des données vitales, de surveillance, de contrôle, d'audit actif, etc.) ;
- **mesures de dissuasion** (notification de l'enregistrement des actions et événements, des poursuites encourues, des plaintes déposées auprès de la police, etc.) ;
- **mesures structurelles** (organisation et responsabilité) ;
- **mesures de protection** (procédures de contrôle d'accès, certification, chiffrement, preuve de l'origine, filtrage, cloisonnement des environnements, etc.) ;

- **mesures de constat et de notification** (enregistrement des actions malveillantes, constat et preuve de l'infraction, information aux dirigeants et aux acteurs touchés par l'infraction, etc.) ;
- **mesures de récupération** (secours, sauvegarde, restitution, retour au contexte initial, etc.) ;
- **mesures judiciaires** (marche à suivre pour porter plainte et poursuivre les fraudeurs).

4.6 PLACE DE L'AUDIT DES SYSTÈMES D'INFORMATION EN MATIÈRE DE SÉCURITÉ

4.6.1 Audit des systèmes d'information

Un **processus général d'audit** répond à l'objectif principal qui est de permettre à l'auditeur d'exprimer une opinion selon laquelle les états financiers ont été établis, dans tous leurs aspects significatifs, conformément à un référentiel comptable identifié. L'audit concerne en premier lieu le système de **contrôle interne** de l'entreprise qui est l'ensemble des principes et procédures prescrits par la direction d'une entreprise, servant à garantir une gestion des affaires correcte et efficace (y compris le respect des principes édictés par la direction de l'entreprise) en matière de :

- protection des actifs ;
- détection et empêchement des fraudes et des erreurs ;
- assurance de l'exactitude et de l'intégralité des enregistrements comptables ;
- compilation en temps utile et dans la mesure du possible, des informations financières fiables.

Ainsi, l'**audit d'un système d'information**, qui intègre celui de sa sécurité, contribue à satisfaire ce même objectif. Un audit de systèmes d'information vise à collecter des **preuves** qui permettent d'attester d'une part que les systèmes et ressources protègent les actifs informationnels de l'organisation et d'autre part, que les différents risques inhérents au système d'information sont pris en compte. Cela contribue à pouvoir formuler une **assurance raisonnable** concernant :

- l'intégrité et la fiabilité des systèmes et des informations ;
- l'utilisation efficiente des ressources ;
- l'atteinte des objectifs organisationnels en fonction du niveau de qualité de contrôles internes.

D'une manière générale, les **contrôles principaux** à prendre en compte dans le cadre d'un audit de système d'information sont :

- l'environnement de direction et de supervision ;
- les procédures de gestion de changement ;
- le cycle de vie des systèmes ;
- les politiques de sécurité ;
- la gestion des incidents ;

- les supports techniques ;
- les standards, politiques et procédures de configuration, installation, tests ;
- le plan de continuité de l'activité.

Un audit de système d'information se déroule généralement en huit étapes :

- analyse du bilan et du compte de résultats ;
- identification des processus métiers et des flux de traitement des données ;
- identification des applications de base et des principales interfaces IT pertinentes ;
- identification des risques et des contrôles clés ;
- vérification de la cohérence et de la fiabilité par des tests de cheminement (*walk-trough audit test*) qui vérifient toutes les étapes par lesquelles un processus passe ;
- évaluation de la conception des contrôles ;
- évaluation du fonctionnement des contrôles ;
- appréciation globale.

4.6.2 Référentiel CobiT

L'ISACA¹⁶ (*Information Systems Audit and Control Association*) diffuse, pour la gouvernance et l'audit des systèmes d'information, la méthode **CobiT** (*Control objectives for information and Technology*). Cette dernière peut être considérée comme un outil de support à l'optimisation des politiques, des mesures et des procédures de gestion des systèmes d'information pour la gouvernance des technologies de l'information. L'objectif étant de contribuer à l'**optimisation des processus de création de valeurs** (et de réalisation des profits) tout en optimisant les coûts et les risques d'une organisation (démarche d'amélioration).

CobiT propose un cadre de référence des meilleures pratiques en termes d'audit des systèmes d'information (figure 4.14). Cela contribue à aider le management à établir des liens entre les risques métiers, les besoins de contrôle et les problématiques techniques. Depuis 1996, CobiT a connu plusieurs mises à jour. La version 5 a été publiée en 2012.

La méthode est structurée autour des principaux domaines d'activité liés à l'exploitation de l'informatique (planification, construction, exécution, évaluation/validation et métrologie), de 37 processus clés avec plus de 200 objectifs de contrôle. Chaque élément est conçu afin de permettre aux responsables des systèmes d'information de s'assurer que les risques significatifs ont été identifiés et que des mesures de contrôle appropriées et fiables ont été mises en place, le tout dans un contexte d'évaluation et de réévaluation permanente.

CobiT 5 insiste sur la distinction entre la gouvernance et la gestion de l'informatique. Dans le cadre de la gouvernance, trois activités clés sont identifiées : l'évalua-

16. L'**ISACA** (*Information Systems Audit and Control Association*, www.isaca.org), sous le patronage de l'*IT Gouvernance Institute* (ITGI ; www.itgi.org), est une association indépendante active dans 160 pays. L'**AFAI** (Association Française de l'Audit et du conseil Informatique, www.afai.asso.fr) est la branche française de l'ISACA.

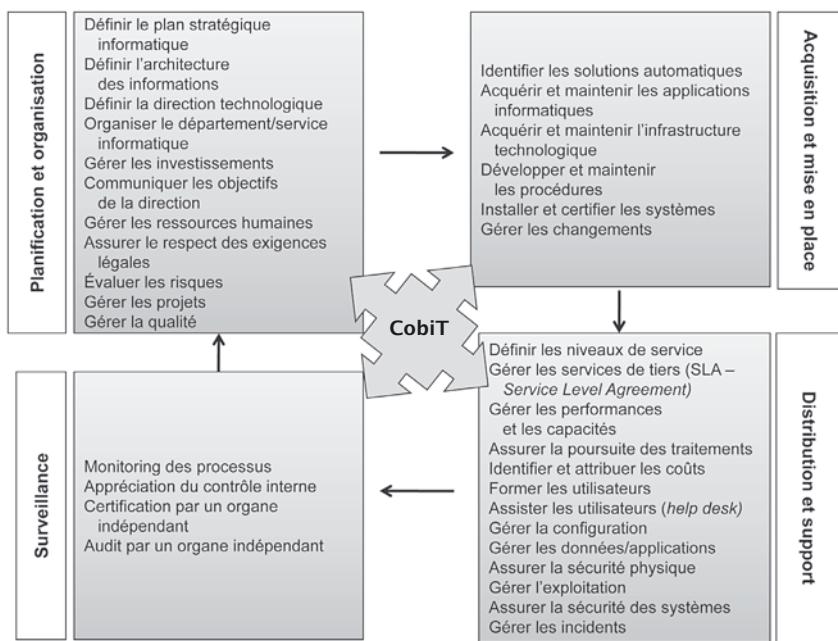


Figure 4.14 – Quelques éléments de la méthode CobiT.

tion de besoins et contraintes afin de fixer des objectifs réalistes et fiables ; le pilotage par priorité et prise de décision ; et la surveillance de performance et de conformité par rapport à des objectifs et directions définis à l'avance. Dans le cadre de la gestion, qui est plus tactique et opérationnelle, la direction de l'organisation planifie, implémente, gère et surveille les activités de l'organisation en conformité avec les objectifs globaux de celle-ci.

 La **norme ISO 38500** de 2015 (*Corporate Governance of Information Technology*) propose des principes généraux pour un usage efficace et efficient des technologies de l'information et la **gouvernance** des processus de gestion des services ICT utilisés dans une organisation.

4.7 MESURER L'EFFICACITÉ DE LA SÉCURITÉ

4.7.1 Métriques de sécurité

La notion de métrique est définie comme un outil pour **faciliter la prise de décision** et **améliorer la performance** des systèmes sur lesquels elle s'applique.



Les métriques sont des éléments caractéristiques, observables et mesurables d'un système. Ils peuvent être de nature qualitative ou quantitative.

Ils sont à considérer comme des **paramètres de référence** dont les valeurs tangibles permettent l'appréciation des systèmes observés. Leur variation reflète la dynamique du système. Leur analyse peut servir à valider leur conformité par rapport à une situation, à un objectif ou encore à des valeurs normées.

Les **métriques** peuvent être imposées par des lois, des réglementations ou encore par des contraintes spécifiques. Ainsi, par exemple, le gouvernement fédéral des États-Unis exige que des métriques fassent partie des programmes de sécurité informatique d'une agence gouvernementale¹⁷.

Les métriques en sécurité informatique peuvent être par exemple utilisées pour atteindre les objectifs suivants :

- établir un niveau de référence pour une surveillance et une amélioration continues du niveau de sécurité d'une organisation ;
- contribuer à la définition des niveaux de sécurité à atteindre, au suivi, à l'évaluation, à la validation et à l'optimisation des mesures de sécurité ;
- contribuer à l'amélioration des pratiques de sécurité existantes et à l'intégration de la sécurité dans les processus business ;
- contribuer à ce que des problèmes techniques puissent être appréhendés au niveau managérial ;
- justifier les budgets liés à la sécurité ;
- etc.

Il est du ressort des organisations de développer et de collecter des informations pour constituer leurs métriques¹⁸. Cela peut être effectué par des mesures d'implémentation d'une politique de sécurité, des résultats des services de sécurité délivrés sur l'impact des mesures de sécurité sur les processus métiers pour ne citer que quelques exemples. Les métriques de sécurité se classifient selon leur finalité et usage pour contribuer à :

- l'analyse des risques, l'estimation de la probabilité des intrusions, leurs conséquences et impacts ;
- la certification des systèmes en classes (niveau de sécurité) selon les caractéristiques et mécanismes de sécurité ;
- la mesure de l'effort requis pour s'introduire dans un système informatique (en termes de compétences, ressources, temps...), ce qui contribue à déterminer indirectement le niveau de résistance aux attaques (difficulté à s'introduire, robustesse des systèmes) ;
- l'audit et l'évaluation du niveau de sécurité.

Selon le NIST, cinq niveaux peuvent servir de base à la définition de métrique de sécurité¹⁹ :

17. Cf. *Clinger-Cohen Act*, *Government Performance and Results Act* (GPRA), *Government Paperwork Elimination Act* (GPEA), and *Federal Information Security Management Act* (FISMA).

18. Les normes internationales traitant de la sécurité informatique, notamment les normes ISO 27001, ISO 27002 et ISO 15408, contribuent à pouvoir définir des métriques de sécurité pour les organisations.

- avoir défini des politiques de sécurité ;
- avoir défini des procédures de sécurité détaillées ;
- implémenter ces procédures ;
- tester la conformité et l'efficience de ces procédures ;
- intégrer des politiques et des procédures dans les opérations quotidiennes.



L'utilisation des métriques de sécurité peut apporter des avantages organisationnels ou financiers pour l'organisation qui les maîtrise et confirme que l'organisation possède une **attitude sécuritaire proactive**.

En utilisant les métriques, le management peut localiser les contrôles techniques, opérationnels ou managériaux et évaluer s'ils sont implantés d'une manière correcte ou non. Ainsi, l'observation de la valeur des métriques permet d'isoler les problèmes pour y remédier. De plus, les métriques constituent souvent un levier pour libérer les fonds nécessaires, auprès du management décisionnel, pour réaliser l'investissement nécessaire à la sécurité. Les métriques mesurant la **performance** peuvent se classifier en deux groupes :

- métriques **d'efficacité**, pour évaluer jusqu'à quel degré les objectifs sont atteints ;
- métriques **d'efficience**, qui permettent d'évaluer la proportionnalité entre les résultats obtenus et les ressources impliquées par rapport à l'atteinte des objectifs fixés.

L'usage de métriques de sécurité permet également de vérifier et d'attester, que les activités de l'organisation sont en accord avec les lois applicables (notion de conformité juridique). Ils peuvent aussi constituer un référentiel commun entre un assureur et une organisation pour l'établissement de **contrats d'assurance** de son système d'information, en proposant des assurances en adéquation aux niveaux de sécurité des ressources.

4.7.2 Modèle de maturité

Un **modèle de maturité** permet de décrire l'état d'un système pour le mesurer, en fonction de certaines caractéristiques ou d'objectifs à atteindre. Ainsi, les métriques de sécurité sont regroupées pour pouvoir donner lieu à une **échelle** indiquant le niveau auquel, compte tenu des critères choisis, se trouve le système étudié. Les éléments les plus importants d'un modèle de maturité sont :

- les niveaux prédéfinis ;
- les éléments explicatifs et mesurables décrivant chaque niveau.

Les modèles de maturité peuvent être exigés et/ou utilisés pour **différentes finalités**, à savoir :

- pour définir des objectifs tangibles, compréhensibles et clairs quant aux aspects de la sécurité à traiter, de la manière de les regrouper et de les gérer ;

- pour contrôler l'efficacité de la sécurité. Une fois l'étalement décidé, il est possible de situer l'état actuel de la sécurité de l'information par rapport à un état désiré ;
- pour constituer une échelle de comparaison entre des organisations ;
- pour prioriser les actions à entreprendre pour l'optimisation ou l'évolution du système.



En général un modèle de maturité contribue à évaluer la qualité de l'architecture, du déploiement, de l'efficience et de l'effectivité, ainsi que la viabilité des processus de sécurité.

Le modèle « *Information Security Management Maturity Model* » du consortium ISM²⁰ structure le concept de management de la sécurité en quatre catégories de processus, à savoir :

- général (audit des SI et des processus business) ;
- gestion stratégique (ressources allouées à la sécurité) ;
- gestion tactique (définition des objectifs de sécurité) ;
- gestion opérationnelle (gestion des sauvegardes).

Il identifie également cinq niveaux d'appréhension de gestion de la sécurité :

- **Indéfini** – investissements minimes de sécurité dans les processus essentiels. Les processus sont utilisés mais pas définis formellement.
- **Défini** – les objectifs de sécurité essentiels sont définis (entreprises agissant dans des environnements qui sont capables de prouver leur conformité vis-à-vis des bonnes pratiques du domaine). Les processus sont utilisés et documentés.
- **Géré** – ce niveau reflète la capacité de se protéger de menaces hautement techniques (investissements importants, processus bien identifiés, utilisés et leurs résultats sont mesurés dans un but d'amélioration).
- **Contrôlé** – les menaces hautement techniques et les menaces internes sont prises en considération (les processus sont gérés, objectifs clairs, ressources allouées).
- **Optimisé** – il existe un système de mesures et de métriques qui contribue aux améliorations et à une réduction effective des coûts.

4.8 CERTIFICATION DES PRODUITS DE SÉCURITÉ

4.8.1 Critères Communs

En 1985, le département de la Défense américain définissait des critères d'évaluation de la sécurité des systèmes informatiques (TCSEC, *Trusted Computer System Evaluation Criteria*). Côté européen, la France, le Royaume-Uni, l'Allemagne et les Pays-Bas ont aussi défini un référentiel de classification du niveau de sécurité des systèmes d'information, l'ITSEC (*Information Technology Security Evaluation Criteria*)). Les critères TCSEC et leurs équivalents européens (ITSEC) et canadiens

20. www.ism3.com

ont donné naissance à des critères communs à l'Europe et aux États-Unis : les **Critères Communs** (CC, *Common Criteria for Information Technology Security Evaluation*) (tableau 4.2).

Tableau 4.2 – Niveaux de sécurité définis par la norme ISO 15408(cc).

Critères communs ISO 15408	Signification	Critères US TCSEC équivalents	Critères ITSEC équivalents
-		D : Protection minimale	E0
EAL1	Testé fonctionnellement	-	-
EAL2	Testé structurellement	C1 : Protection discrétionnaire	E1
EAL3	Testé et vérifié méthodiquement	C2 : Protection des accès contrôlés	E2
EAL4	Conçu, testé et revu méthodiquement	B1 : Protection labellisée	E3
EAL5	Conçu et testé semi-formellement	B2 : Protection structurée	E4
EAL6	Vérifié, conçu et testé semi-formellement	B3 : Domaines de sécurité	E5
EAL7 (niveau le plus élevé)	Vérifié, conçu et testé formellement	A1 : Conception vérifiée	E6

EAL : *Evaluation Assurance Level*



Les **Critères Communs** constituent une typologie des niveaux de sécurité (ou classes), reconnue par l'ensemble des acteurs du marché de la sécurité.

La norme multipartie « Critères Communs » ISO 15408 définit le modèle général de la certification (partie 1), les exigences fonctionnelles de sécurité, qui sont les éléments techniques qui vont entrer dans la définition de la cible de sécurité (partie 2), et les exigences d'assurance de sécurité, qui sont la manière d'effectuer l'évaluation menant à la certification (partie 3).

4.8.2 Acteurs concernés par les Critères Communs

Les Critères Communs ont été élaborés :

- pour assister les **développeurs** de produits de sécurité dans l'identification des exigences de sécurité afin que ces derniers soient en conformité avec la norme et les préparer à l'évaluation de leurs produits ;
- pour que les **utilisateurs** puissent aisément comprendre quel est le niveau de sécurité objectif offert par un produit et ainsi choisir le produit qui satisfait au mieux leurs besoins de sécurité ;
- pour que les **évaluateurs** puissent effectuer des tests de conformité des produits et leur attribuer un label de sécurité tel que spécifié dans la norme ISO 15408.



Pour les **éditeurs**, un produit labellisé « Critères Communs » leur permet d'obtenir un avantage marketing pour leurs produits sur ceux de leurs concurrents. Pour le **certificateur**, c'est une manière de renforcer la souveraineté du pays auquel il appartient.

Pour tout ce qui concerne, en France, la **certification** par les **Critères Communs** (démarche, procédure, produits certifiés, dossier d'évaluation, conditions, portée de la certification, pilotage de l'évaluation, centres de certification, etc.), il est recommandé de se rapporter au site de l'Agence nationale de la sécurité des systèmes d'information²¹ ([ANSSI <http://www.ssi.gouv.fr>](http://www.ssi.gouv.fr)). De plus, l'ANSSI propose une certification de sécurité de premier niveau (CSPN), qui est plus facile à obtenir que la certification « Critères Communs ».



Un produit certifié « Critères Communs » présente son niveau de sécurité et atteste un certain seuil de sécurité garantie. L'utilisateur peut également comparer différents produits à partir d'un même référentiel d'analyse dont les critères sont connus et homogènes.

4.8.3 Principales limites des Critères Communs

Le **processus de certification** d'un produit débute par la rédaction des documents à déposer en vue d'une accréditation « Critères Communs », qui dépend de l'organisme de certification agréé. En effet, chaque organisme de certification a sa propre formalisation des rapports. Ces organismes offrent une formation spécifique pour l'équipe en charge du développement d'un produit afin que cette dernière puisse élaborer les rapports et les documents demandés. Le processus d'évaluation est souvent long et coûteux. L'effort d'investissement en termes de personnes à mobiliser et le coût lui-même de la certification sont souvent rédhibitoires pour certaines petites sociétés. De plus, du fait qu'il s'agit d'une norme internationale, il peut exister un certain décalage entre les spécifications de la norme, figée jusqu'à une nouvelle révision, et les technologies, qui doivent être en conformité avec cette même norme, mais qui possèdent un cycle d'évolution beaucoup plus rapide. Par ailleurs, les produits n'ont pas forcément besoin de répondre aux exigences de sécurité de la norme mais aux exigences des **tests de conformité**. Enfin, il s'agit d'un label statique attribué à un instant donné pour une version spécifique d'un produit, chaque modification, même mineure, chaque nouvelle version, nécessite une réévaluation et une nouvelle certification, plus facile à obtenir si l'option maintenance de la certification a été demandée.

21. « La certification dite tierce partie est la certification de plus haut niveau, qui permet à un client de s'assurer par l'intervention d'un professionnel indépendant, compétent et contrôlé, appelé organisme certificateur, de la conformité d'un produit à un cahier des charges ou à une spécification technique. La certification tierce partie apporte au client la confirmation indépendante et impartiale qu'un produit répond à un cahier des charges ou à des spécifications techniques publiées. Ces spécifications techniques peuvent être élaborées dans un cadre normatif ou non. » Source : ANSSI ; <http://www.ssi.gouv.fr/>

Bien souvent le label « certifié ‘Critères Communs’ » est avancé à des fins de marketing et ne reflète pas l'état de sécurité réel d'un produit. Il concerne fréquemment une version antérieure de celui-ci ou n'est relatif qu'à une sous-partie du produit (la cible de sécurité), généralement de peu d'intérêt du point de vue de l'assurance d'un niveau de sécurité du produit dans son intégralité. Se pose également le problème de la confiance dans l'organisme de certification et de son indépendance vis-à-vis de fournisseurs de solutions et autres acteurs impliqués dans la sécurité : Quelle confiance accorder à un organisme de certification ? Qui certifie les organismes ? Toutefois, il y a en France les organismes d'évaluation, les CESTI (centres d'évaluation de la sécurité des technologies de l'information), qui sont agréés par le COFRAC (Comité français d'accréditation), et les organismes de certification comme l'ANSSI, qui n'ont pas à être validés.

4.8.4 Principes de base des Critères Communs

L'utilisation des Critères Communs repose sur les principes de sécurité suivants :

- La **défense en profondeur** : la sécurité est augmentée quand une série de couches de contrôle et de contre-mesures sont implantées pour assurer la prévention, la protection, et la réponse en cas d'incident. Ce concept d'origine militaire stipule que la faiblesse d'un mécanisme doit être protégée par deux ou plusieurs autres mécanismes.
- La sécurité informatique dépend de deux types d'exigences. Les **exigences fonctionnelles** (ce qu'un système peut faire de par sa conception) et les **exigences d'assurance** qui permettent de spécifier qu'un niveau minimum de résistance cohérent est visé, en fonction des objectifs de sécurité.
- La **sécurité absolue n'existe pas** : les outils de sécurité permettent éventuellement de « gagner » du temps, permettant de réagir pour résoudre un problème. Les CC ne prennent pas en considération « le non-intentionnel » comme les erreurs.

4.8.5 Vocabulaire et concepts

Les Critères Communs (CC) possèdent beaucoup d'acronymes et une **terminologie** qui définissent une taxonomie et un langage semi-formel afin de constituer un référentiel de langage commun à toutes les parties intéressées.

Les concepts clés sont :

- **Target of Evaluation (TOE)** : il s'agit de l'objet à évaluer, que ce soit un produit ou un document. On essaye de protéger les objets en les assignant à des classes basées sur leur degré de sensibilité.
- **Protection Profile (PP)** : il s'agit d'un document qui détaille les exigences de sécurité pour une classe de produits qui offrent les mêmes fonctions de sécurité.
- **Security Target (ST)** : ensemble d'exigences de sécurité et de spécifications à utiliser comme base pour l'évaluation d'une cible d'évaluation. La cible de

sécurité atteste que la cible d'évaluation est conforme aux différents Profils de Protection, quand ils existent.

- **Evaluation Assurance Level (EAL)** : niveau d'assurance de l'évaluation qui définit le degré de confiance que l'on peut accorder au produit certifié.
- Pour comprendre les composantes des CC, il est nécessaire de les situer dans le cadre sécuritaire dans lequel la cible d'évaluation sera opérationnelle. Il s'agit de :
- **l'environnement de sécurité** dans lequel la cible d'évaluation va fonctionner : cadre juridique, politique de sécurité de l'organisation, menaces, etc. ;
- **les objectifs de sécurité**, qui sont les mesures qui vont répondre aux menaces identifiées ;
- **les spécifications de sécurité** de la cible d'évaluation, qui sont les exigences techniques qui dérivent des objectifs de sécurité.

Ceux qui rédigent le document décrivant la cible d'évaluation vont **estimer les menaces** possibles, pour constituer une liste de menaces avec des risques potentiels pour que les objectifs de sécurité soient remplis. Cette liste va aider les éditeurs désirant faire certifier leur produit à définir les contre-mesures pour réduire le risque à un niveau acceptable. En revanche, à ce stade il n'est pas possible d'évaluer les **contre-mesures** et leur efficacité en repoussant les attaques malicieuses. Il faut donc avoir confiance dans les contre-mesures utilisées. Dès lors, les CC permettent de vérifier que les contre-mesures sont développées et implémentées de telle manière que les menaces communes puissent être repoussées.



Les Critères Communs permettent de s'assurer que les exigences de sécurité sont intégrées dans un produit dès sa conception (**Security by design**).

L'évaluation de la cible d'évaluation peut se faire pendant ou après le développement du produit. Ces deux activités se font d'une manière complémentaire pour pouvoir modifier le produit et corriger les failles trouvées. La confirmation que la cible d'évaluation remplit les objectifs et les spécifications de sécurité, tels qu'établis dans la cible de sécurité, est le résultat attendu de l'évaluation. L'évaluation aide le développeur à identifier les erreurs et les vulnérabilités dans la construction et dans le développement de son produit.

L'approche de certification « Critères Communs » commence par l'identification des hypothèses sur l'environnement auquel la cible d'évaluation sera confrontée. Toutes les menaces doivent alors être identifiées. La politique de sécurité organisationnelle pourra être établie pour pouvoir identifier la politique de sécurité et les règlements. Le résultat de cette analyse est l'expression des objectifs de sécurité.



La certification « Critères Communs » (ou ISO 15408) porte sur un produit, alors que la certification ISO 27001 porte sur un organisme.

Résumé

Le développement de nouveaux usages, l'ouverture du système d'information aux clients et aux partenaires, l'essor de la mobilité ainsi que l'augmentation croissante de la complexité technologique, organisationnelle et juridique, ont conduit les organisations à se doter d'outils de management de la sécurité. Parmi eux, retenons la politique de sécurité, véritable ligne directrice de la mission sécuritaire.

Il appartient à la direction d'une entreprise d'évaluer les risques encourus par le système d'information, d'élaborer une politique de sécurité et d'établir une structure organisationnelle chargée de coordonner et de superviser la mise en œuvre de cette politique dans le respect des diverses législations et réglementations en vigueur (notion de conformité juridique). Faire de la gestion des risques et de la sécurité un facteur de performance de la gestion d'entreprise constitue un véritable défi pour les organisations.

L'efficacité d'une politique de sécurité ne se mesure pas au budget investi, mais dépend de la politique de gestion du risque et de la qualité de l'analyse des risques. Toutefois, la qualité de la sécurité informatique dépend aussi de l'identification et de l'évaluation de la valeur du patrimoine informationnel de l'entreprise et de la mise en œuvre opérationnelle, à partir de la politique de sécurité, de mesures de sécurité adaptées. La pertinence de la politique de sécurité ainsi que l'efficacité de la gestion de la sécurité, comme l'existence d'une culture de sécurité des employés, des prestataires et des fournisseurs, constituent également un garant de l'adéquation des mesures aux besoins.

Le choix de suivre une norme ou une méthode pour spécifier une politique de sécurité se fait en fonction des besoins, de l'adéquation des méthodes existantes et des compétences et ressources disponibles pour établir la politique. Choisir une norme et une méthode comme référentiel et support qui permet de s'appuyer sur un cadre existant est parfois nécessaire mais jamais suffisant.

La sécurité n'est pas seulement un problème technique mais un problème de gouvernance, de gestion et de personnes (ces dernières constituent autant une menace pour la sécurité qu'un moyen de défense contre d'éventuelles violations de cette sécurité). La politique de sécurité doit donc également mettre l'accent sur la nécessité de disposer d'une bonne infrastructure de gestion des ressources humaines.

Au vu de la complexité de la réalisation d'une mission sécurité, certaines organisations optent pour l'externalisation (*outsourcing*) de tout ou partie de leur sécurité. La stratégie d'externalisation d'une politique de sécurité peut concerner la définition, la mise en œuvre et le contrôle, les accès distants, l'hébergement de sites web ou d'applications, l'administration de routeurs ou de pare-feu, la télémaintenance des systèmes et réseaux, la tierce maintenance applicative, la gestion des sauvegardes, etc. Le choix d'un prestataire doit toujours s'accompagner d'une démarche de contrôle qualité et peut tenir compte, par exemple, de l'expérience du prestataire, des compétences internes, des technologies utilisées, du délai de réaction, du service support, des clauses contractuelles (engagement de résultat, etc.), ou du partage des responsabilités légales.

Exercices

- 4.1** Quels sont les avantages relatifs à la définition d'une politique de sécurité pour une organisation ?
- 4.2** Quels sont les éléments qui permettent de justifier la mise en place d'une politique de sécurité pour le système d'information d'une entreprise ?
- 4.3** Comment s'exprime la rentabilité d'une politique de sécurité ?
- 4.4** Identifiez les principales étapes d'une démarche sécurité.
- 4.5** Quels sont, pour une entreprise, les avantages et les inconvénients potentiels liés à l'externalisation de la sécurité informatique (*outsourcing*) par rapport à une gestion interne de la sécurité ?
- 4.6** Proposez une modélisation des différents éléments intervenant dans la gestion des risques.
- 4.7** Quelles sont les principales limites de la norme ISO 27002 pour la réalisation de la sécurité ?
- 4.8** Pourquoi, dans une politique de sécurité, doit-on disposer d'un plan de secours et de gestion de la continuité ?
- 4.9** Quelle est la principale fonction d'un modèle de maturité en sécurité informatique ?
- 4.10** À quels besoins répond une certification « Critères Communs » ?
- 4.11** Quelles sont les analogies et les différences entre la méthode CobiT (*Control Objectives for Information & Technology*) et les normes ISO de la série 27000 ?
- 4.12** De quels paramètres dépend la prise en compte des besoins de sécurité d'une ressource ?
- 4.13** Quelles différences existe-t-il entre la notion de protection et celle de sécurité ?
- 4.14** Identifiez des paramètres qui permettent de mesurer l'efficacité d'une politique de sécurité.
- 4.15** Pourquoi les organisations utilisent-elles parfois des modèles de maturité de la sécurité ?

Solutions

- 4.1** L'avantage principal de la **définition d'une politique de sécurité de l'entreprise** est de traiter la problématique de la sécurité informatique dans son intégralité, selon une approche systémique.

La définition d'une politique de sécurité permet de ne pas se focaliser d'abord sur les outils de la sécurité mais de s'intéresser en premier lieu au pourquoi de la sécurité (tableau 4.3). La définition d'une politique de sécurité force à avoir une réflexion stratégique des enjeux et des moyens de la maîtrise de la sécurité et permet d'appréhender les différentes dimensions de la sécurité (organisationnelle, managériale, humaine, juridique et technologique).

Tableau 4.3 - La politique de sécurité doit répondre à des questions simples.

Éléments d'une politique de sécurité	Des questions simples Des réponses précises
Organisation de la sécurité	Que protéger ?
Attribuer des responsabilités à des personnes compétentes possédant l'autorité et les moyens nécessaires	De qui ? De quoi doit-on se protéger ? Pourquoi ? Quels sont les risques réellement encourus ?
Identifier les cibles sécuritaires de chaque domaine et de chaque composant du système d'information	Ces risques sont-ils supportables ? Quel est le niveau que l'on désire atteindre ?
Définir les menaces Identifier les vulnérabilités	Quelles sont les contraintes effectives ? Quels sont les moyens disponibles ?
Définir les mesures de sécurité	Comment les mettre en œuvre ?
Définir les comportements de sécurité	

4.2 Une politique de sécurité est un **outil de gouvernance** qui permet de traiter la sécurité comme un processus de gestion continu en fonction d'objectifs stratégiques clairement définis.

Elle reflète l'analyse des valeurs et l'appréciation des risques encourus ainsi que les plans d'action à mener pour satisfaire les besoins, les exigences, les objectifs de sécurité et définit les mesures pertinentes qui permettent de les satisfaire.

4.3 Tant qu'un sinistre n'est pas survenu, mais qui pourrait permettre de quantifier le coût d'un défaut de sécurité, il est très difficile de mesurer la **rentabilité** comme l'efficacité d'une politique de sécurité. Des métriques objectives manquent. En revanche, on sait qu'un niveau adapté de sécurité permet à l'organisation d'être compétitive, pérenne et de ne pas perdre des valeurs. Il ne faut pas perdre de vue que les mesures de sécurité permettent de protéger une valeur d'un risque réel (et non théorique) dont la potentialité d'occurrence est forte et les impacts graves, qu'il ne faut pas faire de la sécurité pour faire de la sécurité, que les mesures de sécurité ne doivent pas avoir un coût supérieur à celui de la perte de valeur à protéger.

4.4 Les principales étapes d'une **démarche sécurité** sont :

- analyse de l'existant, évaluation des valeurs, des besoins, des menaces, des vulnérabilités ;
- appréciation des risques ;
- identification des contraintes financière, technique, humaine, organisationnelle, juridique ;

Chapitre 4 • Politique de sécurité

- définition des objectifs et de la politique de sécurité ;
- mise en place de la structure organisationnelle et d'une culture de la sécurité ;
- sensibilisation et responsabilisation ;
- identification et implantation des mesures (outils et procédures) de sécurité ;
- gestion opérationnelle de la sécurité (maintenance, exploitation, surveillance) ;
- évaluation, audit et optimisation de la politique et des mesures de sécurité ;
- veille technologique.

4.5 L'avantage majeur d'une **solution d'externalisation** (*outsourcing*) réside essentiellement dans le fait que le service est fourni par des professionnels de la sécurité pouvant, du fait de leur degré de compétence et d'expérience, répondre de manière plus performante aux besoins de sécurité. En revanche, cela peut introduire de nouveaux risques pour l'entreprise. En effet, parmi les inconvénients citons par exemple ceux liés à :

- la dépendance de l'entreprise vis-à-vis de la société qui fournit le service ;
- des solutions pas forcément adaptées aux processus, aux valeurs de l'entreprise si ceux-ci sont insuffisamment identifiés ;
- une déresponsabilisation des problèmes de sécurité des acteurs internes de l'entreprise.

4.6

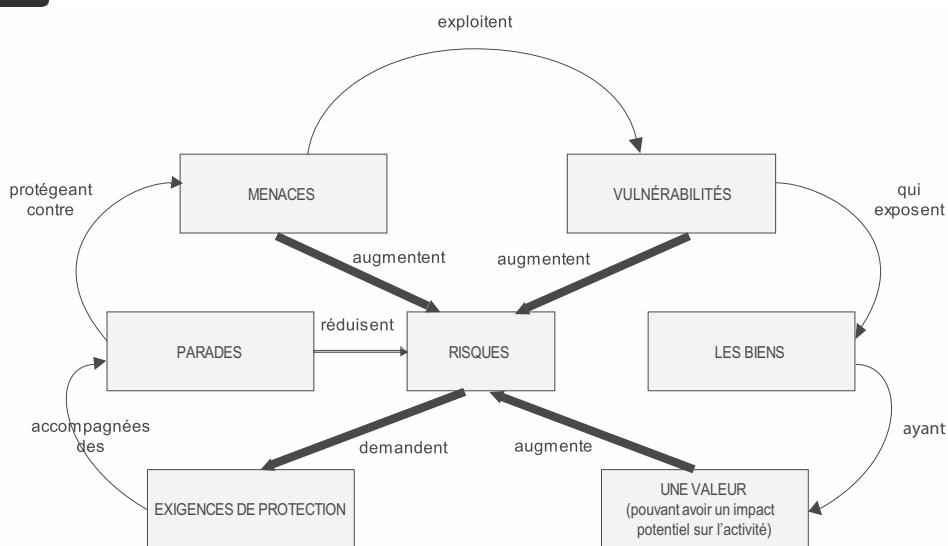


Figure 4.15 – Schéma relationnel de la gestion du risque
(issu de la norme Afnor Z 74-260-1).

4.7 La **norme ISO 27002** peut être vue comme une *check-list* dont l'intérêt réside dans l'identification des points à prendre en considération lorsqu'une organisation souhaite définir une politique de sécurité. Elle permet de ne pas oublier certains aspects de la sécurité et ainsi d'appréhender la sécurité de manière exhaustive.

Toutefois, tous les points identifiés dans la norme ne sont pas forcément pertinents pour une entreprise particulière. Un travail « d'appropriation » de la norme doit être réalisé, ce qui demande un certain effort.

De plus, la norme n'est ni une méthode de travail pour la mise en place de la politique de sécurité informatique, ni une méthode d'évaluation des risques. Elle ne propose pas non plus des mesures concrètes de sécurité. La norme constitue un cadre de référence pour appréhender la sécurité selon une approche globale. Elle est à la sécurité ce que le modèle de référence OSI pour l'interconnexion des systèmes ouverts (norme ISO 7498) est aux réseaux de télécommunication. Si on tient compte de ces faits, une des limites que l'on pourrait identifier, qui est inhérente aux normes internationales, est celle liée à la fréquence de sa révision qui peut introduire un certain décalage entre l'état d'un document statique et l'état des environnements à protéger.

4.8 Quelle que soit la finalité d'un système d'information, ses éléments constitutifs sont susceptibles de dysfonctionner ou d'être la cible d'une malveillance (ils peuvent également être utilisés pour perpétrer une fraude sur un système d'une autre organisation [malveillance indirecte]). Il est donc impératif de pouvoir prévenir ces incidents ou à défaut de pouvoir en limiter les dégâts, grâce à leur détection rapide et par une réaction appropriée afin de maintenir le système en état opérationnel ou encore permettre un retour à la normal dans les meilleurs délais.

Ainsi, des **plans de secours et de gestion de la continuité des services**, comme des directives claires, précises et compréhensibles spécifiant aux différents acteurs ce qu'ils doivent faire face à une situation d'urgence, sont primordiaux. Prévoir ces situations de crise, planifier les actions de reprise contribue à faciliter la prise de décision dans une situation critique et permet d'éviter un état de panique préjudiciable au maintien de la sécurité et à la continuité des activités lorsque les incidents surviennent.

La pérennité de l'entreprise étant l'objectif et la raison d'être des gestionnaires de celle-ci, le processus assurant la survie de l'entreprise doit être initié, géré et maintenu par les mêmes instances directrices de l'organisation. Pour ce faire, les principaux éléments à prendre en compte pour assurer la pérennité de l'entreprise seront :

- la protection des vies humaines ;
- la protection contre les événements naturels tels que les tremblements de terre, les inondations, les glissements de terrain, le feu, les actions terroristes ;
- la protection des services vitaux comme l'électricité, les gaz, l'eau, etc.
- la protection des actifs de l'entreprise ;
- la conformité juridique.

4.9 Un **modèle de maturité en sécurité informatique** permet, via des indicateurs (métriques) pertinents préalablement définis par l'organisation, d'exprimer l'état global et le niveau général d'un dispositif de sécurité.

4.10 Les **Critères Communs**, dont une version est spécifiée par la norme ISO 15408, fournissent des briques de base permettant de spécifier la sécurité du produit ou du système à développer ou à acquérir. Cette norme contient des définitions des critères à utiliser comme base pour l'évaluation des propriétés de sécurité

d'un produit ou d'un système. Elle contient aussi la terminologie et la définition des autres concepts nécessaires à l'utilisation de ces critères. La certification « Critères Communs » permet de développer la confiance des utilisateurs envers les produits dont on connaît le niveau de sécurité. Ce type de certification permet de s'assurer du fait que les processus du développement des produits ont tenu compte des exigences de sécurité. Ainsi, leur évaluation atteste du niveau de sécurité des produits.

4.11 CobiT présente un cadre de référence des meilleures pratiques en termes d'audit et de maîtrise de risques des systèmes d'information afin d'établir des liens entre les risques métiers, les besoins de contrôle et les problématiques techniques. Les normes ISO 27xxx proposent des codes de pratiques pour la gestion de la sécurité, basés sur la gestion des risques. Les normes définissent, entre autres, un vocabulaire standard, les exigences de sécurité d'un système de management de la sécurité, un code de bonnes pratiques de gestion, des métriques du management, la gestion du risque, etc. Les normes ISO présentent donc des standards pour la mise en place de la sécurité tandis que CobiT propose un cadre pour l'évaluation des contrôles internes non seulement liés à la sécurité.

4.12 La prise en compte dépend des **paramètres** de classification de la ressource et de son degré de criticité – son niveau d'importance pour l'entreprise et le niveau de dépendance de celle-ci vis-à-vis de la ressource. Le plus conséquent sont les impacts négatifs dus à l'indisponibilité de la ressource (perte, destruction, vol) ou à son manque d'intégrité ; plus ils sont importants, plus la ressource est évaluée comme critique.

4.13 La notion de **protection** concerne le renforcement de la robustesse des ressources et la diminution des détériorations consécutives à la réalisation d'une menace. La notion de **sécurité** est plus large et concerne les mesures de protection ainsi que les mesures préventives, structurelles, de dissuasion, palliatives, correctives et de récupération.

4.14 L'**efficacité d'une politique de sécurité** est évaluée par rapport à sa performance vis-à-vis des objectifs à atteindre. On définit des métriques basées sur des paramètres tels que : nombre d'attaques réussies/attaques stoppées ; nombre de jours de travail perdus suite à des incidents ; nombre de points relevés par les auditeurs ; nombre d'incidents nécessitant l'implication du senior management ; nombre de changements aux droits d'accès effectués afin de satisfaire les besoins du business, etc.

4.15 Les organisations utilisent parfois des modèles de maturité de la sécurité :

- pour définir des objectifs tangibles, compréhensibles et clairs pour les aspects de sécurité à traiter ;
- pour contrôler le niveau de la sécurité et situer l'état actuel par rapport à un état désiré ;
- pour suivre l'évolution du niveau de sécurité ;
- pour constituer une échelle de comparaison entre des organisations ;
- pour prioriser les actions à entreprendre pour améliorer le système.

LA SÉCURITÉ PAR LE CHIFFREMENT

5

PLAN

- 5.1 Principes généraux
- 5.2 Principaux systèmes cryptographiques
- 5.3 Services offerts par la mise en œuvre du chiffrement
- 5.4 Infrastructure de gestion de clés
- 5.5 L'apport du Blockchain

OBJECTIFS

- Présenter et analyser les principaux systèmes de chiffrement ainsi que les mécanismes mis en œuvre pour offrir des services de confidentialité, d'intégrité et d'authentification.

5.1 PRINCIPES GÉNÉRAUX

Le **chiffrement des données** (la cryptographie) est l'outil fondamental de la sécurité informatique. En effet, la mise en œuvre de la **cryptographie** permet de réaliser des services de confidentialité des données utilisées, transmises ou stockées, des services de contrôle d'intégrité de données et d'authentification d'une entité, d'une transaction ou opération.

5.1.1 Vocabulaire

Le **chiffrement** est l'opération par laquelle on chiffre un message, c'est une opération de codage. Chiffrer ou improprement dit « **crypter** »¹ une information permet de la rendre incompréhensible en l'absence d'un décodeur particulier. Un **cryptogramme** (ou message caché) est écrit en caractères secrets, en code, en langage chiffré. Chiffrer et cryptographier sont synonymes. On déchiffre un message chiffré avec la clé de déchiffrement, on décrypte un message chiffré quand on n'a pas la clé. Le chiffre de défense : chiffrement/déchiffrement n'est pas synonyme du chiffre d'attaque : décryptement.

1. Crypto est issu du grec *kruptos*, qui signifie « caché ».



Le chiffrement des données est parfois qualifié de scellement.

La **cryptographie** est la science qui consiste à écrire l'information (quelle que soit sa nature : voix, son, texte, donnée, image fixe ou animée) pour la rendre inintelligible à ceux ne possédant pas les capacités de la déchiffrer (la convention de déchiffrement).

La **cryptanalyse** comprend l'ensemble des moyens qui permettent d'analyser une information préalablement chiffrée, afin de la décrypter. Plus un système de chiffrement sera robuste, plus sa cryptanalyse sera difficile et longue.

La **rétro-ingénierie** des systèmes de communication s'apparente à la cryptanalyse dans la mesure où elle s'emploie à extraire des données, non chiffrées, mais cachées dans du bruit.

5.1.2 Algorithmes et clés de chiffrement

Les systèmes de chiffrement font appel à des **algorithmes de chiffrement** qui reposent sur des procédures mathématiques complexes qui, à l'aide d'une **clé de chiffrement**, modifient les données sensibles en générant des données apparemment incompréhensibles à ceux qui ne possèdent pas la clé de déchiffrement permettant d'obtenir le texte initial en clair (*plaintext*). Le texte chiffré (cryptogramme ou *ciphertext*) peut alors être transmis sur un réseau non sécurisé. La fonction miroir du chiffrement est celle de déchiffrement qui met en œuvre le même algorithme et, selon la nature de ce dernier (symétrique ou asymétrique), une clé de déchiffrement identique ou non.

Taille de la clé

Si une clé est codée sur n bits (taille de la clé), elle peut être l'une de 2^n valeurs. Plus la clé est longue, plus le nombre de clés possibles est important. Ainsi, plus cela nécessite, pour quelqu'un qui cherche à la connaître, de la puissance et du temps de calcul.

De la sorte, une clé de chiffrement/déchiffrement doit avoir une **taille minimale** afin d'éviter qu'elle puisse être déterminée trop facilement par des entités non habilités hostiles.

Dans le cas du chiffrement symétrique, comme il est devenu relativement simple de « casser » (c'est-à-dire de trouver) des clés d'une longueur de 40 bits par force brute (environ 10^{12} possibilités de clés différentes), il est indispensable de chiffrer les informations sensibles avec des clés plus longues, de 128 (10^{38} possibilités) ou de 256 bits, par exemple. Casser de telles clés nécessite alors une très lourde infrastructure informatique et des temps de traitement importants, ce qui peut être rédhibitoire pour certains. De plus, le temps de calcul pour casser la clé pourrait être infiniment plus long que la durée de confidentialité du message à déchiffrer.

Remarquons par ailleurs que le moyen le plus simple pour obtenir une clé est de se la procurer directement auprès de l'utilisateur ou à partir du système qui la stocke, plutôt que d'essayer de la deviner par itérations successives.

Robustesse du système

La **puissance de l'algorithme**, la taille de la clé utilisée et la capacité à garder les clés secrètes de façon sécurisée, déterminent la **robustesse** d'un système de chiffrement. L'algorithme n'a pas besoin d'être secret. Il est même recommandé qu'il soit public et publié afin que la communauté scientifique puisse tester sa résistance aux attaques et trouver les failles, les communiquer, les réparer, avant qu'un attaquant ne les exploite. Le secret réside au niveau de la clé.

 Garder un algorithme secret ne renforce pas sa sécurité.

Il n'est déjà pas aisément de garder des clés secrètes alors garder confidentiel un algorithme l'est encore moins dans la mesure où les algorithmes sont utilisés par un grand nombre d'utilisateurs et durant de longues périodes. De plus, si les concepteurs d'un algorithme secret ne sont plus disponibles, cela pose un problème pour la maintenance et l'évolution de cet algorithme.

Un **système de chiffrement** est dit fiable, robuste ou sûr, s'il reste inviolable indépendamment de la puissance de calcul ou du temps dont dispose un attaquant. Il peut être alors qualifié d'**opérationnellement sécurisé** (*computational secure*) si sa sécurité dépend d'une série d'opérations réalisables en théorie, mais irréalisables pratiquement (temps de traitement trop long en appliquant les méthodes de résolution connues et en utilisant la puissance de calcul disponible).

Constatons que, plus une clé est spécifique et son utilisation limitée dans le temps, voire à usage unique, meilleure est la sécurité du système de chiffrement. La question qui se pose alors est de savoir si le renouvellement fréquent d'une clé de chiffrement rend un système de chiffrement plus sécurisé ? À ce jour, aucune preuve formelle n'a été fournie sur ce point. Toutefois, si la **robustesse d'un système de chiffrement** réside dans l'algorithme de chiffrement lui-même et non sur la clé (l'algorithme est incassable), changer fréquemment les clés de chiffrement le rend encore plus sûr. En revanche, si l'algorithme constitue le maillon faible du système de chiffrement, changer la clé fréquemment n'augmente pas sa robustesse.

5.2 PRINCIPAUX SYSTÈMES CRYPTOGRAPHIQUES

La **cryptographie** classique ou traditionnelle inclut tous les mécanismes et algorithmes basés sur des fonctions mathématiques ou logiques. Elle regroupe tous les systèmes de chiffrement utilisés depuis l'Égypte ancienne jusqu'aux principaux systèmes de chiffrement actuellement en vigueur. Elle se compose principalement de deux classes de systèmes de chiffrement : les systèmes de chiffrement symétrique et les systèmes de chiffrement asymétrique.

5.2.1 Système de chiffrement symétrique

Mode opératoire

Pour chiffrer ou déchiffrer un texte, il faut détenir **une clé et un algorithme de chiffrement**. S'il s'agit de la même clé pour effectuer ces deux opérations, le système de chiffrement est qualifié de **symétrique**. L'émetteur et le récepteur doivent posséder et utiliser la même clé secrète pour rendre confidentielles des données et pour pouvoir les comprendre (figure 5.1).

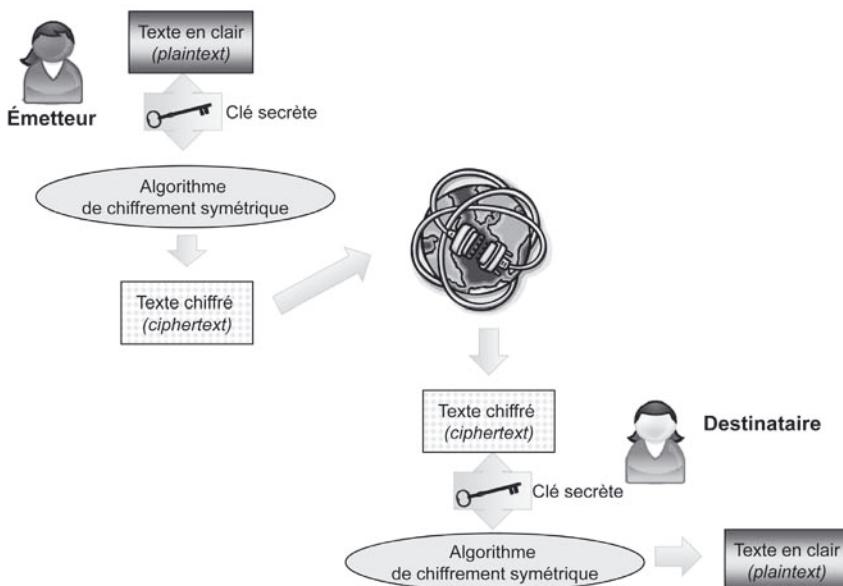


Figure 5.1 – Le chiffrement symétrique.

Chaque entité doit posséder autant de clés secrètes qu'elle a d'interlocuteurs. Il faut donc disposer d'autant de paires différentes de clés qu'il y a de paires de correspondants. En effet, pour N personnes désirant communiquer deux à deux, il doit exister $N(N-1)/2$ clés. Ce qui devient vite impossible à réaliser et inadapté aux communications multipartenaires et aux services d'Internet : 1 000 utilisateurs nécessitant par exemple la disponibilité de 499 500 clés qui doivent être échangées mais rester secrètes !

Un système de chiffrement symétrique pose donc le problème de la gestion et notamment de la diffusion des clés secrètes. Cela constitue une faiblesse des systèmes de chiffrement symétrique. Toutefois, les algorithmes symétriques sont puissants, ne nécessitant que des clés de taille relativement faible (128 bits par exemple) et assez peu de ressources. Ils peuvent chiffrer des données en temps réel ou en différé.

Principaux algorithmes

Les principaux algorithmes symétriques sont les suivants :

- **DES** (*Data Encryption Standard*) a été adopté par le NIST² (*National Institute of Standards and Technology*) en 1977. Les données sont chiffrées par blocs de 64 bits avec une clé de 56 bits utiles. Cet algorithme est largement répandu et est souvent mis en œuvre en un mode dit de **chaînage de blocs** (CBC, *Cipher Block Chaining*), où le chiffrement d'un bloc dépend du précédent. Les différentes variantes **Triple DES**, **DESX** (*DES XORed*), **GDES** (*Generalized DES*), **RDES** (*Randomized DES*) sont issues de l'algorithme DES, elles utilisent des clés plus longues, rendant ainsi l'algorithme plus puissant (DES avec une clé de 56 bits a été cassé en 1997). Le Triple DES tire son nom du fait que l'on réalise trois chiffrements en série ce qui donne une clé effective de 168 bits.
- **RC2**, **RC4** et **RC5** sont des algorithmes propriétaires à clé symétrique développés par Ronald Rivest et diffusés par la société RSA Security Inc³. Ils utilisent des clés de longueur variable pouvant aller jusqu'à 2 048 bits. Ils sont largement utilisés pour rendre confidentiels des flux applicatifs.
- **IDEA** (*International Data Encryption Algorithm*), développé conjointement par des chercheurs de l'école polytechnique fédérale de Zurich et de la société Ascom, utilise une clé de 128 bits pour coder les données par blocs de 64 bits en opérant huit rondes d'une même fonction. Il est notamment utilisé par le protocole de messagerie sécurisée PGP⁴ (*Pretty Good Privacy*).
- **Blowfish** est un algorithme de chiffrement symétrique développé par Bruce Schneier en 1993⁵.
- **AES** (*Advanced Encryption Standard*) a été publié pour la première fois en 1998 par deux chercheurs belges, Vincent Rijmen et Joan Daemen⁶. Il utilise des clés de 128 bits, 192 ou 256 bits sur des blocs de 128 bits. L'AES est jugé rapide, facile à implémenter et ne requiert que peu de ressource mémoire. Jusqu'à ce jour, ce système de chiffrement demeure incassable et reste le plus sûr des systèmes de chiffrement symétrique.

5.2.2 Système de chiffrement asymétrique

C'est pour pallier la complexité induite par la gestion et la distribution des clés des systèmes de chiffrement symétrique qu'un autre type de système de chiffrement, qualifié d'**asymétrique ou à clé publique** a été conçu et est actuellement largement utilisé dans le monde d'Internet.

Les algorithmes asymétriques permettent de réaliser plusieurs fonctions de sécurité relatives à la confidentialité, l'intégrité, l'authentification et à la non-répudiation.

-
2. <http://www.itl.nist.gov>
 3. <http://www.rsasecurity.com>
 4. <http://www.pgp.com>
 5. <http://www.schneier.com/blowfish.html>
 6. <http://www.csrc.nist.gov/publications/fips/fips197/fips-197.pdf>

Mode opératoire

Un système de chiffrement **asymétrique** est basé sur l'usage d'un couple unique de deux clés différentes mais complémentaires et mathématiquement liées, calculées l'une par rapport à l'autre possédant une solidité mathématique difficile à briser.

Cette bi-clé est constituée d'une **clé publique** et d'une **clé privée**. Seule la clé dite publique doit être connue de tous, tandis que la clé privée doit être confidentielle et traitée, comme dans le cas des algorithmes symétriques, comme un secret. Les interlocuteurs connaissent les clés publiques des autres mais ne peuvent en déduire leurs clés privées. Ceci est rendu possible parce qu'il existe des problèmes difficiles à résoudre avec les calculateurs classiques, comme celui de la factorisation d'un grand nombre, produit de deux nombres premiers ou encore la résolution du logarithme discret.

Pour envoyer un message confidentiel à un destinataire, l'émetteur le chiffre avec la clé publique du destinataire. À sa réception, ce dernier le déchiffra avec sa clé privée, qu'il est le seul à connaître. Ainsi, le message est confidentiel pour le destinataire dans la mesure où lui seul peut le déchiffrer (figure 5.2).

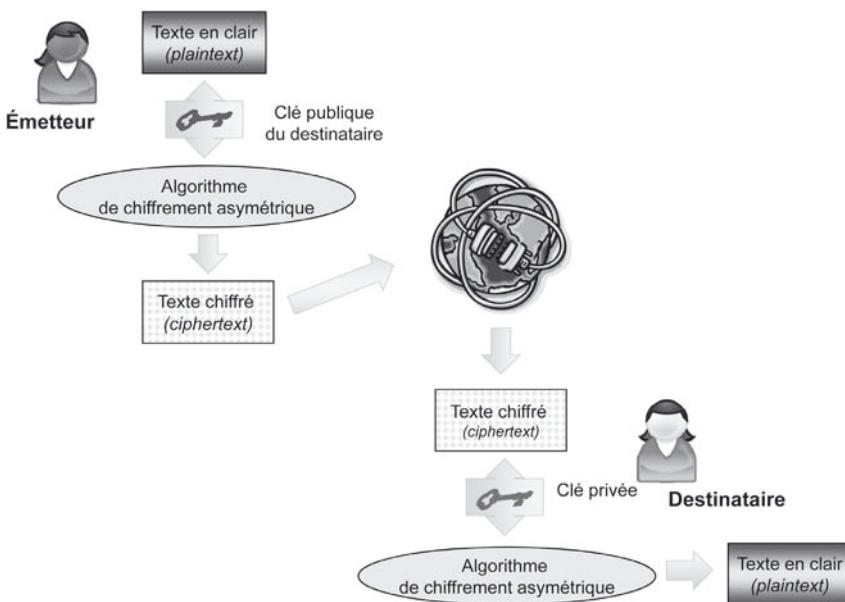


Figure 5.2 – Le chiffrement asymétrique.

Bien sûr, il reste à prouver qu'une clé publique est bien celle qui est mathématiquement liée à la clé privée détenue par son propriétaire. Ceci est réalisé par le certificat numérique du propriétaire de la clé publique, et qui détient donc aussi la clé privée, et par la signature électronique, notions que nous décrirons par la suite.

Par ailleurs, la mise en œuvre du chiffrement asymétrique permet également de réaliser la signature électronique de document, d'authentifier un émetteur, de vérifier l'origine d'un message et son intégrité.

L'exécution de ce type d'algorithme est consommatrice d'énergie et demande un temps de traitement processeur important, ce qui rend ces algorithmes non performants pour le chiffrement de messages longs. Les algorithmes asymétriques sont estimés être de 10 à 100 fois plus lents que les algorithmes symétriques, et ils nécessitent des clés également plus longues (la taille courante est de l'ordre de 1 024 bits). 2048 bits sont aujourd'hui conseillés en France par l'Agence nationale de la sécurité des systèmes d'information (ANSSI).

Le chiffrement asymétrique est principalement utilisé pour le chiffrement de messages courts, comme par exemple la clé secrète d'un algorithme de chiffrement symétrique (voir paragraphe 5.3.1).

Principaux algorithmes

Les principaux algorithmes de chiffrement à clé publique, dont le nom est celui de leurs inventeurs, utilisent le plus souvent des clés de longueur variant de 512 à 1 024 bits voire 2 048 bits. Nous retiendrons les algorithmes suivants :

- **RSA** (pour Ron Rivest, Adi Shamir, Len Adelman)⁷, qui est basé sur la factorisation des nombres premiers. RSA utilisé avec une clé de 640 bits a été cassé en 2005, on l'utilise généralement avec une clé de 1 024 bits.
- **Diffie-Hellman**⁸, inventé en 1976 par Whitfield Diffie et Martin Hellman (pionniers de la cryptographie asymétrique), et l'algorithme **ElGamal**, qui sont basés sur le calcul de logarithmes discrets. Ce dernier, conçu en 1984 par Tahar ElGamal, est disponible en logiciel libre⁹.

Certains algorithmes basés sur les équations de calcul de circonférences des ellipses sont à l'origine de la **cryptographie à courbe elliptique** (ECC, *Elliptic Curve Cryptography*)¹⁰. Bien que développé au milieu des années 1980 et relativement robuste, ce type de cryptographie reste d'un usage marginal.

5.2.3 Quelques considérations sur la cryptanalyse

La **cryptanalyse** des systèmes de chiffrement se base généralement sur la découverte des clés de chiffrement (*related-key attack*), sur l'analyse des messages sans nécessiter la connaissance des clés (*chosen-plaintext/chosen ciphertext attacks*) ou sur l'existence de collisions¹¹. Toutes les techniques de cryptanalyse ont toutes pour

7. <http://www.rsa.com>

8. <http://www.ietf.org/rfc/rfc2631.txt>

9. GNU Privacy Guard, open PGP ; <http://www.gnupg.org>

10. Neal Koblitz, « Elliptic curve cryptosystems », *Mathematics of Computation* 48, 1987, pp. 203-209, Miller V., « Use of elliptic curves in cryptography », CRYPTO 85, 1985.

11. Cela fait référence au « paradoxe de l'anniversaire » qui indique que sur une assemblée de 23 personnes, il y a plus de 50 % de chance pour que deux personnes aient leur anniversaire le même jour. Transposé dans le monde de la cryptographie, ce paradoxe peut conduire au fait que le chiffrement de données différentes par un mauvais algorithme pourrait donner le même résultat (notion de collision, à partir de laquelle les cryptanalystes savent casser les textes chiffrés).

objet de casser les systèmes de chiffrement ou les mécanismes qui permettent de réaliser les services de sécurité impliquant des fonctions cryptographiques.

En réalité, la plupart des systèmes de chiffrement symétrique résistent relativement bien aux attaques dites de force brute (*brute force attack*), du fait du temps nécessaire pour tester toutes les combinaisons possibles de clés. Toutefois, si nous tenons compte du progrès scientifique dans le domaine de l'informatique, de l'évolution de mise en réseau des ressources (*Grid & Cloud Computing*) et de l'électronique, les systèmes qui sont jugés actuellement sûrs ne le seront peut-être plus dans un futur proche du fait de l'augmentation de la capacité et de la rapidité de traitement.

Le **cryptanalyste** (la personne en charge de la cryptanalyse) peut par exemple tester plusieurs clés qui ne diffèrent les unes par rapport aux autres que de quelques bits sur un seul message pour deviner le comportement du système de chiffrement. Ensuite, il tente de retrouver les messages originaux à partir des messages chiffrés sans avoir recours à l'utilisation effective de la clé de déchiffrement. Cette pratique est assez puissante et permet, par exemple, de casser les systèmes de chiffrement AES à 256 bits et en 9 rondes.



Une **ronde** (*round*) est le déroulement en une seule fois de toutes les étapes décrites par l'algorithme. Le nombre de *rounds* minimal de l'AES est relatif à la longueur de la clé. Il est respectivement de 10, 12 ou 14 pour une clé de taille 128, 192 ou 256 bits.

La robustesse des algorithmes de chiffrement asymétrique dépend pour l'essentiel d'avancées mathématiques concernant, entre autres, la théorie des nombres, la factorisation de grands nombres entiers et d'autre part, de la puissance informatique disponible pour effectuer des calculs.

La cryptanalyse peut se concentrer par exemple sur la résolution ou la réduction de la complexité de la factorisation des nombres.

En 1983, Donald Coppersmith¹² a d'ailleurs trouvé une méthode permettant de calculer les logarithmes discrets dans un temps polynomial qui varie linéairement avec la longueur de la clé. Celle-ci est devenue un outil incontournable pour les casseurs de l'algorithme Diffie-Hellman.

Par ailleurs, en février 2005, une équipe chinoise a démontré qu'elle avait cassé l'algorithme SHA-1 (*Secure Hash Algorithm*). Il faut savoir que l'algorithme SHA-1 est largement mis en œuvre dans les mécanismes de signature électronique. Ainsi, l'exploit réalisé par les scientifiques chinois ébranle la confiance que l'on peut avoir dans la sécurité réalisée par SHA-1.

De plus, c'est la première fois dans l'histoire de la cryptanalyse qu'un algorithme a été cassé sans que ceux qui l'ont démontré ne fassent connaître et partager à la communauté scientifique internationale la manière dont il a été cassé. Ce non-partage des connaissances diminue la capacité des autres scientifiques (et pays) à maîtriser le chiffrement.

12. Donald Coppersmith : <http://www.research.ibm.com/people/c/coppersmith>

Insistons sur le fait que tous les concepts de chiffrement qui exploitent les propriétés des mathématiques, qu'ils soient symétriques ou asymétriques, ne sont pas inconditionnellement sûrs. En effet, même en l'absence de la diffusion d'une méthode prouvant qu'un algorithme a été cassé, cela ne veut pas dire que la méthode n'existe pas ou que l'algorithme n'a pas été cassé. Aucune preuve mathématique ne permet d'affirmer que ce n'est pas possible, sauf pour la méthode dite du « masque jetable », s'il n'est utilisé qu'une seule fois. De plus, la robustesse des algorithmes asymétriques issus de la théorie des nombres ne peut pas être garantie dans le temps. C'est pour cela que de nouveaux paradigmes de chiffrement émergent, pour baser non plus la robustesse du chiffrement sur des principes mathématiques qui, à terme, seront cassés, mais sur des principes issus de la physique quantique. La faisabilité opérationnelle de tels mécanismes a été démontrée lors d'une première mondiale à Vienne en octobre 2008 dans le cadre du projet intégré européen SECOQC (*Development of a Global Network for Secure Communication based on Quantum Cryptography*)¹³.

5.2.4 Cryptographie quantique

Contrairement à la cryptographie classique, qui se base sur les mathématiques, la **cryptographie dite quantique** exploite les lois de la physique et notamment le concept d'incertitude tel que révélé par Werner Heisenberg¹⁴ en 1927.

Fonctionnement et principes de base

L'apport majeur des mécanismes quantiques pour le traitement de l'information réside dans le fait que les données peuvent être codées sur des photons de lumière (notion de **bit quantique** ou **qubit**), polarisés selon différentes orientations. Six types de polarisations sont possibles : horizontale (0°), verticale (90°), diagonale droite (45°), diagonale gauche (135°), circulaire droite et circulaire gauche.

Le concept d'un protocole de communication utilisant une transmission de **bits quantiques** — tel qu'énoncé par Gilles Brassard et Charles Bennett en 1984 par le protocole BB84 avec quatre états de polarisations — est de manière schématique le suivant (figure 5.3).

L'émetteur (Virginie) et le destinataire (Paul) communiquent à travers deux canaux : un **canal optique** (une fibre optique ou simplement l'air) et un **canal public** de communication comme Internet.

Paul et Virginie doivent se mettre d'accord sur la signification des polarisations des photons. Ils conviennent par exemple de retenir la **polarisation verticale** et

13. www.secoqc.net

14. Les bases de la physique quantique ont été élaborées par Einstein en 1905, ce sont les travaux du physicien Werner Heisenberg sur la mesure et l'observation des états de particules qui ont permis le développement de la physique dite quantique (http://www.nobel-winners.com/Physics/werner_karl_heisenberg.html). Durant les années 1980, l'information a pu être codée sur des photons, cette technologie a ensuite été appliquée à la cryptographie pour générer des secrets (clés cryptographiques).

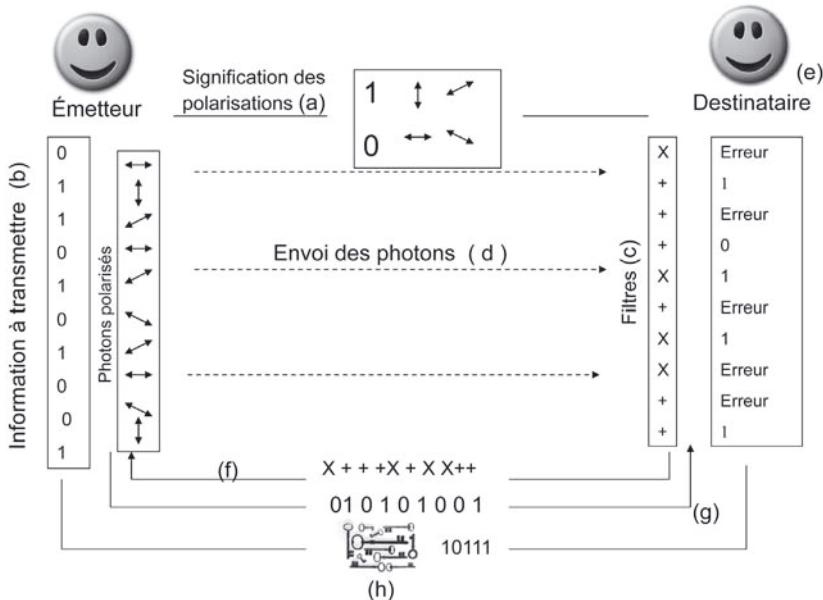


Figure 5.3 – Principes de base en cryptographie quantique.

diagonale droite pour coder l’information « **1** » ; **horizontale** et **diagonale gauche** pour coder l’information « **0** ». Cet accord peut être public (a).

Virginie génère ensuite une suite de bits aléatoires (comme par exemple 0110101001) et choisit au hasard la polarisation adéquate à chaque bit. Par exemple, le résultat est ceci « — | — / \ / — \ | ». Il est indispensable de coder un bit sur un seul photon (b).

De son côté, Paul, choisit au hasard une suite de bases (filtres) qui serviront à détecter le photon et à mesurer sa polarisation. Il existe deux types de filtre : un filtre « + », qui permet de mesurer les polarisations horizontale et verticale ; un filtre « X », qui permet la détection des photons ayant une polarisation diagonale. Prenons la configuration suivante « X + + + X + X X + + ». Notons qu’il n’existe pas de filtre capable de détecter, à la fois, les polarisations verticales-horizontales et les polarisations diagonales (c).

Virginie envoie, un par un, à Paul les photons polarisés sur le canal optique (d).

Du côté du destinataire, si la polarisation d’un photon ne correspond pas au filtre choisi, le photon est détruit. Paul perd donc l’information portée par le photon détruit. Dans notre exemple, Paul obtiendra les informations suivantes « erreur 1 erreur 0 1 erreur 1 erreur erreur 1 », i.e. Paul est alors en possession de la suite binaire suivante (10111) (e).

La taille de cette suite binaire est de l’ordre de 50 % de la taille du message original transmis. En effet, il existe une chance sur deux que le **filtre de réception** choisi par Paul corresponde à la polarisation des photons choisie par Virginie (le taux d’erreur relatif au fait que le filtre du récepteur soit mauvais est de l’ordre de 50 %).

Paul transmet à Virginie les filtres qu'il a choisis *via* le canal public, qui peut être non sécurisé (f).

Parmi ces filtres, Virginie en sélectionne certains (tout ou partie des filtres proposés par Paul, dont l'orientation laisse passer les photons polarisés et dont l'information peut être extraite). Ce processus s'appelle la **distillation¹⁵** (g).

À l'issue de cette réception, Paul applique une opération arithmétique et logique sur l'information envoyée par Virginie et sur le résultat de l'échange quantique. Il obtient un secret : la clé, dite **clé quantique**. Virginie effectue la même opération et détient également le même secret que Paul (h).

Ainsi, Virginie et Paul partagent un secret qu'ils sont seuls à connaître sans qu'il y ait eu la transmission du secret. Si le canal optique est espionné (écouté) durant la phase d'échange de photons, le taux d'erreur chez Paul augmente et passe d'une probabilité de 50 % à 75 %. Avec ce taux d'erreur, Paul sait que le canal optique est espionné et en informe Virginie.

Par ce mécanisme d'échange d'informations, constituant la clé secrète de chiffrement symétrique, basé sur la polarisation de photons et le choix de filtres, on peut assurer la confidentialité de l'information secrète générée et partagée par uniquement deux interlocuteurs sans que cette information soit stockée ou transmise. Cette information secrète peut être une clé de chiffrement à utiliser dans un système de chiffrement classique (AES par exemple).

Ce mécanisme de création d'une clé commune, partagée et à usage unique, est qualifié d'**inconditionnellement sécurisé**. Il est *a priori* impossible à un tiers de trouver la clé par un calcul mathématique, de la deviner, de l'intercepter, de la connaître. La clé ne peut donc être devinée ou soutirée à un utilisateur ou à un système.

De plus, la physique quantique permet de générer des nombres vraiment aléatoires et non prédictibles qui peuvent être utilisés pour construire les clés de chiffrement des systèmes de cryptographie classique, qui verraienr de ce fait leur niveau de sécurité augmenté.

Précisons qu'il ne s'agit pas ici de « chiffrement quantique », mais seulement d'utilisation des propriétés de la physique quantique pour apporter des solutions au chiffrement classique (basé sur les mathématiques).

5.2.5 Principaux algorithmes et techniques

Plusieurs algorithmes de cryptographie utilisant une transmission quantique de clés de chiffrement ont été publiés. Le premier fut le BB84, conçu par Gilles Brassard et Charles Bennett en 1984.



Les algorithmes de cryptographie quantique diffèrent selon le nombre d'états polarisés des photons, la sécurité apportée et la facilité d'implémentation.

15. La distillation est le processus qui permet d'obtenir un secret (une clé) à partir d'un échange de photons.

Le **protocole BB84** – décrit dans le paragraphe précédent – utilise quatre états de polarisation de photons. Il fonctionne d'une manière non déterministe. La sécurité de ce protocole a été démontrée à maintes reprises, entre autres par les travaux de Dominic Mayers¹⁶. Ce protocole, relativement facile à planter, est le plus commercialisé et utilisé.

Le **protocole à deux états** : Charles Bennett a annoncé, en 1992, que seulement deux états orthogonaux étaient nécessaires¹⁷.

Afin d'améliorer le protocole BB84, qui utilise des polarisations symétriques (verticale, horizontale et diagonale gauche, diagonale droite), le **protocole à trois états** propose l'utilisation de trois polarisations non symétriques (par exemple : verticale, diagonale gauche et circulaire droite). Le destinataire doit utiliser trois détecteurs. Ce protocole diminue la probabilité de détecter/trouver les polarisations correctes, aussi bien pour les attaquants que pour le destinataire.

Le **protocole à six états** ressemble au protocole à trois états, mais utilise les six polarisations possibles pour un photon.

Des techniques de génération de photons ont été inventées pour mettre en pratique la cryptographie quantique (la plupart sont basées sur le protocole BB84). Nous retiendrons les quatre principales techniques suivantes :

- **La technique de système à source d'impulsions cohérentes atténuées**¹⁸ est basée sur l'atténuation de la lumière émise par un laser à impulsion. Elle a fait l'objet de plusieurs études et brevets et est implémentée dans les produits cryptographiques commercialisés actuellement.
- **La technique dite de paires de photons intriqués**¹⁹ (*entangled photons*) consiste à générer deux photons intriqués. Un photon est alors envoyé à l'émetteur et l'autre au destinataire. Chaque entité mesure la polarisation du photon et puisque les photons sont intriqués, les mesures obtenues seront corrélées. Cette technique est supposée robuste dans la mesure où la clé de chiffrement ne sera créée que si les photons sont mesurés par les deux entités.
- **La technique dite de variable continue**²⁰ n'utilise pas la polarisation des photons pour coder l'information, mais la modulation ou la phase d'une impulsion de

16. Mayers D., Unconditional Security in Quantum Cryptography. *J. Assoc. Comput. Math.* 48, 351, 1998.

17. 1992. Clark, C. W ; Bienfang, J. C ; Gross, A. J ; Mink, A ; Hershman, B. J ; Nakassis, A ; Tang, X ; Lu, R ; Su, D. H ; Williams, C. J ; Hagley E. W ; Wen, J (2000). *Quantum key distribution with 1.25 Gbps clock synchronization*, Optics Express (2000).

18. Donald S. Bethune and William P. Risk (2002). AutoCompensating quantum cryptography. *New journal of physics* 4 (2002) 42.1-42.15 URL : <http://www.iop.org/EJ/article/1367-2630/4/1/342/nj2142.html>.

19. Artur Ekert (1991). Quantum Cryptography based on Bell's Theorem. *Physical Review Letters*. URL : http://prola.aps.org/abstract/PRL/v67/i6/p661_1.

20. Grosshans, F ; Van Assche, G ; Wenger, J ; Brouri, R ; Cerf, N. J ; Grangier, P (2003). Quantum key distribution using quassian-modulated coherent states. *Nature*. http://www.nature.com/cgi-taf/DynaPage.taf?file=/nature/journal/v421/n6920/full/nature01289_fs.html

lumière. Cela permet l'utilisation de plusieurs photons par impulsion (entre 100 et 250 photons).

Limites de la cryptographie quantique

L'application de la physique quantique à la cryptographie est actuellement **limitée à l'échange de clés cryptographiques** (QKD, *Quantum Key Distribution*), ou à la génération de vrais aléas qui entrent dans la création de clés secrètes pour le chiffrement symétrique. Le terme de cryptographie quantique est donc un abus de langage. Seul l'échange d'information permettant de générer une clé de chiffrement est basé sur une transmission quantique. La génération de clés quantiques peut être mise en œuvre avec des algorithmes de chiffrement et des protocoles cryptographiques existant principalement aux niveaux liaison, réseau, session ou application. La distribution quantique de clés permet de réaliser des réseaux métropolitains, des réseaux de capteurs ou encore des transmissions dans l'espace pour des applications civiles ou militaires.

Du fait notamment de la propriété du non-clonage d'un photon, la cryptographie quantique permet d'obtenir un niveau de sécurité qui peut être qualifié de robuste pour ce qui concerne la génération et l'échange de clés.

La normalisation de la cryptographie quantique a débuté en 2008 à l'ETSI (*European Telecommunications Standards Institute ; Industry-Specification Group (ISG)*)²¹ et des solutions commerciales émergent, toutefois leur adoption par le marché reste à faire. Outre le fait que la distribution quantique de clés ne résout qu'un des aspects de la problématique de mise en œuvre du chiffrement, des limites existent en terme de traitement des qubits, de l'industrialisation et de l'intégration de ces technologies, en particulier quand on souhaite transmettre des clés sur de longues distances.

5.3 SERVICES OFFERTS PAR LA MISE EN ŒUVRE DU CHIFFREMENT

5.3.1 Optimisation du chiffrement par une clé de session

L'inconvénient majeur d'un système de chiffrement à clé publique réside dans la lenteur de traitement des messages de taille importante. Aussi, pour réduire le nombre d'informations à coder par un système à clé publique, pour s'affranchir également du problème de distribution et de gestion des clés secrètes, et pour tirer parti du meilleur des systèmes de chiffrement symétrique et asymétrique, on combine leur usage.

Pour chiffrer les messages de grande taille, on utilise une **clé de session symétrique**, valide pour les deux interlocuteurs durant la durée de l'échange et détruite à la fin de la session de travail. De cette manière, seule la clé de session est chiffrée à

21. <http://www.etsi.org/WebSite/Technologies/QKD.aspx>

l'aide d'un algorithme asymétrique à clé publique, en utilisant la clé publique de son destinataire, tandis que le message, pouvant être long, est chiffré avec un algorithme symétrique à clé secrète, cette clé étant transmise chiffrée au destinataire.

L'échange sécurisé des données entre deux correspondants se déroule alors de la façon suivante (figure 5.4) :

- génération aléatoire, par un des partenaires de la communication, d'une clé secrète dite clé de session ;
- le message à émettre est chiffré avec cette clé et un algorithme à clé symétrique ;
- la clé de session est chiffrée avec la clé publique du destinataire, elle constitue alors l'**enveloppe digitale** du message ;
- le message chiffré et son enveloppe sont envoyés au destinataire ;
- le destinataire déchiffre l'enveloppe avec sa clé privée pour connaître la clé de session dont il se servira pour déchiffrer le message ;
- le destinataire peut alors utiliser cette même clé de session pour émettre des messages chiffrés à son interlocuteur.

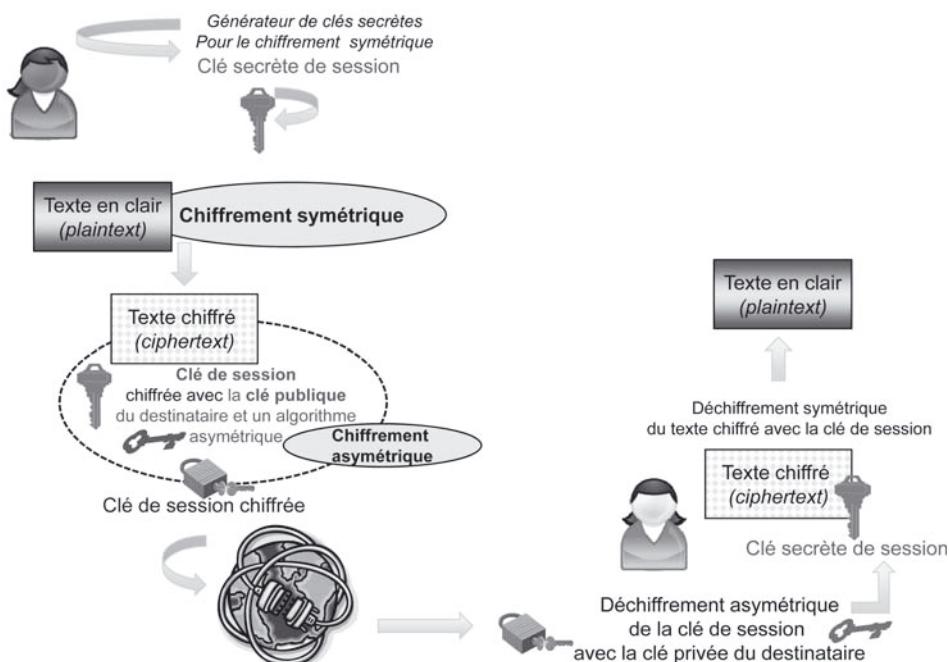


Figure 5.4 – Notions de clé de session et d'enveloppe digitale.

5.3.2 Vérifier l'intégrité des données

Vérifier que les données n'ont pas été modifiées lors de leur transfert est possible en y associant un **résumé** (condensat ou **empreinte**, ou encore en anglais, **hash**) qui est émis en même temps que les données. Celui-ci est le résultat d'une fonction de

calcul à sens unique appliquée aux données. Le destinataire recalcule avec la même fonction la valeur de l'empreinte à partir des données reçues. Si la valeur obtenue diffère, il en déduit que les données ont été modifiées. Bien sûr, si une personne qui n'est pas le destinataire intercepte le message, le modifie, recalcule l'empreinte et renvoie le tout au vrai destinataire, ceci ne prouvera donc pas que le message n'aura pas été modifié. L'empreinte peut être elle-même chiffrée par la clé de chiffrement asymétrique de l'émetteur, avant que les données ne soient émises ou stockées. Le déchiffrement de cette empreinte avec la clé asymétrique correspondante par le destinataire et la comparaison avec l'empreinte recalculée du message reçu prouvera alors réellement l'intégrité de ce message et prouvera l'identité de l'émetteur.

L'un comme l'autre, les systèmes de chiffrement à clé symétrique ou asymétrique permettent de savoir si des données transmises ont été modifiées, car leur déchiffrement devient alors impossible. Cela contribue à réaliser un contrôle d'intégrité, mais ne permet pas de s'assurer que des données n'ont pas été complètement détruites.

Pour un contrôle d'intégrité plus performant, on applique au message original une fonction le transformant en une petite suite aléatoire de bits qui constitue en quelque sorte son **empreinte digitale** (*digest, hash* ou encore *résumé*).

Une fonction dite **fonction digest** (ou *one-way hash function*), génère un message *digest*, c'est-à-dire son empreinte digitale, plus courte que le message original. Le but n'est pas d'obtenir une empreinte compréhensible, mais une empreinte qui caractérise le message. Celle-ci est ensuite chiffrée avec la clé privée de l'émetteur et associée au message à transmettre. À la réception du message et de son empreinte, le destinataire déchiffre cette dernière avec la clé publique de l'émetteur, trouvée dans un certificat numérique qui prouve que c'est bien la clé publique de l'émetteur, puis la recalcule à partir du message reçu avec la même fonction *hash*, et la compare ensuite avec celle reçue et déchiffrée. Si le résultat est identique, le destinataire a ainsi vérifié l'identité de l'émetteur et est assuré de l'intégrité du message. En effet, si le message est altéré, même légèrement, son empreinte est alors considérablement modifiée.

Par une utilisation conjointe des mécanismes de chiffrement et de signature on peut estampiller les messages pour garantir l'intégrité des données. Ces procédures sont consommatrices de temps de calcul et ralentissent de façon non négligeable les performances d'un environnement d'exécution, même s'il est sous-tendu par un réseau haut débit et des systèmes puissants. Il est donc primordial de ne les appliquer qu'en cas de nécessité absolue et donc de bien réaliser la phase en amont d'analyse de ce que l'on désire protéger et contre quoi. En déterminant correctement le degré de sensibilité des données ainsi que les objectifs de sécurité, on limite le chiffrement aux seules données pertinentes et aux applications et transactions concernées.

5.3.3 Authentifier et signer

Principe de la signature numérique

Le système de chiffrement asymétrique propose un mécanisme implicite de **signature de messages**. L'émetteur chiffre un message avec sa clé privée. Une entité

connaissant la clé publique de l'émetteur peut déchiffrer le message et le lire, cela signifie que le message a bien été créé à l'aide de la clé privée correspondante dont l'émetteur est censé être le seul propriétaire. On peut ainsi s'assurer de l'origine d'un message et en authentifier l'émetteur (figure 5.5).

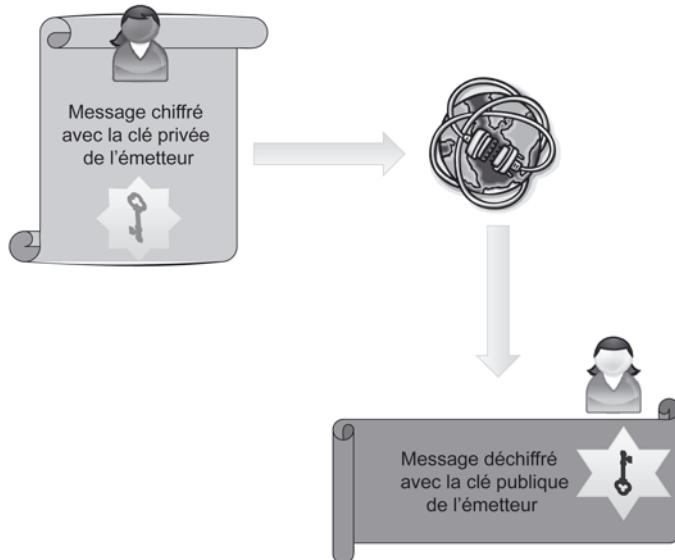


Figure 5.5 – Principe de base de la signature numérique.

Signer électroniquement un document est possible en utilisant un algorithme de chiffrement à clé publique. Pour cela, il suffit d'effectuer les actions suivantes :

- créer un petit message de déclaration d'identité tel que « je m'appelle Bobibi », le chiffrer avec sa clé privée pour constituer une signature que l'on attache au message à envoyer ;
- chiffrer ensuite le message et sa signature avec la clé publique du destinataire, puis émettre le message ;
- à sa réception, le destinataire déchiffre le message avec sa clé privée et détache la signature, qu'il déchiffre avec la clé publique de l'émetteur.

Cela contribue à réaliser l'authentification de l'émetteur. Lors de litige, la validation de cette preuve devra être faite par un organisme indépendant reconnu par les parties en contentieux.

Cependant, bien que performant, ce système de signature possède des failles. En effet, rien n'empêche de réutiliser la **signature digitale** d'un message en lieu et place de l'émetteur réel. Par ailleurs, on peut également constituer une **signature numérique** à la place d'un partenaire après lui avoir volé sa clé privée.

Augmenter le niveau de sécurité d'un mécanisme de **signature électronique** (authentification du message et de la signature) est possible en appliquant sur les données une fonction *hash* et en ayant recours à l'usage d'une infrastructure de gestion de clés offrant des services de certification (autorité de certification).

Une autre variante de mise en œuvre du mécanisme de signature consiste, pour une session de communication, à réaliser une génération aléatoire de déclaration d'identité. Cette dernière est envoyée au destinataire, qui la signe avec sa clé privée et qui la retransmet à l'émetteur. Pour cela, n'importe quel algorithme de chiffrement peut être utilisé.

Algorithme de signature DSA

En 1994, aux États-Unis, le NIST²² (*National Institute of Standards and Technology*) et la NSA²³ (*National Security Agency*) ont développé un algorithme dénommé **DSA** (*Digital Signature Algorithm*) pour être utilisé avec le standard DSS²⁴ (*Digital Signature Standard*) sur la base d'une variante de l'algorithme ElGamal. Son origine gouvernementale a freiné considérablement son adoption par la communauté scientifique et commerciale, notamment du fait du manque de confiance et de l'absence de garantie concernant la présence éventuelle de « porte dérobée » (*backdoor*) qui autoriserait des écoutes clandestines.

Cas particulier : Kerberos

Le service d'authentification **Kerberos** est un exemple d'authentification des applications par un serveur dédié. Il est né d'un projet de recherche développé au MIT (*Massachusetts Institute of Technology*)²⁵, le projet ATHENA. Ce service est réalisé par un serveur central d'authentification qui permet d'authentifier serveurs et utilisateurs de serveurs *via* des mots de passe.

Serveurs et clients doivent être enregistrés auprès du serveur Kerberos. Celui-ci stocke alors dans sa base de données des informations relatives à leur identification, à leurs mots de passe, à leurs permissions et droits d'accès (base de données du profil des utilisateurs). Kerberos partage avec chacun d'entre eux une clé secrète. Un serveur dessert alors plusieurs utilisateurs et serveurs qu'il connaît et qui appartiennent à son domaine (*Kerberos realm*). L'**authentification interdomaine** Kerberos est assurée par un mécanisme de dialogue entre différents serveurs Kerberos, à condition qu'ils se connaissent et qu'ils partagent pour cet échange une clé secrète.

Un utilisateur désirant réaliser une transaction auprès d'un serveur demande au préalable au serveur d'authentification de Kerberos un ticket de validité. Après vérification des droits d'accès des utilisateurs, le serveur retourne au client un ticket d'accord ainsi qu'une clé de session chiffrée avec une clé dérivée du mot de passe de l'utilisateur.

22. <http://www.nist.gov/>

23. <http://www.nsa.gov/>

24. *Federal Information Processing Standards Publication 186*, 1994 May 19 : <http://www.itl.nist.gov/fipspubs/fip186.html>

25. Le nom Kerberos fait référence au chien à plusieurs têtes, Cerbère, de la mythologie grecque, gardien des enfers <http://web.mit.edu/kerberos/>. La RFC 4120 traite de la version 5 de Kerberos (The Kerberos Network Authentication Service (V5)) <http://www.ietf.org/rfc/rfc4120.txt>.

L'utilisateur se sert de son mot de passe pour déchiffrer l'information produite par Kerberos et l'utilise pour effectuer la demande de validation pour l'utilisation d'un serveur particulier.

Étant basé sur l'échange de mots de passe, Kerberos est sensible aux attaques par mots de passe. Il est à protéger et à contrôler comme tous les éléments sensibles d'un système d'information.

5.3.4 Rendre confidentiel et authentifier

En théorie, une seule paire de clé peut servir à la fois au chiffrement du message et à l'établissement d'une signature numérique. Utiliser la même clé pour rendre confidentielles les données d'un message et pour authentifier son émetteur peut poser des problèmes de gestion et d'archivage de clés dont les besoins divergent. Il est souvent judicieux de disposer de **deux paires de clés** distinctes, l'une pour assurer la **confidentialité**, l'autre destinée à l'**authentification et à l'intégrité**.

En effet, pour la signature numérique, la clé privée doit être détruite à la fin de sa période d'activité. Si elle est découverte, les échanges pourraient être falsifiés, cela même après la fin de la validité de la clé privée. En revanche, si la paire de clés sert au chiffrement des messages, la clé privée doit être conservée le plus longtemps possible, car si la clé privée était perdue, il serait impossible de lire les données chiffrées avec la clé publique associée.

On voit donc que les deux applications de sécurité ont des exigences contradictoires sur les modalités de conservation de la clé privée.

5.3.5 Offrir un service de non-répudiation

Le service de **non-répudiation** consiste à prévenir le refus, le démenti qu'un message ait été émis ou reçu ou qu'une action, transaction ait eu lieu. Cela permet de prouver, par exemple, qu'une entité est liée à une action ou à un événement.

La non-répudiation est basée sur une signature unique ou sur une identification qui prouve qui a créé le message. Pour assurer ce service, on peut faire appel à un algorithme de chiffrement à clé publique. On peut également avoir recours à un tiers de confiance pour lui faire jouer un rôle de notaire. En effet, cet organisme « notarisera », enregistrera toutes les actions, transactions réalisées entre les prestataires pour pouvoir certifier la véracité des échanges. On voit effectivement apparaître, avec l'expansion des transactions commerciales et financières au travers d'Internet, un nouveau type d'intermédiaire et de service, celui de **cybernotaire**. On peut extrapoler ce rôle de garant de véracité d'informations à toutes sortes d'applications électroniques se déroulant dans le cyberspace.

5.4 INFRASTRUCTURE DE GESTION DE CLÉS

5.4.1 Clés secrètes

Les clés secrètes des systèmes de chiffrement, véritables données sensibles, nécessitent d'être gérées de manière fiable et confidentielle. Répétons-le, une clé est un

secret pour protéger un autre secret (notion de secret du secret). La sécurité du processus de chiffrement repose en grande partie sur la **sécurité**, la **confidentialité** et **l'intégrité** pour les clés publiques, attestée par les certificats numériques des clés utilisées, sur la robustesse des algorithmes et sur la sécurité des plates-formes matérielles et logicielles qui les supportent.

La **durée de vie** d'une clé de chiffrement (et de déchiffrement) dépend de son utilisation.

Les fonctions d'un système de gestion de clés sont celles qui permettent de réaliser les services de :

- génération d'une clé en fonction des besoins et des systèmes de chiffrement ;
- distribution des clés aux entités (vérification, authentification des entités, etc.) ;
- stockage des clés de manière sécurisée (chiffrement des clés, sécurité du serveur, archivage fiable afin d'assurer la confidentialité et l'intégrité des clés) ;
- surveillance (*monitoring*), d'enregistrement, d'audit, de traçage, de sécurité, de test de bon fonctionnement, d'alarme de contrôle d'accès aux clés, etc. ;
- destruction des clés inutiles (destruction physique, etc.).

Dans un système d'information, plusieurs clés de chiffrement sont généralement utilisées. Il peut alors exister une certaine hiérarchie des clés (notion de clé maîtresse, physiquement protégée, et de clés « filles » chiffrées à partir de celle-ci). Une **hiérarchisation des clés** répond au besoin de restreindre le nombre d'éléments de déchiffrement directement appréhendables. Des architectures à deux ou trois niveaux de clés sont courantes. À partir d'une clé de base (la clé maîtresse) sont dérivées, pour les architectures à deux niveaux, des clés de session et pour celles à trois niveaux, une clé de chiffrement des clés de session. Les systèmes de chiffrement à clé publique (ou asymétrique) sont basés sur ce type d'architecture. Minimiser le risque sécuritaire au niveau des clés implique de bien gérer les relations entre les clés et de définir correctement les recommandations attachées à l'utilisation de celles-ci.

5.4.2 Objectifs d'une infrastructure de gestion de clés

Afin de mettre en œuvre les mécanismes nécessaires à la réalisation des systèmes de chiffrement asymétrique, des infrastructures qui assurent la gestion et la distribution des clés sont nécessaires (**IGC, infrastructure de gestion de clés**, plus connues sous leur sigle anglais **PKI, Public Key Infrastructure**).

Il est impossible de mémoriser l'ensemble des clés publiques de tous les correspondants potentiels d'un environnement Internet. Leur demander leur clé publique préalablement à chaque envoi ne serait pas optimal. Le recours à une IGC ou **infrastructure à clé publique (PKI)** permet de répondre, d'une part, à la nécessité de disposer des clés de chiffrement afin de mettre en œuvre un système de chiffrement asymétrique à clés publiques et, d'autre part, au besoin de s'assurer de l'authenticité des clés publiques des correspondants (qui pourraient être fausses ou usurpées).

Les principales fonctions supportées par une infrastructure de gestion de clés sont :

- la génération d'un couple unique de clés (clé privée, clé publique), son attribution à une entité avec la certification de l'origine de la clé distribuée ;

- la création et la gestion de certificats numériques : signature, émission, validation, révocation, renouvellement des certificats ;
- la sauvegarde des informations nécessaires à la gestion des clés : archivage des clés, procédures de recouvrement en cas de pertes par l'utilisateur ou de demandes de mise à disposition par les autorités judiciaires ;
- la diffusion des clés publiques aux ressources qui la solliciteraient et qui seraient habilitées à les obtenir ;
- la certification des clés publiques (signature des certificats numériques par une autorité de confiance).

5.4.3 Certificat numérique

Un **certificat numérique** (certificat digital ou certificat électronique) constitue la carte d'identité numérique d'une entité (personne morale ou physique) ou d'une ressource informatique à qui il est associé. Il contient, entre autres, l'identification de son propriétaire, les dates de validité, la clé publique qui lui est attribuée ainsi que l'identification de l'organisme qui l'a délivrée (figure 5.6). Le tout est chiffré avec la clé privée de l'organisme de certification (signature de l'organisme). Le propriétaire du certificat le déchiffrera avec la clé publique de l'organisme de certification.



Figure 5.6 – Exemple de certificat numérique.

Selon le degré de vérification de l'identité de l'entité effectuant la demande d'obtention de certificat, différents types de certificats de niveaux variables de sécurité peuvent être émis. Plus le processus d'authentification est rigoureux, plus le niveau de confiance que l'on pourra avoir dans le certificat sera important.

La recommandation X.509 de l'UIT (Union internationale des télécommunications) propose un cadre architectural pour la réalisation d'un service d'authentification basé sur l'usage de certificats.

Sans spécifier un algorithme de chiffrement particulier, X.509 définit une structure de certificats basés sur des algorithmes à clé publique et signés par une **signature digitale**. La figure 5.7 présente les principaux champs et paramètres d'un certificat numérique selon la norme X.509v3 « *Directory authentication framework* ». La structure normalisée d'un **certificat X.509** est largement adoptée et est à la base de nombreuses solutions du marché comme par exemple S/MIME (*Secure/Multipurpose Internet Mail Extentions*), IPSec (*Internet Protocol Security*), SSL (*Secure Socket Layers*), SET (*Secure Electronic Transaction*) (cf. chapitre 9).

Version du certificat	
Numéro de série	
Algorithme utilisé pour signer le certificat	
Nom de l'organisme qui a généré le certificat <small>Le couple numéro de série – nom de l'organisme doit être unique</small>	
Période de validité	
Nom du propriétaire du certificat	
Clé publique du propriétaire	
Informations additionnelles concernant le propriétaire ou les mécanismes de chiffrement	
Signature du certificat <small>Algorithme et paramètres utilisés pour la signature et signature à proprement parlé</small>	

Figure 5.7 - Principaux paramètres d'un certificat numérique selon la norme X.509v3.

Pour valider le certificat reçu, le client doit obtenir la clé publique de l'organisme qui a créé le certificat relatif à l'algorithme utilisé pour signer le certificat (champ 3) et doit déchiffrer la signature contenue dans le dernier champ « Signature du certificat ». À l'aide des informations également contenues dans ce champ, le client calcule la valeur du condensé (résumé ou *hash*) et compare la valeur trouvée avec celle contenue dans le dernier champ ; si les deux valeurs correspondent, le certificat est authentifié. Ensuite, le client doit s'assurer que la période de validité du certificat est correcte.

Attestant que la clé publique, entre autres paramètres que le certificat contient, est bien celle qui correspond à la clé privée asymétrique que le propriétaire du certificat

est le seul à connaître, le certificat numérique est le garant de l'authenticité de son possesseur dans toutes les transactions. Encore faut-il, pour établir la confiance, connaître la manière par laquelle le certificat d'un individu lui a été attribué.

Pour établir la fiabilité d'un certificat numérique, différentes classes ont été définies :

- certificat de classe 1 : attribution sans vérification de l'identité du propriétaire ;
- certificat de classe 2 : le propriétaire décline juste son identité mais on ne vérifie pas que c'est bien la sienne ;
- certificat de classe 3 : le propriétaire du certificat doit être physiquement présent lors de sa remise et on vérifie qu'il est bien celui qu'il prétend être. Il peut aussi être exigé un support matériel (comme un token USB) pour lui remettre le certificat, on dit alors que le certificat est de classe 3+.

Suivant la classe, le prix d'un certificat n'est pas le même, ni le degré de confiance apporté. En France, seules les signatures numériques faites en utilisant un certificat de classe 3 sont reconnues équivalentes à une signature manuscrite.

Un certificat de classe 1 peut garantir par exemple que l'adresse e-mail de son propriétaire existe, mais ne dit pas qui est le propriétaire.

Un certificat de classe 2 a vérifié qui est le propriétaire d'après des renseignements envoyés par voie postale.

Un certificat de classe 3 implique que le propriétaire a été reçu physiquement par un employé de l'autorité de certification, qui lui a remis le certificat après avoir vérifié l'identité de son titulaire. La classe 3+ impose que le certificat a été remis sur un support cryptographique fiable. Seuls les certificats de classe 3+ sont reconnus à l'échelle européenne.

5.4.4 Organismes de certification

Un organisme reconnu compétent pour offrir ces services de gestion de clés publiques peut être qualifié de :

- **Tiers de confiance** : on accorde la confiance à cet organisme qui détient toutes les informations d'identification des utilisateurs et leurs clés de chiffrement. Toutefois, il ne faut pas oublier que la confiance est un sentiment : pas une preuve de sécurité !
- **Autorité d'enregistrement** : une clé ou un certificat sont obtenus sous réserve d'être enregistré — notion d'inscription auprès de l'organisme.
- **Autorité de certification** : notion de certification d'informations, elle signe électroniquement les certificats.
- **Autorité de dépôt et de séquestre** : données et transactions peuvent être mémo-risées à des fins de preuve et de non-répudiation afin de prouver *a posteriori* que des actions particulières ont bien eu lieu.

À l'instar d'un notaire, une autorité de certification peut enregistrer et prendre acte de la réalisation d'événements.



Quelle que soit son appellation, l'organisme qui met en place une infrastructure à clé publique (PKI, *Public Key Infrastructure*) a pour fonction principale de produire des certificats établissant la valeur de la clé publique attribuée à une entité (notion de certificats clients).

Un client émet une demande d'enregistrement (demande de certification) auprès d'une autorité de certification (inscription du client *via* un service web). Des preuves de l'identité du client peuvent être demandées par le serveur d'enregistrement selon les procédures d'identification et d'authentification mises en place par l'autorité.

Après validation des données, le serveur de certification génère les clés de chiffrement, privée et publique, et construit un certificat numérique, qui contient la clé publique, au nom du client, signe avec sa clé privée le certificat (certification du certificat numérique) et envoie le certificat au client. Ce dernier utilisera la clé publique de l'autorité pour s'assurer que le certificat est bien produit par l'autorité en question.

5.4.5 Exemple de transaction sécurisée par l'intermédiaire d'une PKI

Prenons pour exemple une entreprise et ses clients qui désirent s'échanger des données de manière confidentielle. Chacun doit s'assurer qu'il est bien en communication avec son interlocuteur (pour le client, le site web de cette entreprise ; pour l'entreprise, ce client). À cette fin, ils peuvent faire appel aux services proposés par une infrastructure à clé publique (figure 5.8).

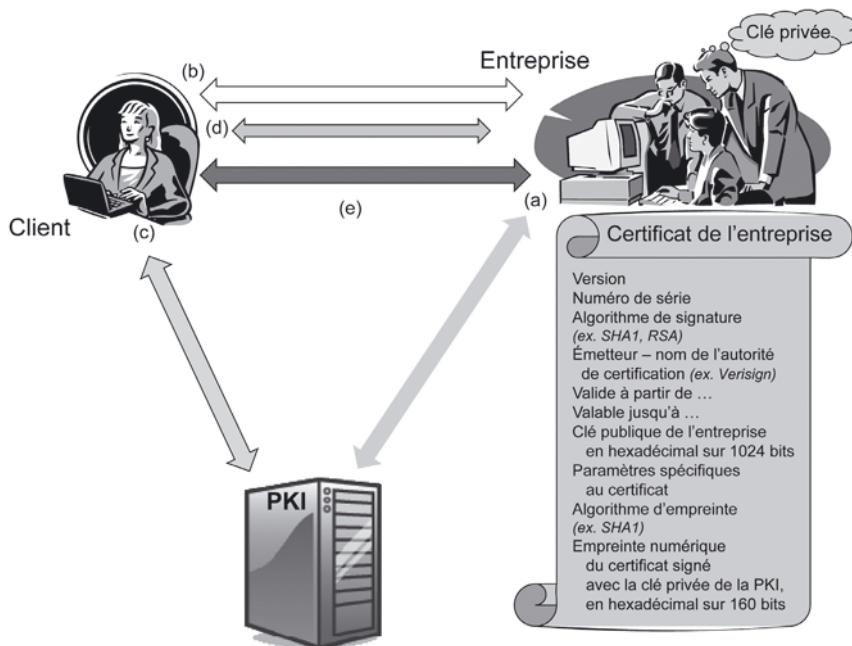


Figure 5.8 - Exemple d'échange faisant appel aux services offerts par une PKI.

L'entreprise doit tout d'abord s'enregistrer auprès d'une autorité d'enregistrement qui lui délivre un certificat numérique (a). Ce certificat est publié par la PKI et peut être délivré sur demande à des entités qui souhaitent communiquer avec l'entreprise.

Le certificat contient des informations sur l'entreprise, la PKI qui l'a délivré, l'algorithme de chiffrement, la fonction de *hashage* ainsi que sur la clé publique de l'entreprise. Ce certificat est signé avec la clé privée de la PKI. La clé privée de l'entreprise lui est transmise par la PKI par voie sécurisée (en mains propres ou par la poste par exemple).

Pour réaliser une transaction Internet sécurisée entre un système « client » et le site de l'entreprise, le client (par le biais de son navigateur web) doit se connecter sur le site web de l'entreprise (b) et obtenir le nom de la PKI ainsi que la référence du certificat numérique de l'entreprise (numéro de série du certificat).

Le navigateur du client se connecte alors sur le site de la PKI et télécharge le certificat de l'entreprise (c). Il s'assure de l'authenticité du certificat en vérifiant la signature du certificat avec la clé publique de la PKI (le certificat a bien été émis par cette PKI particulière). Il s'assure de l'intégrité des données en appliquant l'algorithme de *hashage* (les données contenues dans le certificat sont correctes, il s'agit bien de l'entreprise). Il extrait la clé publique de l'entreprise.

Le client génère ensuite une clé de session symétrique, selon le mécanisme intégré dans le navigateur, puis l'envoie en la chiffrant avec la clé publique de l'entreprise, à celle-ci (d).

Sur réception, l'entreprise déchiffre le message avec sa clé privée, obtient la clé de session qu'elle utilisera pour chiffrer/déchiffrer les données échangées avec ce client particulier durant une session de travail déterminée (e).

5.4.6 Cas particulier d'autorité de certification privée

Une entreprise peut émettre des certificats pour son propre compte et devenir sa propre autorité de certification. Ces certificats peuvent éventuellement se substituer au badge personnel, ils sont utilisés le plus souvent dans un **environnement intranet** et ne sont d'aucune autorité en dehors du contexte de l'organisation. La validité des certificats se limite aux frontières de l'entreprise et ceux-ci ne peuvent servir pour accéder à des serveurs internet externes à moins que le certificat ne soit lui-même signé par une autre autorité de certification reconnue. Il faut alors être capable de bien sécuriser la machine dédiée à l'attribution et à la gestion des certificats. La gestion d'un service de certification peut s'avérer complexe.

L'organisation peut, si elle le désire, créer une arborescence d'entités distribuées habilitées à délivrer des certificats et construire ainsi une hiérarchie de confiance. Elle **délègue** alors **la certification** à des départements ou à sites géographiques déterminés. Le certificat de la racine est utilisé occasionnellement pour signer ou pour renouveler les certificats des entités qui en dépendent. Ces dernières sont ainsi responsables de la certification des clients et des serveurs qui leur sont rattachés. Si la clé privée de la racine est compromise, tous les serveurs peuvent l'être. Certaines

entreprises isolent physiquement et déconnectent la machine « maître » du reste du réseau et la sécurisent fortement.

L'avantage principal, lorsque l'on devient sa propre autorité de certification, réside dans le fait que l'on possède un contrôle complet de la politique d'émission et de révocation des certificats. On est alors libre de déterminer la période de validité d'un certificat, d'en spécifier les attributs et de déterminer la façon dont les priviléges d'accès et les certificats sont liés.

5.4.7 Limites des solutions basées sur des PKI

Les limites inhérentes aux infrastructures de gestion de clés résident dans :

- la complexité, le coût du déploiement et de la gestion d'une infrastructure ;
- le haut niveau de sécurité nécessaire à la réalisation des services ;
- la validité, la durée de vie, la résiliation des certificats.

La **certification électronique** constitue une de ces mesures de sécurité, qui nécessite un cadre légal approprié, une organisation particulière, des ressources technologiques, des procédures et des personnes compétentes. C'est bien une infrastructure à part entière, lourde, complexe, consommatrice de ressources, d'ordre technologique mais aussi managérial, qu'il s'agit de déployer et de faire adopter par l'ensemble des acteurs de la chaîne numérique.

Comme il n'est pas souhaitable de ne disposer que d'une seule autorité mondiale de certification – du fait du pouvoir étendu et excessif qui lui serait *de facto* conféré, et de la volonté des pays d'avoir un cyberspace souverain, – diverses autorités de certification devraient exister. Il est alors nécessaire de déployer des mécanismes assurant leur interopérabilité. Toutefois, la multiplicité des autorités de certification pose le problème de leur reconnaissance mutuelle, de la compatibilité des certificats, qui devraient être tous en principe au format de la norme X509v3, et du champ de leur validité en vue de délivrer un service universel et reconnu par tous. Ainsi pour que les certificats numériques puissent être compréhensibles par tous les fournisseurs de e-services, garantissant l'interopérabilité des certificats, les fournisseurs de e-services qui nécessitent l'usage d'une PKI et les utilisateurs de ces e-services ont tout intérêt à souscrire à la même PKI et donc de dépendre de la même PKI, cela à l'échelle d'un pays, d'une région mais aussi au niveau international.

Enfin, il peut exister un relatif manque de confiance des utilisateurs dans les autorités de certification, dans la mesure où elles constituent des intermédiaires pour lesquels il n'y a pas de moyen de contrôle mis à disposition des utilisateurs pour bâtir la confiance envers ce tiers. Aucune garantie de leur capacité à garder des clés secrètes n'est offerte : quelle est la valeur réelle des certificats ? Quelle est la robustesse des mécanismes et procédures d'authentification offerts ? Comment sont protégées les données personnelles ? Quel niveau de sécurité est garanti pour la gestion des identités, pour la réalisation des transactions, etc. ?

Cette méfiance peut être renforcée par le fait que le plus souvent les utilisateurs passent par des autorités de certifications étrangères et les recours en cas de problème deviennent alors extrêmement difficiles à effectuer, voire impossible.

En effet, pour des raisons de performances, il pourrait être tentant de passer par une seule PKI qui serait en position de *leader* mondial de ce marché. Elle serait alors devenue l'intermédiaire incontournable de toutes les transactions qui nécessitent de la sécurité, et qui sont donc des transactions critiques.

Comment peut-on avoir confiance dans une entité qui détient la clé de tous les secrets et qui éventuellement les enregistre pour en prouver l'existence si nécessaire ?

De plus, si l'on tient compte du fait que les mécanismes de chiffrement mis en œuvre dans la signature électronique sont cassables (il a été démontré qu'ils ne sont pas inviolables), la robustesse de solution de sécurité basée sur la certification électronique semble désormais désuète. Dans ce contexte, quelles pourraient être les garanties qui permettraient de construire la confiance dans une infrastructure de gestion de clés (PKI) ? Par ailleurs, comment peut-on avoir confiance dans des institutions publiques ou privées qui dépendent pour la gestion de leur identité et de leur secret de telles infrastructures ?

Ainsi, tout laisse à penser que l'édifice de sécurité que sont la certification et la signature électronique ressemble à des infrastructures en béton de l'époque où l'on n'avait pas encore inventé le béton armé. Impossible de faire confiance au béton seul, le béton est cassable, pour lui faire confiance il faut de l'acier ! En poursuivant cette analogie, l'urbanisation de la société de l'information nécessite d'inventer le béton armé électronique.

Il est d'usage de dire que la confiance n'exclut pas le contrôle. Mais est-il vraiment possible de développer des procédures de contrôle sur les infrastructures tentaculaires que sont les PKI ? En effet, l'interopérabilité au niveau international des certificats nécessite la mise en place de PKI de structure hiérarchique, il s'agit en fait d'une arborescence de plusieurs PKI. Une PKI peut être locale mais elle dépend le plus souvent d'une suprastructure régionale ou internationale. Il s'agit alors de filiales qui agissent par procuration et qui dépendent d'une maison mère, située dans un autre pays, voire sur un autre continent, et dont les lois sont celles du pays où est situé le siège social de celle-ci.

Lorsqu'il s'agit de définir des stratégies nationales de sécurité, il ne faut pas faire l'économie de la compréhension des différentes dimensions des problématiques **géostratégique**, technique et idéologique liées au contrôle d'Internet, et ce contrôle passe par celui de la gestion des identités et des accès et des mesures de sécurité et donc des PKI.

Toute démarche de sécurité répond à celle de la gestion des risques et donc des opportunités. La frontière entre le **risque acceptable** et celui qui ne l'est pas et qui nécessite des mesures particulières de sécurité est parfois difficile à déterminer objectivement et dépend fortement du **contexte politique** et des objectifs d'un pays. Une stratégie nationale de sécurité n'échappe pas à ce contexte. Il est donc primordial de pouvoir identifier les multiples facettes des dépendances et des interdépendances de solutions et fournisseurs de solutions et de ne pas s'arrêter uniquement aux aspects matériels, techniques « palpables » des solutions de sécurité. La balance des intérêts doit permettre de trouver le bon équilibre entre dépendance, **souveraineté**, sécurité,

qualité de service, coûts, faisabilités organisationnelles, techniques et juridiques et aussi, délais de disponibilité.



Le bon sens nous fait penser que des situations de dépendance ou de monopole en matière de sécurité ne sont pas forcément les meilleures sur le long terme.

5.5 APPOINT DES BLOCKCHAINS

La confiance en l'intégrité d'une transaction et l'authenticité de l'émetteur et du récepteur sont supportés par les technologies de chiffrement et par la signature électronique. Le chiffrement asymétrique qui achemine la clé secrète symétrique, de même que la signature électronique, repose sur l'utilisation de certificats. Les utilisateurs utilisent ces certificats parce qu'ils sont signés par une autorité à laquelle les émetteurs et les récepteurs font confiance. La confiance est donc ici centralisée chez le signataire des certificats, tout comme dans une transaction immobilière on fait confiance à un notaire.

Mais ce scénario où la **confiance** repose sur une autorité centralisatrice est-il obligatoire ? N'existe-t-il pas une autre solution où la confiance reposera sur l'ensemble des utilisateurs, émetteurs et récepteurs, plutôt que sur une autorité centralisatrice ? C'est à ce besoin que répond la technologie « **blockchain** », où la confiance est distribuée entre tous grâce aux mécanismes de la cryptographie.

Avec la blockchain ou « **chaîne de blocs** », l'émetteur et le récepteur échangent en toute sécurité des éléments sans qu'une autorité centrale n'ait à les valider. C'est le cas par exemple pour les **bitcoins** et autres monnaies virtuelles. Aucune banque, aucun État, ne doit se porter garant de cette monnaie, tous les utilisateurs sont garants de l'intégrité des transactions. Toute transaction est chiffrée (par la clé publique du récepteur) et signée. Elle est alors soumise à plusieurs nœuds du réseau (les mineurs) qui réalisent des opérations de cryptographie, avant de valider le bloc. Ce bloc est ajouté alors à un registre, puis d'autres blocs viennent s'y ajouter. Ce registre est dupliqué sur tous les nœuds du réseau qui utilisent cette blockchain. Impossible de modifier incognito ce registre, tous s'en apercevraient puisqu'ils n'auraient plus le même contenu du registre qu'ils hébergent. De la confiance de tous est induite la confiance de chacun, et chacun est le garant de la confiance de tous.

Une blockchain n'est pas unique. Il peut y avoir une blockchain pour un vote par Internet dans un pays ou un comité d'entreprise, une autre blockchain pour les diplômes d'une université ou d'une grande école, et une autre pour gérer les bitcoins. Avec cette technologie, le tiers de confiance qui signe les certificats numériques est toujours nécessaire pour attester que la clé publique contenue dans le certificat est bien celle qui correspond à telle clé privée, mais c'est à l'ensemble des utilisateurs qu'on fait confiance, pas à une seule autorité de confiance.

La mise en œuvre du concept de blockchain devrait se multiplier et de nombreux services autour de cette technologie basée sur le chiffrement à clé publique seront sans doute proposés.

Résumé

Dans un environnement informatique, la mise en œuvre des techniques de chiffrement permet de réaliser la confidentialité des données, de vérifier leur intégrité et d'authentifier des entités.

Divers algorithmes de chiffrement existent. Quel que soit leur mode opératoire (symétrique ou asymétrique), ils reposent sur l'usage de clés. Généralement leur degré de robustesse est lié à la capacité à gérer les clés de chiffrement de manière sécurisée, à la longueur de la clé (attention la longueur minimale de la clé est fonction du type d'algorithme), et à la sécurité de la plate-forme matérielle et logicielle dans laquelle les algorithmes de chiffrement sont implantés.

La confiance envers les solutions de chiffrement commercialisées ne peut être que toute relative, dans la mesure où aucune garantie, aucun moyen de vérification ne sont offerts (existe-t-il des portes dérobées — *backdoor* — dans les logiciels ? Les clés secrètes ont-elles été dupliquées, divulguées ? etc.).

Par ailleurs, aucune preuve n'est donnée quant au fait que les algorithmes actuellement réputés fiables le seront encore dans un futur proche. Une alternative pour pallier au défaut de sécurité inconditionnelle de la cryptographie classique est de réaliser des mécanismes de chiffrement basés sur la cryptographie quantique.

La mise en œuvre du chiffrement asymétrique, l'usage de certificats numériques et de la signature électronique, via des infrastructures à clés publiques (PKI) et des tiers de confiance (autorités de certification) s'avèrent être une solution possible mais non optimale en termes de complexité de déploiement, de coûts, de performances et du niveau de sécurité réellement offert.

Exercices

5.1 Quels sont les principaux avantages, inconvénients et limites associés au chiffrement symétrique ?

5.2 Quels sont les principaux avantages, inconvénients et limites associés au chiffrement asymétrique ?

5.3 Pourquoi l'usage du chiffrement asymétrique pourrait-il être préféré à celui du chiffrement symétrique dans des transactions commerciales sur Internet ? Dans quelles circonstances le chiffrement symétrique peut-il être utilisé ?

5.4 Qu'est-ce qui permet de qualifier de robuste un algorithme de chiffrement ?

5.5 Pourquoi est-il difficile d'avoir confiance dans des produits de chiffrement commercialisés ?

5.6 À quels besoins répond une infrastructure de gestion de clés (PKI, *Public Key Infrastructure*) ?

5.7 Citez quelques inconvénients et quelques limites des infrastructures de gestion de clés (PKI).

5.8 Quel est le rôle d'un certificat numérique ? Pourquoi un certificat numérique comporte-t-il un champ « durée de validité » ?

5.9 Quels sont les principaux apports de l'utilisation de la physique quantique à la cryptographie ?

5.10 Pourquoi certains algorithmes de chiffrement possèdent-ils un mode opératoire dit de « *block cipher* » ? À quels besoins correspond-il ?

5.11 Quels sont les facteurs de faiblesse des clés de chiffrement ?

5.12 Que signifie un mode hybride de chiffrement ?

5.13 Expliquez la notion de « *digest* », quels services de sécurité permet-elle de réaliser ?

Solutions

5.1 De manière générale, la mise en œuvre d'un système de chiffrement permet de réaliser des services de confidentialité, d'authentification et de vérification de l'intégrité des données et éventuellement de non-répudiation.

La mise en œuvre d'un procédé de **chiffrement symétrique**, basé sur l'usage d'une même clé secrète pour chiffrer à l'émission et déchiffrer des données à leur réception, peut être performante du point de vue de la rapidité des actions de chiffrement/déchiffrement. Toutefois, l'inconvénient majeur est lié au fait que chaque paire de communicants doit posséder une même clé, ce qui pose des problèmes de gestion et de distribution des clés.

Ces clés (véritables secrets servant à protéger des secrets) doivent être distribuées et sauvegardées de manière sécurisée. De plus, ce système n'est pas approprié, tout seul, dans l'environnement Internet, qui fonctionne pour l'essentiel en mode client/serveur, car si tous les clients d'un même serveur possédaient la même clé, rien ne serait vraiment confidentiel.

5.2 Dans un système de **chiffrement asymétrique**, la clé de chiffrement diffère de la clé utilisée pour le déchiffrement, mais ces clés sont mathématiquement liées. Pour mettre en œuvre un système de chiffrement asymétrique, il faut utiliser une bi-clé constituée d'une clé privée (secrète, connue de son seul propriétaire) et d'une clé publique (non secrète et mise à la disposition de tous les interlocuteurs habilités à l'obtenir, dans des certificats numériques). L'avantage principal réside dans le fait qu'il n'est pas nécessaire de partager une même clé secrète. En revanche, la gestion des clés des systèmes de chiffrement asymétrique fait appel à une infrastructure de gestion de clés (PKI, *Public Key Infrastructure*) relativement complexe, dans laquelle les clients doivent avoir confiance et qui constitue un intermédiaire incontournable.

Les limites des chiffrements asymétrique et symétrique résident d'une part sur le fait que les algorithmes sont basés sur une logique mathématique (qui peut être cassée) et sur des clés qui doivent être gérées comme des secrets (qui peuvent être découverts) et d'autre part sur le fait que les systèmes de chiffrement sont mis en œuvre sur des plates-formes matérielles et logicielles non fiables. La vulnérabilité essentielle des systèmes de chiffrement est liée à l'environnement informatique dans lequel ils s'exécutent, sans oublier les utilisateurs qui ne protègent pas suffisamment leurs clés privées.

5.3 L'**usage du chiffrement asymétrique** est préféré dans des transactions commerciales, du fait qu'il résout le problème de la distribution des clés, *via* l'usage de certificats numériques mis à disposition des correspondants par une tierce partie de confiance (l'infrastructure de gestion de clés). Chaque acheteur possède sa propre clé et le vendeur ne doit pas toutes les connaître. Le chiffrement symétrique peut toutefois être utilisé dans la réalisation de service de contrôle d'intégrité (fonction *hash, digest*) pour réaliser des empreintes ou des résumés.

Pour des raisons de rapidité de chiffrement de gros volumes de données à transmettre, les chiffrements asymétrique et symétrique sont combinés et on tire ainsi parti de leurs avantages réciproques. Le chiffrement asymétrique étant utilisé pour chiffrer/déchiffrer les clés de chiffrement symétrique.

5.4 Un **algorithme de chiffrement** est qualifié de **robuste** tant que des processus de cryptanalyse n'ont pas démontré sa fragilité. Il s'agit le plus souvent de réputation au regard de la résistance des algorithmes aux diverses attaques connues. Ce qui est considéré comme robuste et relativement fiable aujourd'hui ne le sera pas forcément demain !

5.5 Il est extrêmement difficile d'avoir confiance dans les **solutions cryptographiques commercialisées** dans la mesure où il est impossible de les contrôler, de savoir si elles intègrent ou non des portes dérobées (*backdoors*), qui permettent le contrôle et la surveillance des données confidentielles à l'insu de l'utilisateur légitime, de savoir si les clés secrètes sont vraiment gardées secrètes, si elles ne sont pas prédictibles, cassables, communiquées à des tiers, etc.

Il en est de même des infrastructures à clé publique et des certificats numériques, dans lesquels les utilisateurs doivent avoir confiance sans pour autant disposer des moyens de contrôle ou de garanties de sécurité.

5.6 Une **infrastructure de gestion de clés** (PKI) permet de répondre aux besoins de disposer de clés de chiffrement pour réaliser certains services de sécurité *via* la mise en œuvre du chiffrement asymétrique entre acteurs qui *a priori* ne se connaissent pas, mais font confiance à une autorité commune.

5.7 La mise en œuvre de services offerts par une **infrastructure de gestion de clés** (PKI) peut poser des problèmes d'ordre différent, comme par exemple :

- **Problème politique** : la majorité des infrastructures PKI et des autorités de certification appartiennent à des entités étrangères. Cela soulève diverses questions dont :
 - ◊ celle de la *confiance* dans ces entités pour les services offerts (création, sauvegarde, distribution des clés privées et publiques, des données d'identification, notarisation des événements) et pour le manque de garantie de l'usage non abusif des données, de la neutralité dans les échanges, de moyens de recours en cas de litige avec l'autorité de certification ;
 - ◊ celle des performances ;
 - ◊ celle de la souveraineté
- **Problème technologique** : les systèmes de chiffrement classiques peuvent être cassés, certains certificats numériques n'ont aucune valeur sécuritaire et ne garantissent rien, des fraudes sont possibles ; la sécurité des infrastructures est assurée par des moyens classiques de sécurité qui peuvent être contournés. De plus, l'usage d'une infrastructure de gestion de clés déplace le problème de la sécurité des échanges mais ne le résout pas à proprement parler.
- **Problème organisationnel** : interopérabilité des infrastructures, déploiement, gestion, maintenance, sécurité, complexité, coûts.

5.8 Le **certificat numérique** peut être vu comme le passeport numérique d'une entité morale (organisation) ou physique (personne). La création et la diffusion d'un certificat contribuent à distribuer la clé publique d'une entité afin de mettre en œuvre des systèmes de chiffrement asymétrique et d'offrir des services de confidentialité, d'authentification et d'intégrité.

Toutefois, bien que contribuant à réaliser la sécurité des transactions, un certificat peut être altéré ou falsifié (par infection virale du poste de travail de l'utilisateur par exemple). La gestion d'une liste de révocation de certificats (CRL, *Certificate Revocation List*) dans laquelle les certificats périmés sont inscrits, introduit des temps de traitement additionnels et est d'une efficacité relative. Le champ « durée de validité » permet de limiter dans le temps, la durée de vie d'un certificat et d'avoir, à l'occasion de son renouvellement, la possibilité de modifier, de mettre à jour certains de ses paramètres. Cela permet d'effectuer des contrôles de validité des certificats, de vérifier que le certificat est valide en fonction de sa date d'expiration et de mieux gérer les changements qui surviennent dans l'organisation représentée par le certificat.

5.9 À l'heure actuelle, la **physique quantique** permet de créer de vrais aléas qui interviennent dans la création des clés de chiffrement non prédictibles, des masques à usage unique, et permet aux utilisateurs de les obtenir sans avoir besoin au préalable de les distribuer sur un réseau non fiable.

L'usage de clé cryptographique augmente le niveau de sécurité des entités et processus qui y font appel. En effet, le mécanisme de génération et d'échange d'information pouvant être basé sur la polarisation de photons et le choix de filtres, via la mise en œuvre des principes de physique quantique, permet d'en assurer une meilleure

confidentialité et protection. Cette information ne peut être recréée, réutilisée, écouteée ou volée. La physique quantique permet de créer et d'acheminer des secrets inviolables, qui peuvent être des clés de chiffrement utilisables dans un système de chiffrement classique (AES par exemple).

5.10 Le *Cipher Block Chaining* (chaînage de blocs) est un mode où le chiffrement d'un bloc de données dépend du précédent. Cette technique permet de renforcer le niveau de robustesse des algorithmes en augmentant le niveau de difficulté du déchiffrement de l'ensemble des données (des blocs de données isolés ne pourront pas être déchiffrés).

5.11 Les facteurs de faiblesse des clés de chiffrement sont liés à leur nature, à leur durée de vie et à leur utilisation. Le processus de création/distribution/sauvegarde/destruction doit être fiable, produire des clés intègres, non cassables, non devinables, non prévisibles. Les clés corrompues ou inutiles doivent pouvoir être non réutilisées et détruites. Chacune de ses activités pose des problèmes de sécurité, de gestion et de logistique.

La faiblesse majeure liée aux clés secrètes réside dans le fait qu'elles doivent rester secrètes et donc elles aussi sécurisées (notion de récursivité de la sécurité).

5.12 Dans un mode hybride de chiffrement, plusieurs techniques de chiffrement sont combinées. Généralement on établit une session de travail *via* un mécanisme de chiffrement asymétrique afin de pouvoir déterminer quel sera l'algorithme de chiffrement symétrique et la clé à utiliser durant cette session de travail.

Cela résout dans une certaine mesure les problèmes de lenteur du chiffrement asymétrique et de l'établissement d'une clé commune secrète liée au chiffrement symétrique qui peut alors être transmise de manière sécurisée.

5.13 Un *digest* est l'empreinte digitale d'un message, c'est un condensé obtenu par l'application d'une fonction à sens unique sur le contenu des données. Celui-ci est une chaîne de bits et ne permet pas de retrouver le message initial (notion de fonction à sens unique) mais permet, selon sa mise en œuvre, de s'assurer qu'un message n'a pas été altéré. Ainsi, un digest contribue à réaliser un service d'intégrité. Combiné au chiffrement asymétrique, il peut également contribuer à offrir un service d'authentification de l'émetteur.

LA SÉCURITÉ DES INFRASTRUCTURES DE TÉLÉCOMMUNICATION



PLAN

- 6.1 Protocole IPv4
- 6.2 Protocoles IPv6 et IPSec
- 6.3 Sécurité du routage
- 6.4 Sécurité et gestion des accès
- 6.5 Sécurité des réseaux

OBJECTIFS

- Présenter les mécanismes contribuant à la sécurité des infrastructures de télécommunication Internet.
- Analyser les limites de la version 4 du protocole IP au regard des besoins de son évolution vers un mode qui intègre des mécanismes de sécurité.
- Présenter les protocoles IPv6 et IPSec.
- Présenter l'importance de la gestion des noms et des adresses ainsi que des processus de routage du point de vue de la sécurité des réseaux.
- Définir les notions de gestion des identités, des autorisations et des accès.
- Examiner les outils de réalisation du contrôle d'accès.
- Présenter une réflexion sur une approche globale de protection des infrastructures réseau.

6.1 PROTOCOLE IPv4

© Dunod – Toute reproduction non autorisée est un délit.

La version 4 du **protocole Internet** (IPv4), qui existe depuis l'origine du réseau Internet, est encore largement utilisée. Or ce protocole n'intègre aucune fonction ou mécanisme de sécurité. En effet, IPv4 ne permet ni l'authentification de la source ou de la destination d'un paquet, ni la confidentialité des données ou celle des adresses IP. La structure d'un paquet IP formaté par le protocole IPv4¹ est donnée par la figure 6.1.

1. IPv4 : RFC 0791, <http://www.ietf.org/rfc/rfc0791.txt> IPv4 et principaux protocoles de la suite TCP/IP : TCP : RFC 0793, <http://www.ietf.org/rfc/rfc0793.txt> UDP : RFC 0768, <http://www.ietf.org/rfc/rfc0768.txt> FTP : RFC 0959, <http://www.ietf.org/rfc/rfc0959.txt> HTTP version 1.1 : RFC 2616, <http://www.ietf.org/rfc/rfc2616.txt> Telnet : RFC 0854, <http://www.ietf.org/rfc/rfc0854.txt>

Chapitre 6 • La sécurité des infrastructures de télécommunication

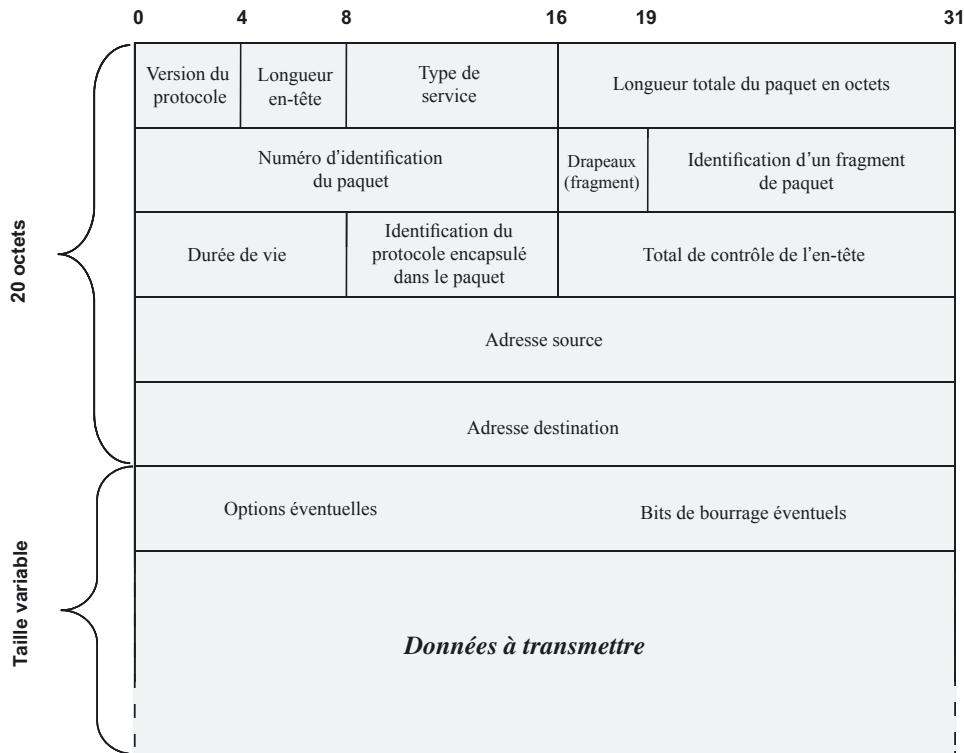


Figure 6.1 – Structure d'un paquet IP formaté par le protocole IPv4.

Le protocole IP, qui s'exécute en mode sans connexion, offre un service non fiable de remise de paquets IP (notion de *best effort*). Ainsi, IPv4 ne garantit pas :

- la remise des données (perte possible de données, pas de mécanisme de reprise sur erreur, c'est le protocole TCP qui offre ce service) ;
- la livraison de données au bon destinataire ;
- l'ordonnancement (séquencement) correct des données à leur réception ;
- la confidentialité et l'intégrité des données transmises (les données peuvent être interceptées, copiées, modifiées ou détruites lors de leur transfert) ;
- l'authentification de la source ou de la destination des données.

Dans le mode non connecté, le fait qu'une liaison logique ne soit pas préalablement établie entre un émetteur et un destinataire signifie que l'émetteur envoie ses paquets sans en avertir le destinataire et qu'ils peuvent se perdre, prendre des routes différentes, ou arriver dans le désordre. La qualité de service n'est donc pas garantie. Un paquet IP peut donc être perdu, modifié, dupliqué, fabriqué (forgé) ou être remis hors séquence. La prise en compte du manque de qualité de service du protocole IP a amené à implanter, dans les systèmes d'extrémité, le **protocole TCP** (*Transmission Control Protocol*). TCP offre un service de transport fiable en mode connecté (niveau 4 de l'architecture OSI). Toutefois, le protocole TCP n'offre pas de service de sécurité à proprement parler (figure 6.2).

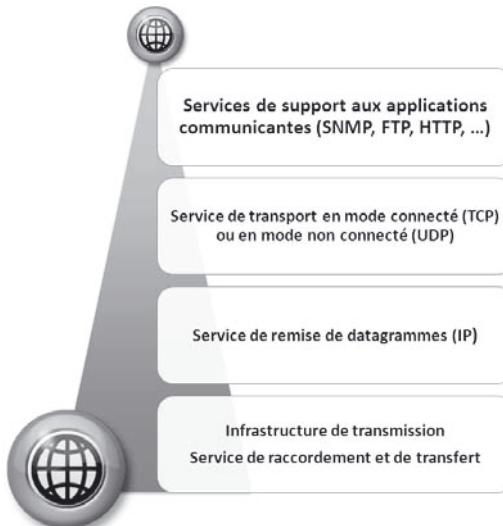


Figure 6.2 – L'architecture TCP/IP.

Prise en compte de nouveaux besoins

Dans le milieu des années 1990, le manque de sécurité du protocole IP a conduit à la mise en place de routeurs filtrants (pare-feu, *firewalls*)², pour se protéger de certains paquets non conformes à la politique de sécurité de l'organisation et empêcher leur arrivée ou leur émission. Néanmoins, cela ne permet pas d'éviter les écoutes passives ou actives d'information (interception et détournement de données).

Outre la nécessité de pouvoir offrir des services de sécurité, le protocole IP doit également satisfaire les besoins de communication d'un nombre croissant de systèmes interconnectés et des applications multimédias. Cela s'exprime par la nécessité de pouvoir :

- rendre confidentiel le contenu des paquets, authentifier leur source et leur destination, s'assurer de l'intégrité des paquets ;
- disposer d'une plage d'adresses plus importante et d'augmenter le nombre d'adresses Internet disponibles pour identifier un plus grand nombre de systèmes ;
- faire une allocation dynamique de bande passante en fonction des besoins de performances des applications multimédias.

Ainsi, la révision de la version 4 du protocole Internet a fait l'objet d'une refonte complète connue sous le nom d'**IPnG** (*Internet Protocol next Generation*) ou **IP version 6** (IPv6)³.

En fait, la version 5 du protocole IP, encore appelée *Internet Stream Protocol* version 2 (ST2), définie par le RFC 1819, a bien existé au début des années 1980

2. Les pare-feu sont traités au chapitre 8.

3. IPv6 : RFC 1883 en 1995, remplacée en décembre 1998 par la RFC 2460, <http://www.ietf.org/rfc/rfc2460.txt>

mais est restée au stade de l’expérimentation. IPv5 n’a jamais été implanté dans les réseaux commerciaux. Il apportait à l’IPv4 la notion de qualité de service de bout en bout dans les transferts en flux continu, comme par exemple pour la voix sur IP (VoIP). L’Internet « *Next Generation* » IPnG s’est parallèlement surtout soucié de résoudre la pénurie des adresses IPv4 en étendant l’en-tête IP de 4 à 16 octets. Mais l’IPnG n’était pas compatible avec l’IPv5. L’IPnG a été renommé IPv6, ce qui explique le saut direct entre IPv4 et IPv6.

6.2 PROTOCOLES IPv6 ET IPSec

6.2.1 Principales caractéristiques d'IPv6

Les principales évolutions d'**IPv6** portent sur les points suivants (RFC 2460) :

- le support d’un adressage étendu et hiérarchisé. Les adresses sont codées sur 128 bits (16 octets) et non plus sur 32 bits (4 octets). La représentation des adresses s’effectue en nombres hexadécimaux séparés par des deux points tous les deux octets et non plus en notation décimale pointée⁴ ;
- l’allocation dynamique de bande passante pour le support d’applications multimédias ;
- la création des réseaux IP virtuels ;
- le support de procédures d’authentification et de chiffrement ;
- des en-têtes des paquets simplifiés afin de faciliter et d’accélérer le routage.

La structure d’un paquet de données formatées avec IPv6 est présentée par la figure 6.3.

L’IETF (*Internet Engineering Task Force*)⁵ a établi en 1995 plusieurs documents (RFC 1825 à 1829), spécifiant les manières de sécuriser une infrastructure Internet, qui traitent respectivement des thèmes suivants : aperçu général d’une architecture de sécurité pour IP ; facilité d’authentification et de chiffrement ; mécanisme d’authentification et de chiffrement.

Le support de ces services est obligatoire dans la version 6 du protocole Internet (IPv6) et facultative dans la version 4.

La migration de la version 4 vers la version 6 du protocole IP sur l’ensemble des routeurs du réseau Internet soulève des problèmes économique et technologique, liés à son déploiement, car l’adoption d’IPv6 impose notamment :

- la modification du schéma d’adressage et de la gestion des adresses⁶ ;
- le support des versions 4 et 6 pendant la période de transition ;
- la synchronisation à grande échelle de la migration des versions.

4. Alphabet d’un système de numération hexadécimal (base 16) : 0 1 2 3 4 5 6 7 8 9 A B C D E F Exemple d’adresse IPv6 : 0123::4567::89ab::cdef:0123::4567::89ab::cdef Exemple d’adresse IPv4 : 130.223.0.0

5. IETF : <http://www.ietf.org>

6. RFC 1886 a identifié en 1995 les modifications à effectuer dans les DNS pour supporter IPv6.

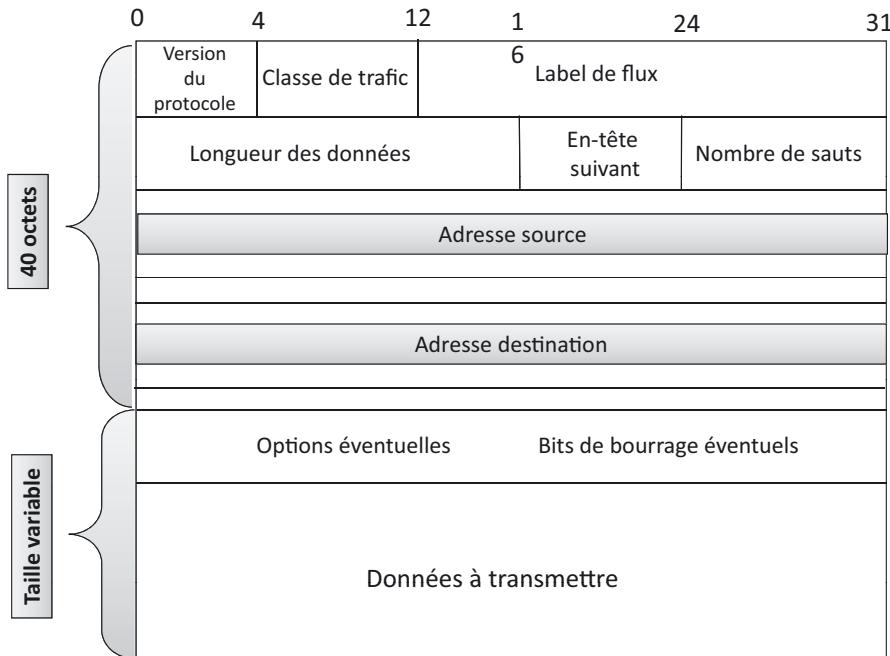


Figure 6.3 – Format d'un paquet IPv6.

Pour toutes ces raisons, la version 6, bien que spécifiée en 1995, n'est toujours pas largement implantée et aucune incitation gouvernementale ou recommandation internationale ne semble pouvoir imposer son adoption sur l'ensemble des réseaux. Seules certaines infrastructures, notamment privées, intègrent IPv6 en mode natif, ou les pays n'ayant pas une infrastructure IPv4 très développée, comme la Chine, qui sont passées directement à l'IPv6.

6.2.2 Principales caractéristiques d'IPSec

Pour toutefois répondre aux besoins de sécurité, sans pour autant devoir modifier tout l'environnement Internet en implantant IPv6 sur tous les routeurs et systèmes d'extrémité, une solution intermédiaire dénommée **IPSec**⁷, compatible avec IPv6 et IPv4 existe et est largement adoptée.

IPSec permet de rendre confidentiel le contenu des paquets véhiculés par le protocole IPv4, d'authentifier mutuellement la source et la destination des paquets et de s'assurer de l'intégrité des données véhiculées.

Ces services de sécurité sont implantés *via* des en-têtes IPSec, devant l'en-tête IP principale. Il en existe deux, l'en-tête d'authentification (*Authentication Header* [AH]) et l'en-tête de confidentialité-authentification (*Encapsulating Security Payload* [ESP]).

7. RFC 2401 : <http://www.ietf.org/rfc/rfc2401.txt>.

6.2.3 En-tête d'authentification (AH)

L'**en-tête d'authentification (AH)** offre des services d'authentification et d'intégrité des paquets IP. Cela permet de garantir que les données n'ont pas été modifiées lors de leur transfert et que l'adresse source est bien celle qui figure sur le paquet. On apporte ainsi une parade aux attaques basées sur le **leurre d'adresses (IP Spoofing)** et sur celles utilisant le **rejeu** de paquets IP (*replay attack*).



Le rejeu est évité en utilisant un numéro de séquence. Il existe un champ de valeur de vérification d'intégrité (ICV, *Integrity Check Value*). Des variantes des algorithmes MD5 ou SHA-1 (HMAC-MD5 et HMAC-SHA-1) permettent d'assurer l'authentification et l'intégrité dans ce mécanisme.

L'authentification est basée sur l'utilisation d'un code d'authentification de message ou MAC (*Message Authentication Code*).

Le format de l'en-tête d'authentification tel que spécifié par la RFC 2402 est présenté par la figure 6.4.

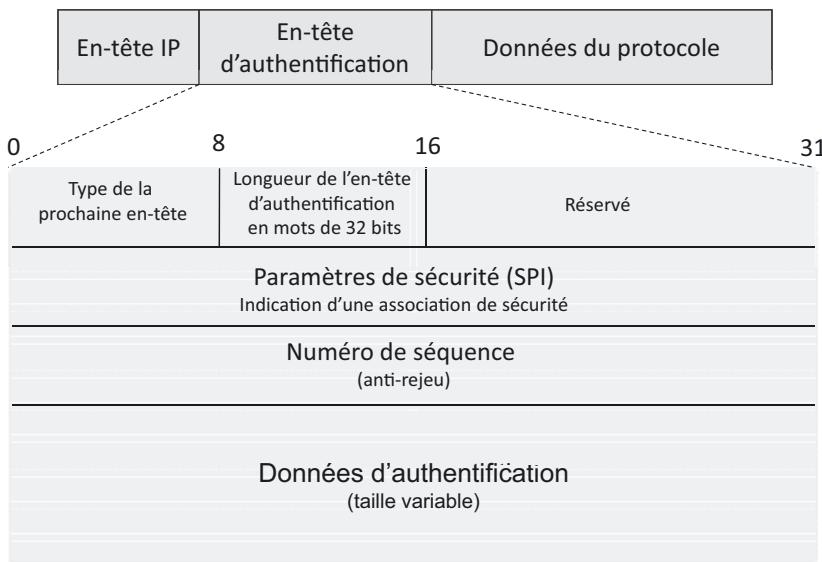


Figure 6.4 – Format de l'en-tête d'authentification (AH).

6.2.4 En-tête de confidentialité-authentification (ESP)

L'**en-tête de confidentialité-authentification (ESP, Encapsulating Security Payload)** permet la réalisation de mécanismes de chiffrement pour rendre confidentiel le contenu du paquet ainsi que le flux.

En option, l'ESP propose des services d'authentification similaires à ceux proposés par l'AH (*Authentication Header*). Le format de l'en-tête ESP est présenté par la figure 6.5 (RFC 2406).

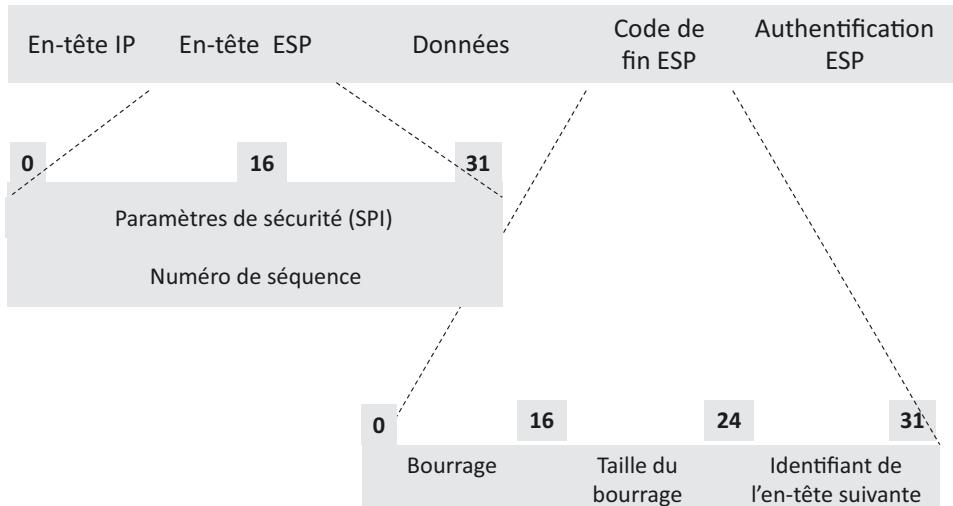


Figure 6.5 – Format de l'en-tête de confidentialité et d'authentification (ESP).

L'émetteur du paquet encapsule les données, ajoute des bits de bourrage si nécessaire, chiffre l'ensemble en utilisant un algorithme de chiffrement symétrique comme DES, Triple DES, RC5, AES ou IDEA. En fait, comme ESP assure aussi l'authentification des paquets, en plus du chiffrement, le champ AH est rarement utilisé.

6.2.5 Association de sécurité

Les services de sécurité offerts par les en-têtes d'extension permettent de réaliser le contrôle d'accès, l'intégrité des données, l'authentification de l'origine des données, le rejet de paquets réémis (anti-rejeu), la confidentialité des données et une relative confidentialité des flux.

Tous ces services reposent sur l'usage d'une **association de sécurité** (SA, *Security Association*) préalablement établie entre les correspondants. En effet, on ne peut assurer la sécurité que dans un mode connecté et on ne peut chiffrer/déchiffrer que si on utilise les mêmes algorithmes aux deux bouts. L'établissement de l'association de sécurité permet d'identifier et d'authentifier les extrémités de la connexion logique (c'est-à-dire les ports d'accès au réseau) et de négocier les mécanismes de sécurité à utiliser (choix de l'algorithme de chiffrement par exemple). En fait, l'association de sécurité est **unidirectionnelle**, deux associations de sécurité sont donc nécessaires pour supporter un échange bidirectionnel. Trois paramètres l'identifient de manière unique, à savoir :

- **l'index des paramètres de sécurité** ou SPI (*Security Parameters Index*) : il s'agit d'une chaîne binaire de signification locale (propre au système qui génère l'association), véhiculée par les en-têtes AH et ESP, qui permet au système destinataire de sélectionner l'association à travers laquelle le paquet reçu va être traité ;

- l'**adresse Internet de destination** de l'association (*IP Destination Address*) : il peut s'agir d'un système d'extrême ou d'un système intermédiaire, routeur ou pare-feu ;
- l'**identificateur de protocole de sécurité** (*Security Protocol Identifier*) : il indique la nature de l'association de sécurité (association AH ou association ESP).

6.2.6 Implantation d'IPSec

La réalisation d'IPSec, dans un système, suppose l'**implantation d'une base de données** permettant de définir le contexte des associations de sécurité (*Security Association Database*). En effet, chaque association est caractérisée par un certain nombre de paramètres dont on peut mentionner les suivants :

- *Sequence Number Counter* : valeur de 32 bits utilisée pour générer le champ *Sequence Number* des en-têtes AH et ESP ;
- *Sequence Counter Overflow* : drapeau indiquant si le dépassement du *Sequence Counter Number* va entraîner un événement à enregistrer (auditabile) et prévenant la transmission future de paquets sur cette association ;
- *Anti-Replay Window* : permet de déterminer si un paquet AH ou ESP est rejoué ;
- *AH Information* : toutes les informations relatives à la mise en œuvre de la procédure d'authentification sont consignées (algorithme utilisé, clés, durée de vie des clés, etc.) ;
- *ESP Information* : les informations relatives aux procédures de confidentialité et d'authentification comme les algorithmes, les clés par exemple, sont regroupées sous ce paramètre ;
- *Lifetime of this Security Association* : ce paramètre permet de limiter la durée de vie d'une association. Au-delà de la valeur spécifiée, et si nécessaire, une nouvelle association doit être établie avec un nouveau SPI (*Security Parameters Index*) ;
- *IPSec Protocol Mode* : il existe plusieurs modes opératoires d'IPSec, ce paramètre permet d'identifier celui utilisé sur l'association ;
- *Path MTU* : taille maximale des paquets supportée sans fragmentation.

Ces paramètres, sauvegardés dans une base de données, permettent de qualifier le mode opératoire d'une association. Ainsi, on sait créer des contextes particuliers aux associations. Il reste à définir la manière dont on peut les utiliser pour transporter des flux applicatifs. C'est le rôle de la **politique de sécurité SPD** (*Security Policy Database*) de spécifier la correspondance possible entre un trafic IP et son support par une association de sécurité déterminée.

Une entrée de la base SPD est un ensemble de sélecteurs composés des adresses IP source et destination, de l'UserID, du niveau de sécurité requis, de l'identification du protocole de transport ou des protocoles de niveau supérieur, de l'identification du protocole IPSec, des numéros des ports source et destination, de la classe et du label du flux d'un paquet IPv6 (issus de l'en-tête), du type de service d'un paquet IPv4. À une entrée de la base SPD correspond une ou plusieurs associations de sécurité.

6.2.7 Gestion des clés de chiffrement

La confidentialité est assurée par la réalisation d'algorithmes de chiffrement qui utilisent des clés qui sont à générer et à diffuser. La **gestion des clés** de chiffrement est donc une tâche importante à réaliser lors de la mise en œuvre de solutions basées sur IPsec. Deux alternatives ont été identifiées pour cela. L'une, manuelle, est effectuée par l'administrateur système. Elle est valable uniquement pour de petits environnements statiques. La seconde, adaptée aux grands environnements à configuration évolutive, invoque un **protocole d'échange de clés**, comme :

- *Oakley Key Determination Protocol*⁸, qui est basé sur l'algorithme d'échange de clés Diffie-Hellman (RFC 2412).
- ISAKMP (*Internet Security Association and Key Management Protocol*), spécifié par la RFC 2408 qui définit les procédures et les formats des paquets pour établir, négocier, modifier, terminer ou détruire une association de sécurité. Les formats sont indépendants du protocole d'échange de clé, des algorithmes de chiffrement et des mécanismes d'authentification qui peuvent être utilisés.
- IKE (*Internet Key Exchange*) (RFC 2409) est une implémentation de ISAKMP. IKE permet de réaliser l'échange de clés (clés authentifierées) et de négocier les services de sécurité pour une association de sécurité. IKE n'est pas spécifique à IPsec et peut être également utilisé pour négocier des services de sécurité pour d'autres protocoles comme des protocoles de routage par exemple (RIPv2, *Routing Information Protocol*).

Tous les mécanismes de confidentialité appliqués au niveau des paquets nécessitent un temps de traitement non négligeable et augmentent le volume des paquets à véhiculer. Ils affectent de ce fait les performances globales du réseau.

La figure 6.6 résume les composants d'une architecture IPsec.

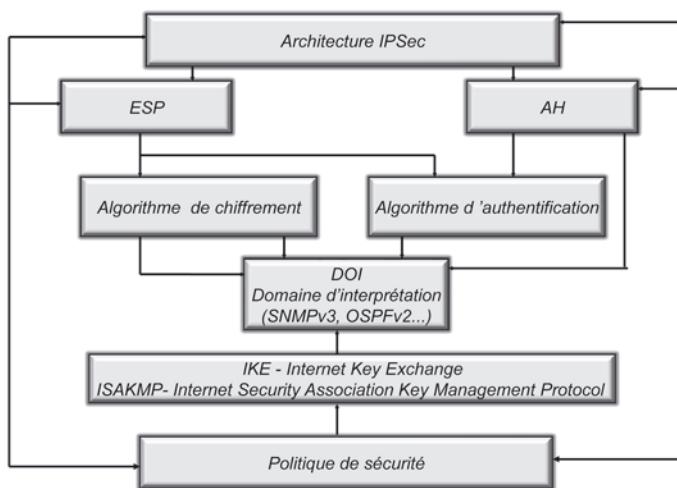


Figure 6.6 – Architecture IPsec.

8. RFC 2412 : <http://www.ietf.org/rfc/rfc2412.txt>

6.2.8 Modes opératoires

Deux modes d'utilisation des services d'authentification et de confidentialité existent. Il s'agit des **modes** dits **de transport** (*transport mode*) et **de tunnel** (*tunnel mode*) (figure 6.7).

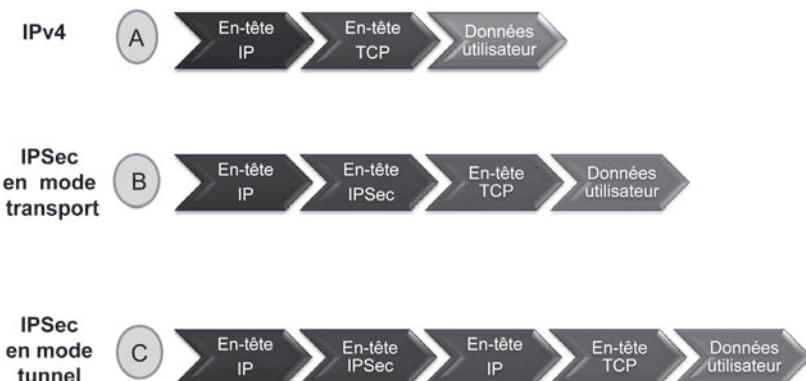


Figure 6.7 – Modes opératoires d'IPSec : format d'un paquet IPv4 (a), d'un paquet IPSec en mode transport (b) et d'un paquet IPSec en mode tunnel (c).

La principale différence entre ces deux modes réside dans le fait que seule la partie « données » du paquet est sécurisée en mode transport, tandis qu'avec le mode tunnel tout le paquet, en-tête y compris, l'est. Ainsi, dans ce mode, il est possible de créer entre deux entités distantes un canal de communication sûr dénommé tunnel, en encapsulant dans un nouveau paquet IP, le paquet IP que l'on veut rendre confidentiel et dont on veut éventuellement pouvoir authentifier l'origine. Aucun système intermédiaire ne peut accéder au paquet IP encapsulé à l'intérieur du nouveau paquet ainsi construit. Cette facilité est largement mise en œuvre pour protéger des communications sur Internet et permet de créer des **réseaux privés virtuels**. Dans le mode tunnel, le VPN se construit entre deux passerelles VPN IPSec (puisque seules les adresses IP de ces passerelles sont en clair, le reste étant chiffré, y compris l'adresse de destination). Dans le mode transport, le tunnel peut de faire directement entre le client et le serveur d'application puisque leurs adresses restent en clair.

6.2.9 Réseaux privés virtuels

L'implantation du protocole IPSec, au niveau des points d'accès au réseau Internet, permet de créer entre ces points un canal de communication dont les extrémités sont mutuellement authentifiées. De plus, selon l'option retenue, les données véhiculées sur cette connexion logique pourront être chiffrées. Ainsi on peut établir, *via* un protocole cryptographique, un chemin sécurisé entre deux points d'une infrastructure de réseau non fiable (notion de réseau privé virtuel). La mise en œuvre d'un tel mécanisme permet aux entreprises de **relier en mode point à point**, *via* un **tunnel**

sécurisé, des sites distants par Internet, pour transmettre des informations confidentielles (figure 6.8).

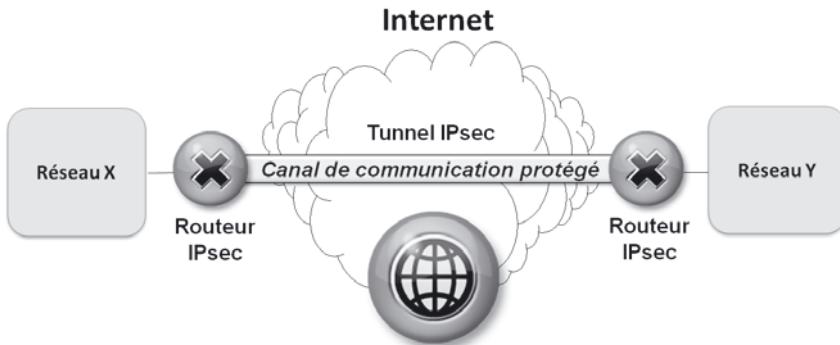


Figure 6.8 - Exemple de réseau privé virtuel réalisé par IPsec.

IPSec permet de sécuriser des paquets de données transférés par le protocole IP. Les extrémités de la connexion IPSec sont authentifiées (preuve de l'origine et de la destination) et se trouvent dans des systèmes de l'organisation, à l'abri derrière des *firewalls*, et sont donc physiquement protégées. L'usage de l'association IPSec est privé et les données qui y transitent peuvent être chiffrées.

 Le terme « réseau » dans l'expression « réseau privé virtuel » est abusif puisque seule une connexion logique (virtuelle) est créée ; il ne s'agit pas d'une liaison physique spécialisée mais d'un tunnel logique.

Chaque application, quelle que soit la nature du trafic qu'elle génère, peut utiliser ces services de sécurité sans être modifiée. Comme IPSec fonctionne en mode point à point (on sécurise les données entre un émetteur et un récepteur *via* une association de sécurité), il n'est pas approprié pour des transferts de données multidestinataires. IPSec n'a pas été conçu pour supporter des trafics de nature *multicast*.

6.3 SÉCURITÉ DU ROUTAGE

6.3.1 Contexte

Il est important de pouvoir **sécuriser les processus d'acheminement** des données à l'intérieur des réseaux de télécommunication. Les fournisseurs de services « réseau » doivent protéger toutes les entités qui interviennent dans ce processus, notamment les routeurs et les serveurs de noms, afin que la qualité du service d'acheminement satisfasse les critères de disponibilité (le service est opérationnel), de confidentialité (les données sont délivrées aux bons destinataires et sont ni écoutes, ni détournées) et d'intégrité (les données ne sont pas modifiées lors de leur transfert). Toutefois, la remise de données aux ayants droit n'est pas garantie par un

service réseau et puisque les données ne sont pas chiffrées, si elles sont interceptées, elles sont alors compréhensibles par des tiers non autorisés.

La sécurité des transmissions peut être éventuellement réalisée en effectuant du brouillage de ligne, en envoyant de l'information non significative pour masquer un flux de données pertinentes dans un flux ininterrompu de données sans importance. Toutefois, s'il fallait protéger les transmissions contre des écoutes passives réalisées par capture des rayonnements électromagnétiques induits par le signal véhiculé sur les supports de transmission, il faudrait isoler complètement ces derniers dans des cages de Faraday. Une telle mesure de protection ne sera mise en œuvre qu'en cas d'absolue nécessité, car sa réalisation est coûteuse. De plus, la sécurité physique des supports de transmission, des boîtiers de raccordement et des équipements de connectique doit être assurée correctement.

La grande difficulté de la sécurisation des échanges au niveau de leur **acheminement** tient au fait que les données utilisateurs sont encapsulées dans celles de contrôle du protocole. Il est alors nécessaire de les distinguer pour faire un chiffrement sélectif, car, dans un VPN en mode tunnel, si l'on chiffre tout, y compris les adresses, l'acheminement devient impossible. Idéalement, il faudrait pouvoir disposer d'équipements de chiffrement qui chiffraient sélectivement uniquement les champs de données utilisateur et qui, en plus, offriraient des services de notarisation, d'horodatage, d'intégrité et de confidentialité.

6.3.2 Principes généraux d'adressage

Notion d'adresses

Une entité, pour communiquer dans un réseau, doit être identifiée par une adresse. On distingue les adresses logiques que l'on désigne par le terme générique de nom, des adresses physiques dépendantes des matériels.

Une **adresse physique**, adresse **matérielle** ou **MAC**, est inscrite sur un équipement de connectique (carte réseau, coupleur ou contrôleur) de raccordement d'un système à un réseau. L'adresse MAC correspond le plus souvent à un numéro de série d'un constructeur et possède une signification pour le protocole de liaison.

Une adresse de messagerie est une **adresse logique** : « popeye@unil.ch » identifie l'utilisateur « popeye » dans le système de messagerie électronique de l'université de Lausanne (Unil) qui dépend du système de nommage suisse (ch). Il s'agit d'un nom ayant une signification particulière dans un contexte spécifique.

 Un nom est un objet linguistique qui désigne une entité particulière parmi un ensemble d'entités. Cet ensemble définit le domaine de dénomination (domaine de désignation ou domaine de nommage).

L'adresse IP est une adresse « réseau » attribuée à un système pour lui permettre d'être raccordé à Internet, d'émettre et de recevoir des paquets IP.

Dans la version 4 du protocole IP, l'adresse est codée sur 32 bits. Par souci de simplification de leur expression et de leur manipulation par des personnes, les

32 valeurs binaires sont représentées sous une forme décimale pointée. Avec 32 bits on peut coder 2^{32} adresses différentes lorsqu'on utilise un adressage à plat. Pour simplifier et aussi pour augmenter les possibilités d'adressage, on utilise un **adres-sage hiérarchique**. L'adresse IP est structurée en deux parties, l'une identifie un réseau, l'autre un système dans un réseau. En fonction du nombre de bits alloués à la désignation de l'un ou l'autre de ces champs, différentes classes d'adresses IP ont été spécifiées. Par ailleurs, quelques bits sont réservés à l'identification de la classe à laquelle une adresse appartient.

Les routeurs qui effectuent le routage en se basant sur l'identifiant du réseau sont dépendants de cette structure. Un système relié à plusieurs réseaux aura donc plusieurs adresses IP (*multi-homed system*). En fait, une adresse IP n'identifie pas une machine mais plutôt un point d'accès à un réseau (notions de connexion à un réseau ou encore d'interface réseau).

L'unicité des **identifiants réseau** est garantie par le fait que ce sont des autorités internationales d'adressage qui les allouent ; alors que c'est du ressort de l'administrateur système d'une organisation d'attribuer des identifiants uniques aux systèmes du réseau dont il a la responsabilité.

Mise en correspondance et acquisition des adresses

Les adresses IP sont attribuées indépendamment des adresses matérielles des machines connectées à un réseau local. Pour envoyer un paquet sur le **réseau local**, le logiciel réseau doit convertir l'**adresse IP** (de niveau 3) d'un système en son **adresse MAC** (de niveau 2). Un paquet IP est encapsulé dans une trame MAC puis transmis sur le réseau local (seule l'adresse MAC est nécessaire au transfert de données dans un réseau local).

La traduction (@IP – @MAC) est effectuée dynamiquement par le protocole **ARP** (*Address Resolution Protocol*). ARP permet aux machines de résoudre ce problème de **mise en correspondance** d'adresses (*addresses resolution*) sans utiliser une table statique. En effet, une machine utilise ARP pour déterminer l'adresse physique (MAC) du destinataire en diffusant, sur le sous-réseau, une requête ARP qui contient l'adresse IP à traduire. La machine possédant l'adresse IP concernée répond en renvoyant son adresse MAC. Pour rendre ARP plus performant, chaque machine tient à jour, en mémoire, une table des adresses résolues, réduisant ainsi le nombre d'émissions de requêtes en mode diffusion.

Au moment de son **initialisation** (*bootstrap*), une machine sans mémoire de masse (*diskless*) doit contacter un serveur pour déterminer son adresse IP et pouvoir utiliser les services TCP/IP. Le protocole **RARP** (*Reverse ARP*) permet à un système d'utiliser son adresse MAC pour déterminer son adresse IP. Le mécanisme RARP permet par exemple à une machine de se faire identifier comme cible en diffusant sur le réseau une requête RARP. Les serveurs recevant cette demande examinent leur table de correspondance et répondent au client. Une fois l'adresse IP obtenue, la machine la stocke en mémoire vive et n'utilise plus RARP jusqu'à sa réinitialisation.

Dans la version **IPv6**, les protocoles ARP et RARP ne sont plus utilisés ; ils sont remplacés par un protocole de découverte des voisins, **ND** (*Neighbor Discovery*),

qui est un sous-ensemble du protocole de contrôle **ICMP** (*Internet Control Message Protocol*).

Toute machine, pour communiquer sur Internet, doit au préalable disposer d'une adresse IP. Celle-ci peut lui être attribuée manuellement ou dynamiquement par des protocoles dits « d'amorce ».

Les protocoles **BOOTP** (*Bootstrap Protocol*) et **DHCP** (*Dynamic Host Configuration Protocol*) permettent aux systèmes d'obtenir une adresse IP sans utiliser le protocole RARP.

DHCP est considéré comme une version plus performante du protocole BOOTP. Le protocole DHCP s'exécute en mode client/serveur. Un client DHCP est implanté dans les machines qui se connectent au réseau d'accès à Internet (réseau local d'entreprise ou infrastructure du fournisseur d'accès Internet [ISP]). Ce client émet des requêtes d'information de configuration à son serveur. Ce dernier lui retourne l'ensemble des données nécessaires à la configuration réseau de la machine (adresse IP, adresse de la passerelle par défaut pour accéder à Internet, adresse du ou des DNS dont elle dépend).

Lors de la configuration d'un **serveur DHCP**, on lui attribue un certain nombre d'adresses IP qu'il pourra attribuer dynamiquement à ses clients. Ces adresses ont en général une durée de validité limitée. Les clients DHCP n'ont pas dans l'absolu toujours la même adresse IP, ni une adresse IP fixe. Cela permet de déplacer des systèmes dans un réseau, d'autoriser la mobilité des utilisateurs sans avoir à mettre systématiquement en œuvre des procédures de gestion manuelle de la configuration réseau.

6.3.3 Gestion des noms

Notion de serveur de noms

La dénomination et l'adressage doivent répondre au double besoin de pouvoir désigner sans ambiguïté les éléments des réseaux, et de les rendre accessibles *via* un processus de routage. Ainsi, il est essentiel de connaître les relations entre nom, adresse et localisation géographique des systèmes. En effet, connaissant le nom d'une application, d'un service, d'un document à atteindre, on doit pouvoir y associer une route. Cette fonction de **mise en correspondance** ou **mappage** (*mapping*) sera accomplie en une ou en plusieurs étapes. Parfois les routes peuvent changer en fonction du trafic ou de l'évolution de la configuration du réseau et de sa topologie.

Les dénominations assurent aux applications la transparence de l'infrastructure de transport qui peut alors évoluer sans modifier l'infrastructure applicative. Par ailleurs, une application gérée par un système hôte possédant plusieurs points d'accès réseau (*Host Multi-Homed*) pourra être atteinte *via* la meilleure route (*via* l'une ou l'autre des adresses IP du système) de manière transparente.

Mémoriser ou encore saisir des adresses IP dans le corps d'un message par exemple deviendrait vite insupportable. C'est la raison pour laquelle l'adressage utilise des noms de structure hiérarchique, beaucoup plus simples à manipuler et à mémoriser.

Un **serveur de noms** (*Directory Services*) procure la possibilité de manipuler des noms mnémotechniques et conviviaux en effectuant une correspondance dynamique entre le nom d'un objet et son adresse. Ce service est rendu en mode client/serveur. Un processus invoque l'exécution d'une requête de traduction d'un nom en adresse réseau, le serveur de noms exécute cette demande et lui restitue le résultat. Les processus de communication interrogeront un serveur de noms, pour obtenir les informations d'adressage et de localisation nécessaires pour réaliser la mise en relation des correspondants, processus ou utilisateurs.

La réalisation de ce service peut être distribuée et un serveur de noms peut devenir le client d'un autre serveur de noms.

Les recommandations de la série X.500 de l'UIT (équivalentes à la norme multi-partie ISO 9594) définissent le modèle fonctionnel, les services et les protocoles permettant de réaliser un système d'annuaire électronique de **gestion de noms** (serveur de noms, *Directory Service*).

Les données d'un serveur de noms sont organisées de manière hiérarchique selon un arbre renversé, appelé **DIT** (*Directory Information Tree*). Elles constituent la base d'information du serveur ou **DIB** (*Directory Information Base*).

Les noms des nœuds ou feuilles de l'arbre, ainsi que les attributs les caractérisant, sont exprimés en langage ASN-1 (*Abstract Syntax Notation One*) à l'aide du type *Object Identifier*, dont la valeur est constituée par la concaténation des numéros d'ordre des branches de l'arbre, à partir de la racine de l'arbre. Chaque numéro est séparé par un point (figure 6.9).

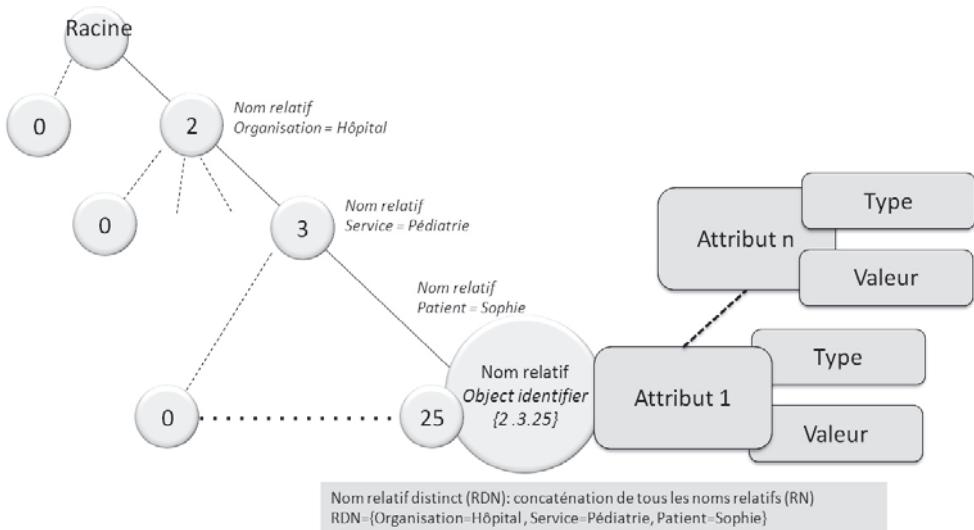


Figure 6.9 – Exemple de structure arborescente d'une base d'information d'un serveur de noms.



ASN-1 (Abstract Syntax Notation-1) : c'est en 1984 que fut normalisé par le CCITT (renommé depuis UIT) le premier langage de description de données manipulées lors d'un transfert. Il s'agissait d'une notation de description de données et des règles d'encodage associées (recommandation X.409). Elle répondait au besoin de pouvoir décrire le contenu d'un message de façon universelle, indépendamment de sa sémantique et de son utilisation. En 1987, pour satisfaire les impératifs communs aux applications réparties de représentation des données transférées, l'ISO, sur les bases du travail du CCITT, a défini une notation abstraite de représentation des données : ASN-1. Cette première et unique notation de syntaxe abstraite fut normalisée à l'ISO et enregistrée sous le label ISO 8824. Le type prédéfini « *Object Identifier* » de ce langage est très largement utilisé pour identifier sans ambiguïté une entité. À la notation ASN-1 sont associées des règles de base d'encodage des données dénommées BER (*Basic Encoding Rules*) (norme ISO 8825), qui masquent aux données, les diverses représentations internes liées aux caractéristiques matérielles des systèmes.

Noms de domaine

La mise en œuvre de communication, dans un environnement ouvert, nécessite de pouvoir attribuer un identificateur unique dans un domaine de dénomination déterminé. Pour assurer l'unicité des noms au niveau international, il existe des procédures d'enregistrement, auprès d'autorités compétentes, dont le rôle est d'attribuer un identificateur non ambigu et unique à l'objet que l'on désire identifier.

La **norme ISO 9834** a spécifié des autorités d'enregistrement et les a organisées selon une structure hiérarchique arborescente. De la racine de l'arbre partent trois branches aboutissant à des nœuds distincts de premier niveau qui représentent le domaine de dénomination de l'**UIT**, de l'**ISO**, et d'un comité joint **ISO-UIT**, qui constituent les autorités internationales d'enregistrement. Le niveau immédiatement inférieur à l'**ISO** autorise, entre autres, l'enregistrement :

- des diverses normes ISO (*standard (0)*) ;
- des membres de l'**ISO** (*member-body (2)*), parmi lesquels on trouvera l'Afnor (208), la France (250), l'ANSI (310), etc. ;
- des organisations (*organization (3)*), parmi lesquelles se trouve par exemple le département de la Défense américaine (DOD) (6).

La figure 6.10 propose un extrait de l'arbre international d'enregistrement.

Un nœud de l'arbre est identifié par un **numéro unique** attribué par l'autorité d'enregistrement de niveau immédiatement supérieur et par une chaîne de caractères alphanumériques déterminée par l'organisation qui propose l'enregistrement de l'objet. Le nom de l'objet doit être unique dans ce domaine d'enregistrement. Cette unicité est garantie par le procédé d'enregistrement.

Grâce à la structure arborescente retenue pour enregistrer les objets, on peut aisément les dénommer de façon non ambiguë en concaténant les numéros des branches (arcs) parcourus à partir de la racine de l'arbre jusqu'à l'objet en question. Ainsi, on peut attribuer un identificateur d'objet unique de type *Object Identifier*, qui représente le **nom relatif de l'objet** (RDN, *Relatif Distinguish Name*).

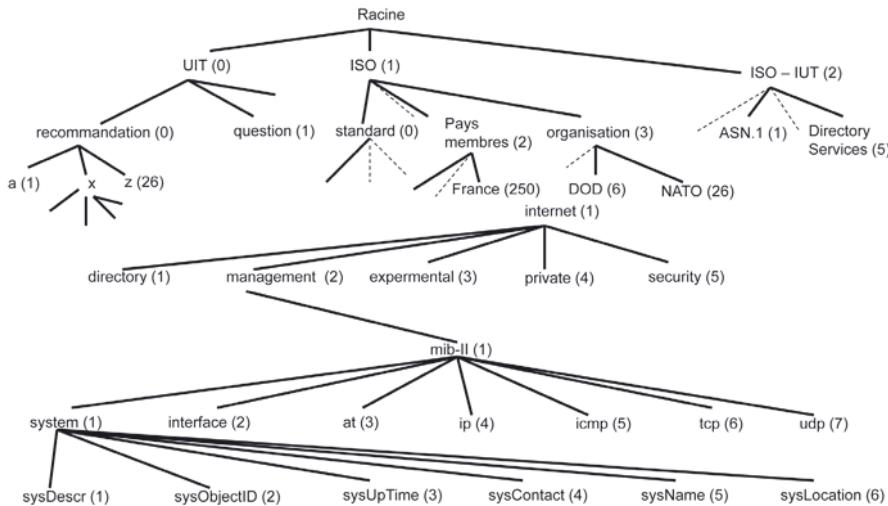


Figure 6.10 - Autorités et arbre d'enregistrement.

La concaténation de tous les noms relatifs forme le **nom distinct** (DN, *Distinguished Name*), qui est également de type *Object Identifier*.

Noms de domaine génériques

Les **noms de domaine** génériques d'Internet sont enregistrés dans cette structure logique d'enregistrement. On ne s'intéresse alors qu'à la partie de l'arbre d'enregistrement dont le nœud constitue la racine des noms de domaines les plus élevés, qualifiés de **TLD** [*Top-Level Domains*]).

Ces derniers identifient des pays indiqués par deux lettres (fr, it, uk, ch, nl, de, etc.) et des domaines fonctionnels comme par exemple :

- **.com** : organisations commerciales ;
- **.edu** : institutions académiques d'Amérique du Nord ;
- **.org** : organisations institutionnelles ou non ;
- **.gov** : gouvernement américain ;
- **.gouv** : administrations françaises ;
- **.mil** : organisations militaires américaines ;
- **.net** : opérateurs de réseaux ;
- **.int** : entités internationales ;
- **.biz** : pour ce qui concerne le monde des affaires ;
- **.info** : pour tous les usages ;
- **.name** : pour les individus ;
- etc.

De ces grands domaines de désignation, en dépendent d'autres (notion de sous-domaines). Enregistrer un nom de domaine consiste à insérer une entrée dans un

annuaire de désignation. Cela revient à créer un nouvel arc dans l'arbre d'enregistrement géré par une organisation habilitée.

L'ICANN (*Internet Corporation for Assigned Names and Numbers*)⁹ est responsable autoproclamé de l'attribution des noms et des adresses de l'Internet et doit s'assurer de leur unicité. Cette responsabilité peut être déléguée à un sous-domaine qui est, d'un point de vue hiérarchique, sous son autorité. Parmi les autorités d'enregistrement accréditées (ARD, *Accredited Registrar Directory*) par l'ICANN, nous retiendrons pour exemples : pour la France l'**AFNIC**¹⁰ (Association française pour le nommage Internet en coopération). Depuis 2012, l'ICANN autorise l'enregistrement de nouvelles extensions personnalisées de noms de domaine génériques (TLD). Ainsi par exemple une entité, qu'elle soit commerciale ou non, pourrait selon certaines conditions acheter, pour un montant en dollars s'exprimant sur six chiffres, un TLD à son nom (un TLD personnalisé possède une valeur marketing non négligeable). Cette nouvelle facilité constitue une source d'enrichissement non négligeable pour l'ICANN.

On constate que c'est une association américaine (sur territoire américain, opérant selon la législation américaine) qui possède le pouvoir de l'attribution et la gestion des adresses IP et des noms TLD. De ce fait, elle contrôle ainsi indirectement l'accès à Internet. Ceci pose un réel **problème de dépendance** des organisations et des États vis-à-vis d'une suprastructure étrangère qui se veut ouverte sur le reste du monde mais dont le poids des représentants non américains est faible.

Mais l'ICANN n'est pas la seule entité pour attribuer des TLD. D'autres organismes, comme par exemple Open-Root, en France, proposent des solutions alternatives, et qui de plus peuvent proposer et gérer des noms de domaines racines constitués de caractères qui peuvent ne pas être des caractères anglo-saxons (lettres accentuées, caractères cyriliques, chinois, etc.).



Le critère de sécurité relatif à la disponibilité (des infrastructures, services, données) qui passe par l'accessibilité au réseau Internet ne peut être ni contrôlé, ni maîtrisé par les organisations qui utilisent Internet. Elles sont tributaires pour leur accès à Internet, de l'attribution des adresses IP et des noms de domaine, d'entités externes.

Serveurs DNS

Dans l'environnement Internet, un **serveur DNS** (*Domain Name Server*) est un serveur de noms qui gère la relation entre un nom logique et l'adresse IP du système dans lequel la ressource nommée est implantée. Toutes les applications font appel, directement ou non, aux services des DNS¹¹. Organisés de manière hiérarchique, (les DNS collaborent entre eux en mode client/serveur), ils jouent un rôle capital

9. <http://www.icann.org>

10. <http://www.nic.fr>

11. Les premières implantations DNS se sont effectuées sur une plate-forme Unix BSD, connues sous le nom **BIND** (*Berkeley Internet Name Domain*) ou sous l'appellation *name daemon*.

dans la réalisation des communications. En effet, c'est à partir des informations qu'ils détiennent concernant l'identification, l'adressage et la localisation des entités, que les transferts de données s'effectuent. Une quinzaine de **serveurs racines DNS** (*root Domain Name Servers*) sont coordonnés par l'ICANN, et la grande majorité des serveurs racines se situe sur le territoire Nord-Américain. Ils gèrent les noms de domaines et les adresses IP de plus haut niveau (*top-levels domains*). Cela comprend l'ensemble des domaines précédemment cités (.org, .com, etc.) et aussi les 244 noms de domaines des différents pays (.ga, Gabon ; .lk, Sri Lanka ; .pf, Polynésie française ; etc.). D'autres serveurs, non gérés par l'ICANN, répartis dans le monde, et en particulier en Europe, rendent le même service.

Des **serveurs DNS locaux** dits de résolution (*resolvers*) possèdent une copie des informations contenues dans les serveurs racines. Souvent associés à des points stratégiques d'accès au réseau ou liés à des fournisseurs d'accès Internet (ISP, *Internet Service Providers*), ils permettent de répondre aux requêtes des utilisateurs relatives à la traduction d'un nom de domaine en une adresse IP.

Le **protocole LDAP** (*Lightweight Directory Acces Protocol*) permet d'accéder à un service DNS. Il constitue une interface d'accès aux serveurs de noms du monde Internet¹².

6.3.4 Principes généraux de l'acheminement des données

Notion de route

Pour acheminer des données entre deux systèmes distribués connectés à un réseau grande distance comme Internet, il est nécessaire de connaître leur adresse réseau. Ainsi l'envoi d'un message électronique de l'utilisateur « popeye@unil.ch » à « mimosa@dunod.com » passe par l'association de ces noms d'utilisateurs de messagerie électronique, à des noms de systèmes informatiques raccordés au réseau Internet et connus de ce dernier par leurs adresses IP. Ce sont les adresses IP des serveurs de messagerie qui sont connues du réseau Internet et non directement les noms des utilisateurs. C'est à partir de ces **adresses IP** que pourront être mis en œuvre les processus d'acheminement.

Une entité possède d'une part un nom qui permet de la désigner parmi d'autres indépendamment de sa localisation, et d'autre part une adresse qui identifie son point d'entrée dans un réseau. Une **route** désigne le chemin entre deux entités. C'est une liste de noms d'entités intermédiaires représentant le chemin d'une source vers une destination.

12. La RFC 4511 est relative à la dernière version du protocole LDAP <http://tools.ietf.org/html/rfc4511>

Fonctions de commutation et de routage

Les **fonctions de commutation** et de **routage** sont complémentaires et répondent à deux problématiques qui sont respectivement :

- l'optimisation du partage des ressources réseaux, qui sont en nombre inférieur par rapport au nombre d'utilisateurs (fonction de commutation) ;
- l'acheminement des données d'un émetteur vers un ou plusieurs récepteurs (fonction de routage).

Les **commutateurs** prennent en charge une fonction d'aiguillage et de mise en relation des lignes de transmission. C'est de leur architecture interne que dépend la façon dont la connexion physique est réalisée à l'intérieur des commutateurs. Plusieurs techniques de commutation existent selon le mode de partage des ressources retenu, le niveau de commutation souhaité et des critères de qualité de service que l'on désire privilégier.

Indépendamment de la structure interne d'un commutateur, mais en s'appuyant sur la fonction de commutation, la fonction de routage a pour objet de déterminer la « meilleure » route pour acheminer les données entre leur source et leur destination. Elle est supportée par des **routeurs**.

Le routage est effectué par chaque système intermédiaire (routeur, passerelle d'interconnexion), à partir de l'identifiant du réseau de l'adresse IP du système de destination, en fonction des informations contenues dans sa table de routage, de la politique et de l'algorithme de routage. Les informations relatives à la route à suivre par un paquet IP pour atteindre sa destination sont contenues dans une **table de routage**. Celle-ci contient, pour chaque réseau à atteindre, l'adresse IP du prochain routeur auquel il faut envoyer le paquet. Une des difficultés majeures de la mise en œuvre d'un processus de routage provient de l'initialisation, de la mise à jour, de la gestion des tables de routage de l'ensemble des systèmes intervenants dans l'acheminement.

Le rôle du protocole IP est d'encapsuler des données pour construire un paquet IP (dont l'en-tête contient les adresses IP de la source et de la destination) afin que les données puissent être véhiculées. Un paquet IP arrive dans un nœud intermédiaire via une ligne d'entrée. Après lecture des adresses IP du paquet et de celles contenues dans sa table de routage, l'algorithme de routage détermine, en fonction de la destination finale du paquet et de l'état du réseau, la ligne de sortie la plus adaptée pour atteindre le nœud suivant. Celle-ci devient alors une ligne d'entrée du système auquel elle aboutit.

La fonction de routage est déterminée par :

- la politique de routage ;
- les tables de routage ;
- les algorithmes de routage ;
- la gestion du réseau.

La **politique de routage** est un choix de stratégie d'acheminement reflétant la façon dont un administrateur de réseau gère le mode de fonctionnement de son réseau. Elle dépend, entre autres, de la capacité des routeurs à supporter ces choix de

gestion. On distingue les politiques **statiques**, où les routes sont prédéfinies une fois pour toutes quel que soit l'état du réseau, des politiques **dynamiques** ou **adaptatives**. Ces dernières permettent d'ajuster les informations contenues dans les tables de routage pour que les routeurs puissent prendre une décision de routage en fonction des caractéristiques effectives du réseau, du trafic en cours, de l'état des lignes et des systèmes (disponibilité, performances, encombrement, etc.).

La mise à jour des **tables de routage** des grands réseaux est un vrai casse-tête opérationnel pour les administrateurs de réseaux, dans la mesure où les différentes modifications des valeurs des tables doivent être synchronisées pour éviter les dysfonctionnements et les pertes de données en transit. Les **protocoles de gestion de réseau** permettent, entre autres, de mettre à jour les tables de routage.

Idéalement un routeur devrait être capable d'accepter tous les paquets qui lui sont remis. Ce qui veut dire qu'un routeur adjacent ne lui achemine pas de données, s'il ne peut les traiter. La meilleure route n'est pas forcément la route la plus courte, mais celle qui passe par des lignes et des routeurs capables de prendre en compte le trafic. Un routeur ne doit pas perdre ni détériorer des données ou les mobiliser trop longtemps. Pour cela, il doit disposer de mémoire suffisante et d'une **gestion des files d'attente** efficace.

C'est de l'intelligence des routeurs, des facilités qu'ils ont à adapter leurs décisions de routage en fonction de l'état du réseau et des demandes d'acheminement du trafic, que dépendent en grande partie les performances, la qualité de service, la disponibilité et la fiabilité d'un réseau.

L'administration de réseau peut contribuer à la sécurisation des routeurs en y effectuant des accès sécurisés lors de leur configuration, en générant des alarmes lors de tentatives d'intrusion, et en sécurisant les centres de gestion et de supervision des routeurs.

6.3.5 Sécurité des routeurs et des serveurs de noms

Tous les éléments matériels et logiciels intervenant dans l'acheminement des données peuvent faire l'objet de dysfonctionnement (pannes...), de détournement ou d'attaques ciblées (dénis de service, re-routage, *spoofing*...).

Sécurité des routeurs

La **fonction de routage** est primordiale dans les activités du réseau dans la mesure où l'objet d'un réseau est de mettre en relation des correspondants et d'acheminer leurs données. Il est donc crucial de savoir la protéger en empêchant tout un chacun de l'altérer en prévenant ou détectant, entre autres, les actions suivantes :

- modification des adresses contenues dans les tables de routage, dans les paquets IP, etc.
- modification des routes, copies illicites des données transportées ;
- surveillance des flux ;
- détournement, modification et destruction de paquets de données ;
- déni de service, effondrement des routeurs, inondation du réseau, etc.

Sécurité des serveurs de noms – DNSSEC

Bien que les serveurs de noms ne supportent pas les processus de routage à proprement parler, ils contribuent activement à la réalisation de l’acheminement des informations. Ainsi, ils constituent des points sensibles de l’architecture de communication, ils sont donc à protéger. La mise en place de **mesures de sécurité** (contrôle d’accès, authentification, surveillance, redondance, chiffrement, etc.) sont nécessaires pour éviter entre autres, la modification mal intentionnée des données, les dénis de service ou encore la création de faux serveurs, pour prévenir par exemple :

- un routage des informations vers des destinataires différents de ceux prévus initialement (détournement) ;
- l’obtention de réponses erronées conduisant à des erreurs de transmission ;
- l’intrusion ;
- l’indisponibilité, l’effondrement du réseau, le déni de service ;
- l’impossibilité de réaliser un mécanisme de contrôle d’accès lorsque celui-ci est basé sur des certificats sauvegardés dans des DNS.

Le **DNSSEC** (*Domain Name System Security Extensions*), défini par les RFC 4033 à 4035, apporte aux protocoles gérant les noms de domaines, des aspects sécurité qui manquaient au DNS, en particulier pour garantir l’intégrité des enregistrements concernant les noms de domaines. En utilisant le chiffrement asymétrique et le calcul d’empreinte, le **DNSSEC** signe électroniquement les enregistrements du DNS, leur conférant ainsi leur intégrité. Le DNSSEC peut, en cascade, transférer les signatures vers des DNS hiérarchiquement inférieurs au DNS racine. Ceci permet de faire face aux attaques dites « d’empoisonnement du DNS » qui permettent, en modifiant les enregistrements des noms de domaines par exemple dans les routeurs, d’inciter de fausses conversions « adresses noms de domaine – adresses IP », de détourner le trafic vers les serveurs des attaquants et de mener des attaques en phishing afin d’usurper les paramètres des victimes. Les DNS étant des éléments fondamentaux pour transformer les noms de domaines en adresses IP et inversement, le protocole DNSSEC apporte un degré supplémentaire de confiance dans l’utilisation d’Internet.

6.4 SÉCURITÉ ET GESTION DES ACCÈS

La **gestion et le contrôle des accès** aux ressources informatiques constituent la pierre angulaire de la mise en œuvre de la sécurité. De la qualité de leur réalisation dépend, pour beaucoup, le niveau de protection des environnements.

6.4.1 Degré de sensibilité et accès aux ressources

C’est en fonction du degré de sensibilité des ressources que sont déterminées leurs exigences de sécurité, sur lesquelles se base la mise en œuvre du contrôle d’accès (tableau 6.1).

Tableau 6.1 – Niveaux de sensibilité et de protection.

Niveaux de sensibilité des ressources	Actions de sécurité
Classification des données	Identifier les exigences de sécurité
Classifications des personnes	Affecter des permissions de manipulation au couple personne/ressources Contrôle d'accès
Classification des flux informationnels	Affecter des niveaux de protection aux flux Chiffrement – Contrôle d'intégrité

6.4.2 Principes généraux du contrôle d'accès

Un mécanisme de **contrôle d'accès logique** aux ressources informatiques est basé sur l'identification des personnes, leur authentification et sur les permissions ou droits d'accès qui leur sont accordés.

C'est sur la base d'une identification et d'une authentification que le mécanisme de contrôle d'accès accorde ou non, en fonction du profil de l'utilisateur, l'accès aux ressources sollicitées (figure 6.11). Cela suppose que **l'identification de l'usager** (gestion des identités, *Identity management*), que les **preuves de son identité** (authentification, gestion des preuves de l'identité, *Identity proof management*) et que **ses droits d'accès**, soient correctement gérés (gestion des autorisations, *Authorization management*).

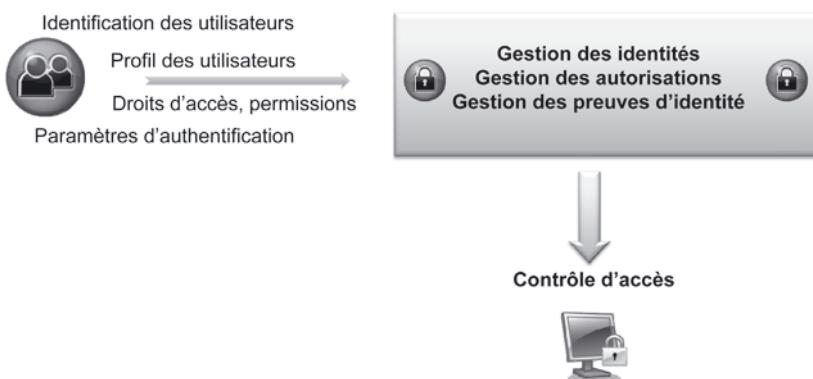


Figure 6.11 – Élément du contrôle d'accès aux ressources.

Le **profil de l'usager** (*user profile*) regroupe toutes les informations nécessaires aux décisions d'autorisation d'accès. Il doit être défini avec soin et résulte de la définition de la politique de gestion des accès.

Pour autoriser un usager à utiliser un service demandé, le système de contrôle d'accès procède à une vérification des droits de l'usager, en fonction de la cohérence du service sollicité, de l'équipement, de la date et de l'heure de la demande. Le

contrôle de cohérence revient à comparer le profil du service avec celui de l'utilisateur et avec celui du système à partir duquel la requête est émise.

L'autorisation est accordée quand l'usager possède des droits sur le service et que les besoins en équipement terminal d'accès et en composants logiciels indispensables au service sont supportés.

Le **service d'authentification** a pour objectif de vérifier la véracité de l'identité (notion de preuve de l'identité). Cela dépend généralement d'un ou de plusieurs des facteurs suivants :

- d'un secret qu'une entité détient (ce qu'elle sait), mot de passe ou numéro d'identification personnel (PIN, *Personal Identification Number*) ;
- de ce qu'elle possède (carte, jeton, etc.) ;
- de ce qu'elle est (empreinte digitale, vocale, rétinienne, etc.).

Une authentification forte peut résulter de la combinaison d'au moins deux de ces trois facteurs.

Une **carte à puce**, par ses capacités à mémoriser des données et à effectuer des traitements, peut jouer un rôle dans le processus d'identification et d'authentification des utilisateurs lors de leur accès aux ressources. Elle implique que les systèmes soient munis d'un lecteur de cartes, ce qui a limité l'usage de la carte à puce dans la mise en œuvre du contrôle d'accès.

Les mécanismes de contrôle d'accès actuels ont largement recours à l'usage de **mots de passe**. Le tableau 6.2 rappelle quelques directives élémentaires relatives à la gestion des mots de passe.

La **vérification de l'identité** dépend d'un scénario où le demandeur d'accès donne son identité et une preuve qu'il est censé être le seul à connaître ou à posséder (mot de passe, clé confidentielle, empreinte, code PIN). Le service d'authentification procède à une comparaison de ces informations avec des données préalablement enregistrées dans un **serveur d'authentification**. Ce serveur doit être hautement protégé et sécurisé par des mécanismes *ad hoc* de contrôle d'accès, de gestion sécurisée de systèmes et par le chiffrement des données qu'il stocke. Un serveur d'authentification ne doit pas être défaillant ou vulnérable car de sa robustesse dépend le niveau de sécurité globale de l'infrastructure informatique et télécoms.

Tableau 6.1 – Directives élémentaires relatives à la gestion des mots de passe.

Mot de passe	Action de sécurité
Mot de passe par défaut	À modifier immédiatement après installation
Choix des mots de passe	Mots longs intégrant des caractères spéciaux
Modification des mots de passe	Modification périodique impérative
Mots de passe « invités »	Règles identiques + vérification de l'annulation dès qu'ils ne sont plus utiles
Mots de passe partagés	À proscrire
Transmission/stockage des mots de passe	Non-divulgation ou affichage effet « POST IT »

Insistons sur le fait que les solutions de sécurité ont aussi besoin d'être protégées et sécurisées afin qu'elles puissent offrir un certain niveau de sécurité (notion de récursivité de la sécurité). Ainsi, la sécurité informatique et télécoms obtenue par une succession de barrières (des mesures de sécurité) qui augmentent le niveau de difficulté que de potentiels attaquants doivent franchir pour accéder aux ressources peut contribuer à réaliser une **sécurité en profondeur**.

6.4.3 Démarche de mise en place du contrôle d'accès

La **démarche de mise en place** d'une solution globale de gestion sécurisée des accès aux ressources informatiques de l'entreprise peut être structurée en cinq phases :

- **identification des besoins** de gestion des permissions d'accès aux ressources ;
- **recherche et analyse de scénarios possibles** en fonction des besoins et des exigences de sécurité ;
- **proposition et validation d'un scénario** ainsi que spécification de ses caractéristiques fonctionnelles, organisationnelles et techniques ;
- **réalisation d'un plan d'actions** ;
- **mise en œuvre** de la solution.

6.4.4 Rôle et responsabilité d'un fournisseur d'accès dans le contrôle d'accès

Un **fournisseur d'accès Internet** (FAI) tient à jour la liste des clients avec leurs droits respectifs, établit les règles de contrôle d'accès et d'authentification et supporte la sécurité de son environnement. Le **contrat** entre un fournisseur de services et ses clients est important et permet d'établir entre autres, les responsabilités, droits et devoirs de chacun notamment en termes de procédures d'identification, d'authentification et de consommation des ressources, de coûts et de facturation. Le fournisseur d'accès doit pouvoir garantir le respect des droits des clients au regard des services souscrits, tout en protégeant ses ressources contre leur utilisation abusive et délictueuse, par des mesures de sécurité performantes. Par ailleurs, le client est seul responsable de l'usage malveillant ou détourné de l'infrastructure du fournisseur, ainsi que le stipule généralement le contrat de services.

6.4.5 Certificats numériques et contrôles d'accès

Pour des applications web, le contrôle d'accès à certains serveurs web est possible via une infrastructure à clé publique (**PKI**) et des **certificats numériques**. Ainsi, le système de vérification est externalisé et n'a pas besoin d'être centralisé sur le serveur web, cela autorise également un nombre élevé d'utilisateurs. Ce mécanisme de certification comporte des limites, dépendant de la véracité des certificats, de la façon dont ils sont attribués et gérés. S'il est aisément d'allouer un certificat à un utilisateur, en revanche, il est plus difficile de le révoquer. Ceci peut être nécessaire lorsque les informations contenues dans le certificat sont devenues obsolètes, lorsque la clé

privée de l'utilisateur a été compromise, ou tout simplement si l'utilisateur ne fait plus partie de l'entreprise, par exemple. Lorsqu'un certificat est devenu invalide, il est alors inscrit dans une **liste de certificats révoqués** (liste de révocation ou CRL, *Certificate Revocation List*).

C'est du ressort de l'**autorité de certification** de gérer les listes de révocation qui contiennent les numéros de tous les certificats invalides et de la consulter à chaque demande. La lourdeur d'une consultation systématique de cette base de données altère considérablement les performances d'un tel système de contrôle d'accès.

Rôle des certificats clients

Un **certificat** contient la clé publique de son propriétaire, son nom, le nom de l'autorité de certification qui l'a signé, un numéro de série et divers attributs additionnels. Ces derniers peuvent qualifier des informations numériques ou textuelles comme les adresses électronique ou postale, l'employeur, la fonction, le département, les numéros de bureau, de téléphone, la date de naissance, le sexe, la nationalité, etc. Ces attributs permettent une grande flexibilité d'utilisation pour assurer le contrôle d'accès et restreindre les accès en fonction de la valeur d'un attribut particulier ou d'une combinaison de valeurs.

Certificat, côté serveur

Pour contacter un serveur dont l'accès est contrôlé par un mécanisme de sécurité basé sur des certificats, le navigateur client doit lui fournir un certificat et prouver qu'il en est bien le propriétaire. Si l'authentification s'avère positive, le serveur contrôle alors les droits de l'utilisateur aux ressources sollicitées, soit directement en fonction des informations contenues dans le certificat, soit en consultant une base de données. Dans ce dernier cas, le certificat sert seulement à authentifier le client, et les droits d'accès sont sauvegardés dans une base de données externe. Si cette approche permet de **distinguer l'identité d'un utilisateur de ses priviléges**, elle pose des problèmes de conception, de partage, de mise à jour, d'accès et de performance de la base de données. En revanche, si **les droits d'un utilisateur sont associés à son identité** dans son certificat, c'est-à-dire indépendamment d'une base de données précise, un serveur peut accepter des certificats provenant de diverses autorités de certification. La durée de vie d'un certificat, la mise à jour des informations du certificat, de leur pertinence et leur validité, restent un problème. De plus, il faut également savoir gérer une liste de révocation des certificats, ce qui revient à devoir accéder à une base de données externe, annulant par là même les avantages de cette solution.

Limites et validité des certificats

La puissance d'un mécanisme de contrôle d'accès basé sur des certificats repose sur le fait que seul le propriétaire du certificat possède la clé privée mathématiquement liée à la clé publique contenue dans un certificat. Un problème majeur de la certification est lié au fait que les utilisateurs oublient ou divulguent leur mot de passe de

protection de leur clé privée. D'autres désagréments sont relatifs à l'altération du certificat ou de la clé privée, suite à un incident du poste de travail de l'utilisateur ou à une mise à jour du navigateur. Il est donc nécessaire de se doter des moyens de retrouver une clé privée.

À ces inconvénients, ajoutons la possibilité de pouvoir fabriquer de fausses signatures numériques en devinant la clé privée ou l'algorithme de chiffrement (l'algorithme n'est pas un secret et en général il s'agit de l'AES). Ainsi, la confiance que l'on peut avoir dans un certificat (qui reflète son degré de sûreté) est limitée d'une part, par la robustesse de l'algorithme de chiffrement employé et d'autre part, par la sûreté de la clé privée de l'utilisateur. Cette dernière est généralement archivée sous forme chiffrée sur un PC et est déverrouillée par un mot de passe à chaque fois que le navigateur en a besoin.

Un élément intervenant dans la qualité du certificat est relatif aux procédures de certification de l'autorité de certification. En effet, le **degré de fiabilité du certificat** dépend de la capacité de l'autorité à valider la véracité de l'identification de l'utilisateur demandant un certificat. Les procédures d'authentification d'un demandeur varient d'une autorité à une autre. C'est de la responsabilité de l'autorité de certification de vérifier et de contrôler l'identité d'un demandeur. Selon le degré de vérification qu'elle effectue lors de l'établissement d'un certificat, différents types de certificats de divers niveaux de sécurité existent (Cf. chapitre 5 – classes de certificats).

Enfin, la **sécurité globale** du système dépend de la sécurité de la clé privée de l'autorité de certification qui permet de signer un certificat pour en garantir son authenticité et établir la confiance. En effet, s'il arrivait qu'elle soit volée, le détenteur pourrait se substituer à la véritable autorité de certification et fabriquer de faux certificats.

6.4.6 Gestion des autorisations d'accès *via* un serveur de noms

Le service d'annuaire qu'offre un **serveur de noms** peut être exploité pour réaliser la gestion des autorisations d'accès aux ressources informatiques mises en réseau. Il constitue alors une véritable plate-forme de réalisation du contrôle d'accès.

Pour des raisons de disponibilité et de sécurité du serveur, celui-ci devrait être correctement protégé et dupliqué avec un système de secours constamment opérationnel. Cette mesure de **back-up** est rarement implantée du fait de son coût de maintenance opérationnelle.

Généralement, les serveurs sont physiquement protégés et font l'objet de procédures d'accès renforcées. S'ils sont plusieurs à contribuer à rendre ce service, leur usage pose le problème de leur **synchronisation** et de leur **coopération**. Même s'ils sont plus ou moins conformes à la recommandation X.509 de l'UIT et que l'on y accède *via* le même protocole (LDAPv3), des implantations divergentes sont toujours possibles si l'on n'utilise pas la même plate-forme. La coexistence d'annuaires différents imposera de développer des interfaces de gestion distinctes.

Une alternative serait, pour disposer d'une seule interface de gestion, de développer un méta-annuaire les intégrant.

Quelle que soit la plate-forme retenue, le fait qu'elle soit unique ou distribuée, de même nature ou non, le fait que ce serveur soit hautement sollicité imposent au réseau une charge de trafic supplémentaire. Cela renvoie à un problème d'architecture et de dimensionnement du réseau pour assurer la disponibilité des ressources.

6.4.7 Contrôle d'accès basé sur des données biométriques

L'application de la **biométrie** au contrôle d'accès permettrait de se soustraire de l'usage de mots de passe en les substituant par une caractéristique physique dont on pourrait aisément extraire une donnée binaire. Associée à des mécanismes « classiques » d'authentification basée sur des mots de passe, la biométrie renforce le niveau de sécurité de ces derniers (notion de double contrôle).

D'après le *Petit Robert*, la biométrie est la « *science qui étudie à l'aide des mathématiques les variations biologiques à l'intérieur d'un groupe déterminé* ». On constate une distorsion de l'usage du sens initial de ce mot. En fait on devrait lui préférer le mot « **anthropométrie** », qui fait référence à une « *technique de mensuration du corps humain et de ses diverses parties* » qui peut alors conduire, par une méthode appropriée, à individualiser une personne (la différencier d'une autre) puis éventuellement à l'identifier.

Afin d'utiliser des **caractéristiques physiques** des personnes pour les identifier et valider leur identification, il est nécessaire d'extraire et d'enregistrer au préalable les **caractéristiques biométriques** des individus (notion de **gabarit**) (figure 6.12). Ces enregistrements doivent être réalisés d'une manière fiable et sauvegardés de façon sécurisée.

L'individualisation biométrique peut servir à contrôler l'identité d'un individu afin de réaliser un contrôle d'accès ou dans le cadre d'un contrôle judiciaire (police, etc.).

La durée du processus d'authentification peut être longue car la phase de comparaison doit tenir compte des variations inhérentes à la caractéristique vivante, donc mouvante, de la donnée testée. Ainsi, par exemple, comme deux échantillons vocaux d'une même personne ne sont jamais strictement les mêmes, la comparaison est basée sur un **traitement statistique et probabiliste** de la donnée biométrique. Cette part de flou introduite dans le système d'authentification ne permet pas d'avoir des résultats d'authentification avec un degré d'exactitude certain (le système ne peut pas certifier à 100 % qu'il s'agisse de la personne « *x* »). Le **taux d'erreur** de ces systèmes reste encore trop élevé pour garantir une sécurité absolue.

Associées à leur manque de précision, aux incertitudes sur la capacité à sécuriser correctement une base de données biométriques et aux coûts d'acquisition, de déploiement et de contrôle, les solutions de contrôle d'accès basées sur l'usage de données biométriques ne peuvent pas être considérées comme optimales. Toutefois,

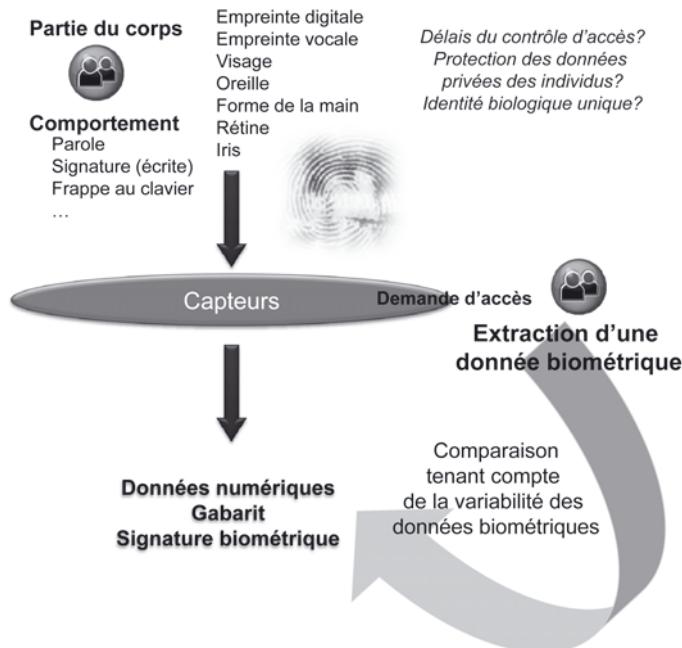


Figure 6.12 – Authentification basée sur des données biométriques.

ce type de solution est retenu pour identifier un citoyen au moyen de son passeport biométrique. Cela pose de nombreux problèmes notamment pour ce qui concerne la base de données contenant les gabarits biométriques. La numérisation d'une caractéristique biométrique pose le problème de son stockage « *Où, par qui et comment sera-t-elle manipulée et sécurisée ?* ». Le processus de numérisation engagé, pourquoi se limiter à deux empreintes, à celle de l'iris, de la rétine, de l'ADN, et ne pas y ajouter des données comportementales, des données relatives à la santé, aux goûts, aux orientations sexuelles, aux opinions politiques, à la religion... ? C'est ce qui est appelé la **biométrie multimodale**. De plus, si une donnée numérisée, telle que l'empreinte digitale, venait par exemple à être altérée ou modifiée dans la base de données, par erreur ou intentionnellement, la personne victime devra prouver qu'elle est bien la personne qu'elle est, avec de vraies empreintes, qui seront différentes de celles codées en binaire... Par ailleurs, une base de données centralisée comporte les risques suivants :

- de croisement de fichiers, d'agrégation, de croisement de données relatives à un individu ;
- d'une évolution de l'usage de la base par les pouvoirs publics ou par des entités commerciales (États autres que celui dont la personne est ressortissante, compagnies aériennes par exemple).

L'usage étendu du contrôle biométrique soulève de nombreux problèmes d'ordres éthique, ergonomique, économique, technologique et juridique. Pour n'en citer que quelques-uns :

- la **confidentialité**, l'**intégrité** et la protection de données biométriques ;
- la possibilité de ne pas avoir des **données biométriques uniques** (cas des vrais jumeaux) ;
- les capteurs de données biométriques sont souvent perçus, et à juste titre, comme étant intrusifs. Ils peuvent constituer également une **menace pour la protection de l'intimité** dans la mesure où il pourrait exister une prolifération de capteurs (caméras vidéo, lecteurs de puce RFID sans contact...) disséminés dans des environnements publics, qui agiraient à l'insu des individus ;
- les cas d'**usurpation** ou d'usages abusifs, frauduleux de données biométriques.

6.5 SÉCURITÉ DES RÉSEAUX

La sécurité des réseaux mis en œuvre et gérés par des entreprises, y compris ceux des opérateurs de télécommunication, dépend de l'entité organisationnelle qui en a la responsabilité et qui a autorité dans ce domaine. Les utilisateurs et clients, véritables abonnés de ces réseaux, sont également administrés par cette autorité. Les fonctions et services de sécurité répondent alors à une politique de sécurité bien déterminée. Cette approche centralisée et globale de la sécurité, qui pourrait apporter une cohérence et une protection « de bout en bout », ne peut pas être mise en œuvre dans une infrastructure Internet publique multiréseau. C'est aux utilisateurs (personnes physiques ou morales) de mettre en place des mesures de sécurité sur leurs systèmes et dans leur environnement ou de faire appel à des intermédiaires comme les autorités de certification par exemple.

6.5.1 Protection de l'infrastructure de transmission

L'**infrastructure de transmission** est à protéger physiquement et logiquement contre les vols¹³, destructions, attaques passives ou actives, accidents ou événements naturels. Il faut également protéger les transmissions d'éventuels rayonnements qui pourraient compromettre leur qualité.

Il existe des chiffreurs que l'on dispose entre le point d'accès à l'infrastructure et l'équipement de l'abonné. Un **boîtier de chiffrement** (chiffreur) exécute un algorithme de chiffrement à partir de clés. Certains sont capables d'autogénérer des clés de chiffrement (élaboration automatique de clés à partir d'un secret donné lors de son initialisation) et de les diffuser. Les équipements de chiffrement programmés pour changer de clés toutes les x secondes s'échangent des informations qui leur

13. Le vol des câbles en cuivre (pour la revente du cuivre) est devenu problématique du point de vue de la disponibilité des ressources de transmission.

permettent de calculer une clé de session. Si les chiffreurs ne sont pas capables de s'autosynchroniser, le problème complexe du maintien de leur synchronisation, ou plutôt de la resynchronisation après interruption, se pose. Les équipements des abonnés doivent détecter cette désynchronisation, la signifier au chiffreur et la traiter. Certains chiffreurs peuvent également s'autoprotéger en détruisant leur contenu en cas de détection d'incidents. Une intervention manuelle est alors indispensable pour relancer leur activité car ils ne sont plus téléchargeables.

6.5.2 Protection du réseau de transport

Il est impératif de savoir **protéger les raccordements** des utilisateurs et leurs données. Pour cela, il faut les identifier (qui sont les usagers ?), les localiser (où sont-ils ?) et connaître leurs besoins (quels sont les flux applicatifs transportés ?).

En tenant compte de la problématique de la sécurité lors du transfert de données et en sachant que tout peut être facilement intercepté sur un réseau, la confidentialité et l'intégrité des données des usagers passent également par le **chiffrement des flux applicatifs** (cf. chapitre 9).

La protection d'un réseau de transport s'obtient par l'adoption dans le réseau de **routeurs chiffreurs** intelligents ayant la possibilité d'effectuer de façon intégrée et sélective des procédures de chiffrement. Elle s'appuie aussi sur des mesures de sécurité physique et logique des systèmes, sur la détection des incidents et des programmes malveillants, et sur le cloisonnement des environnements réseau par des systèmes pare-feu (cf. chapitre 8).

6.5.3 Protection des flux applicatifs et de la sphère de l'utilisateur

La protection des données au niveau de l'équipement **de l'utilisateur** qui met en œuvre une application distribuée ne dépend plus du transporteur de données, mais bien de son **environnement direct**, en fonction de l'application traitée, du service sollicité et de la plate-forme informatique sur laquelle il s'exécute. La difficulté de la protection des applications réside dans le fait qu'il faille protéger tout l'environnement applicatif matériel et logiciel (et non pas seulement l'application elle-même) et par extension son environnement physique (locaux, énergie, etc.). Le système d'exploitation de l'équipement de l'utilisateur joue un rôle prépondérant dans sa protection (impossibilité de prendre la main lors d'une session, déconnexion automatique après un certain temps, etc.). Cela passe également par la **protection des cartes réseaux**, par le support de **protocoles d'application cryptographiques**, par des opérations de **mirroring** et de **duplexing** (protection des informations en les dupliquant sur des disques, redondance des opérations d'écriture et des équipements...). Pour rendre confidentielles les données et assurer leur intégrité, il faut mettre en œuvre des procédures de chiffrement.



Pour la visioconférence, par exemple, on utilise la technique de **codage MIC** (modulation par impulsions codées) pour véhiculer les données. On constitue alors des trames d'information, basées sur l'utilisation judicieuse d'intervalles de temps. Pour chiffrer ce type d'application, on doit pouvoir disposer de chiffreurs capables de chiffrer indépendamment les intervalles de temps (on chiffre intervalle de temps par intervalle de temps).

Chaque applicatif peut nécessiter un équipement de chiffrement/déchiffrement particulier. Il en est de même au niveau du raccordement au réseau de transport et au niveau de l'infrastructure de support. Le plus compliqué n'est pas de réaliser des matériels de chiffrement (les équipementiers savent très bien le faire) mais de les mettre en œuvre et de les gérer de façon optimale et performante. Il n'est pas nécessaire de tout chiffrer car toutes les données ne sont pas des informations sensibles et de plus, les temps de traitement additionnels induits par les processus de chiffrement sont importants. Ainsi, il faut pouvoir distinguer les données qui doivent absolument être chiffrées des données non confidentielles (notion de **discrimination des données**). Ceci doit être réalisé en amont de l'implantation de mesures techniques et opérationnelles de chiffrement, notamment lors de la définition de la politique de sécurité.

6.5.4 Protection optimale

Une offre complète de sécurisation des échanges consiste à assurer :

- la sécurité physique des équipements et des infrastructures ;
- la sécurité des télécommunications au niveau de leur transmission ;
- la sécurité des échanges au niveau du transport ;
- la sécurité des données et des applicatifs.

Trois domaines de **responsabilités** interviennent lors des échanges : celui de l'utilisateur final, celui du transporteur et celui qui offre le service de support (à moins que ces deux derniers ne soient la même entité). Il se pose alors le problème de gestion (au sens « gestion de réseau ») de l'interface de raccordement (appartenance, boîtier de chiffrement, universalité).

Pour sécuriser le transfert de données, diverses options complémentaires existent. Des mécanismes d'authentification et de chiffrement peuvent être directement intégrés au niveau des **protocoles « réseau »**, comme le propose la nouvelle version du protocole Internet (IPv6, IPSec). Le trafic applicatif est alors protégé sans que l'application ne s'en préoccupe. Arrivées à destination, les données reçues sont automatiquement déchiffrées avant d'être délivrées à l'application.

Cela revient à intégrer les processus de sécurité **au niveau de l'infrastructure de communication**. Cette dernière doit donc être à même de les supporter dans leur intégralité. Cela nécessite le plus souvent la mise à jour de l'ensemble des routeurs la constituant, pouvant parfois conduire à des problèmes d'interopérabilité de ceux-ci et de gestion du changement.

L'avantage principal du chiffrement au niveau de l'infrastructure du réseau réside dans l'indépendance de l'application et des mécanismes de chiffrement liés au transfert, qui sont alors complètement transparents pour l'utilisateur.

Par ailleurs, chiffrer les données au niveau « réseau » génère des paquets de données de taille supérieure à des paquets non chiffrés ; leur transfert monopolise donc plus de bande passante et de ressources de communication. Associées au fait que le processus de chiffrement augmente le temps de traitement des paquets, les performances du réseau peuvent considérablement être affectées par la mise en œuvre de la sécurité à ce niveau.

En revanche, la sécurité des transactions **au niveau applicatif** modifie l'application elle-même et les données sont chiffrées avant d'être livrées au protocole de réseau qui en effectuera l'acheminement. Elles sont ensuite déchiffrées par le serveur d'application destinataire. C'est lors de la phase d'établissement du dialogue entre des entités applicatives (un client et un serveur par exemple) que l'on réalise l'authentification et la négociation d'une clé de session. La complexité de cette phase peut varier et demande un délai d'établissement lui aussi variable.

Sécuriser l'infrastructure de transport ou sécuriser l'application revient à traiter, à des niveaux différents, un même type de problèmes :

- les processus et les utilisateurs doivent être identifiés et authentifiés ;
- l'émetteur et le récepteur doivent utiliser un même algorithme de chiffrement/déchiffrement (ce dernier doit pouvoir éventuellement être négocié) ;
- les clés de chiffrement/déchiffrement doivent être gérées, distribuées et attribuées à chaque entité communicante.

6.5.5 Sécurité du cloud

Désormais, certains fournisseurs de services proposent aux organisations et aux individus d'externaliser tout ou une partie de leur informatique (capacité informatique, traitement et stockage de données) sur leurs propres infrastructures et ressources, dont ils assurent la sécurité. L'informatique en nuage (**cloud computing**) est révélatrice de l'évolution de l'infrastructure du réseau et des services, et de la manière d'appréhender les traitements sur une communauté de ressources mises en commun, partageables selon les besoins des utilisateurs et consommables à la demande.



Le cloud : des services génériques, configurables ou spécifiques, à la demande : *Software as a Service* (SaaS) ; *Platform as a Service* (PaaS) ; *Infrastructure as a Service* (IaaS).

Cela permet, en théorie, de disposer d'une infinité de ressources et d'une puissance de calcul quasi illimitée, durant un laps de temps déterminé, sans pour autant avoir à acquérir et à financer une telle infrastructure mais en payant uniquement le service rendu. En fait, le nombre des ressources cloud impliquées est fonction des besoins de l'organisation (mise à l'échelle – *scalability*) et peut donc s'adapter à ceux-ci (notion d'élasticité, augmentation ou réduction du nombre de ressources en

fonction des traitements). Il s'agit alors de payer spécifiquement la consommation des ressources, selon des modèles économiques variables (forfaitairement, à l'usage...) des propriétaires des ressources. Cela permet de répondre également au besoin de réduction ou de rationalisation des coûts en personnel de l'organisation qui externalise son informatique. L'usage de l'infrastructure informatique est alors considéré comme un service fourni par un prestataire tiers. Cela peut conduire des entreprises à externaliser des applications informatiques vues comme des services pour les métiers concernés (notion de **virtualisation des ressources**). L'informatique en nuage s'appuie sur une grande quantité de serveurs de stockage et de traitement des données (fermes de serveurs) ainsi que sur une infrastructure de télécommunication basée sur des technologies Internet.

Cette vision de l'informatique n'est pas sans poser des questions technologiques, économiques, juridiques, sécuritaires et environnementales. Elle renforce considérablement l'importance du réseau, puisque sans réseau il devient impossible d'accéder à l'information et aux services délocalisés dans le nuage informatique. Elle accroît la dépendance vis-à-vis des fournisseurs de ces services, des opérateurs de centres de données (*datacenters*) et du réseau dans son ensemble. Au **niveau géopolitique**, on commence à prendre conscience de ces nouveaux risques et **enjeux stratégiques**.

Il faut être attentif aux enjeux de la **perte de la maîtrise des données** sur le long terme et ne pas regarder uniquement les avantages économiques que procurent, à court terme, voire immédiatement, des solutions d'externalisation de cloud computing. La **dépendance** à un seul fournisseur de cloud est également un problème, ce dernier se trouve en situation de monopole vis-à-vis des données et des traitements d'une institution ou d'une personne. La possibilité de diversifier son externalisation sur différents fournisseurs de cloud est quasi impossible, comme l'est d'ailleurs le retour arrière à des solutions de « non-cloud ».

Par principe, lorsque l'informatique ou les données sont sensibles, stratégiques et vitales pour l'organisation, le bon sens nous dit qu'il ne faudrait pas externaliser.

Les **principaux risques** lors d'une externalisation cloud sont :

- la perte de la maîtrise (de la gouvernance) de ses données ;
- la difficulté à assurer et à vérifier que les contraintes de conformité réglementaire auxquelles les données sont soumises sont satisfaites ;
- les données étant localisées « ailleurs » (on ne sait pas où), en tous les cas sur des serveurs potentiellement localisés dans des pays différents de celui où se trouve le siège de l'entreprise et donc, dans d'autres juridictions, cela peut entraîner des risques liés au fait qu'elles dépendent ainsi d'une autre juridiction et que d'autres lois s'appliquent ;
- la défaillance du réseau entraînant l'indisponibilité d'accès au cloud, aux traitements, aux données (incapacité de travailler) ;
- le droit excessif – priviléges d'accès accordés aux gestionnaires du cloud (et aux prestataires qui travaillent pour eux), possibilité d'usage abusif de ces droits (risque interne au fournisseur) ;

- la difficulté à assurer des audits de ses propres données et traitements dans un cloud de prestataire externe ;
- le cloud héberge l'informatique de multiples entreprises. Il peut y avoir des problèmes liés au fait que les environnements/les données qui appartiennent à des entreprises différentes, et qui doivent être en principe disjoints, ne soient pas bien séparés (risque de perte de confidentialité, d'intégrité, de disponibilité des données) ;
- il est difficile de s'assurer que les données que l'entreprise veut détruire – effacer du cloud – soient effectivement bien effacées (un peu comme sur Facebook quand on souhaite de plus y être, les données persistent chez le fournisseur).

Est-ce qu'on donnerait la seule clé de la porte blindée de son appartement à un prestataire externe qui va l'héberger ailleurs – on ne sait où – peut être dans un endroit où il y a une réglementation qui demande de copier les clés, de les utiliser pour vérifier que le ménage est bien fait (contrainte légale du pays de l'hébergeur) ? Est-il imaginable d'être obligé de demander à un prestataire sa clé à chaque fois que l'on souhaite entrer chez soi ? *Quid* si ce dernier n'est pas disponible pour des problèmes techniques, ou qu'il sous-traite la garde de notre clé à un autre prestataire ? Il s'agit d'un problème de **confiance** envers le prestataire et les contrats ne protègent pas de tout !

Pour qu'une donnée sensible ait sa place dans un cloud extérieur, il faudrait qu'elle soit chiffrée. Se pose alors ce problème : Qui gère les clés de chiffrement ? D'autre part, pour faire des calculs sur des données chiffrées résidant dans le cloud, et obtenir le bon résultat quand on le déchiffre, il faudra attendre que le **chiffrement homomorphe** (capacité à pouvoir réaliser des traitements sur des cryptogrammes sans avoir accès aux données en clair) puisse prévoir tous les cas de calcul et se généralise.

L'**ENISA** (*European Network and Information Security Agency*)¹⁴, comme l'Agence nationale de la sécurité des systèmes d'information (**ANSSI**)¹⁵, propose des guides concernant les risques liés au cloud computing.

Avant toute décision d'externalisation de données ou de traitement de celles-ci, il faut identifier les principaux risques pour comprendre que s'il s'agit de données sensibles, que cela soit pour une administration publique ou une entreprise privée, la prise de décision d'externaliser ou non est un choix stratégique d'assumer la prise de risque que cela comporte, en toute connaissance de cause. Une analyse des risques qui tient compte notamment du type et de l'importance des informations à externaliser et des contraintes légales et réglementaires auxquelles l'organisation est soumise doit impérativement être réalisée. Ainsi, s'il est alors décidé d'opter pour des solutions **d'infogérance**, il sera alors possible d'exprimer des exigences de sécurité qui pourront être intégrées dans un contrat de service afin d'engager la responsabilité du fournisseur à les satisfaire.

14. <http://www.enisa.europa.eu/activities/risk-management/files/deliverables/cloud-computingrisk-assessment>

15. <http://www.ssi.gouv.fr/fr/bonnes-pratiques/recommandations-et-guides/securite-de-l-externalisation/externalisation-et-securite-des-systemes-d-information-un-guide-pour-maitriser.html>

Résumé

La sécurité des infrastructures de communication est primordiale à la sécurité des organisations. Afin de sécuriser les infrastructures de communication, il est obligatoire de passer par l'utilisation de protocoles cryptographiques offrant des services de sécurité (authentification, intégrité, confidentialité et non-répudiation) et de mettre en œuvre des mécanismes efficaces de contrôle des accès logiques et physiques.

IPSec permet de remédier à certaines failles sécuritaires de IPv4. Il assure ainsi les critères de sécurité mentionnés précédemment par l'intermédiaire des en-têtes AH (*Authentication Header*) et ESP (*Encapsulating Security Payload*). L'utilisation d'IPSec reste optionnelle dans le protocole IPv4 mais obligatoire dans le protocole IPv6, qui apporte, en plus de la sécurité, des services additionnels (adresage étendu, étiquetage de flux d'information, allocation dynamique de bande passante, etc.).

D'autres mesures de sécurité doivent être réalisées pour protéger les transferts de données. Il est primordial que les adresses, les processus, les systèmes impliqués dans la gestion des noms et des adresses ou dans l'acheminement des données, soient disponibles, intègres, fiables et sécurisés. Il est de la responsabilité des entités en charge des infrastructures de télécommunication et des fournisseurs de service de cloud de protéger et de gérer efficacement leurs environnements et ressources partagées afin d'offrir des niveaux de sécurité satisfaisant les exigences et besoins des utilisateurs.

Exercices

6.1 Est-ce que le protocole TCP permet de pallier le défaut de sécurité du protocole IPv4 ?

6.2 À quels besoins répond la version 6 du protocole IP (IPv6) ? Quelles sont les principales caractéristiques du protocole IPv6 ?

6.3 Quelles différences et relations existe-t-il entre IPv6, IPSec et IPv4 ?

6.4 Comment garantir l'authentification des paquets IP et leur intégrité ?

6.5 Comment s'effectue la gestion des clés de chiffrement dans le protocole IPSec ?

6.6 À quels besoins répondent les modes opératoires « mode transport » et « mode tunnel » du protocole IPSec ?

6.7 Quels sont les risques sécuritaires liés au routage dans un réseau Internet ?

6.8 Pourquoi doit-on particulièrement bien protéger des serveurs de noms (DNS) dans une infrastructure de réseau ? Comment doit-on faire ?

6.9 Quelles sont les limites des certificats numériques utilisés pour le contrôle d'accès ?

6.10 Quelles sont les limites de l'usage de données biométriques pour le contrôle d'accès ?

6.11 Quelles relations existe-t-il entre la gestion des identités et le contrôle d'accès ?

6.12 Quel protocole permet de créer un réseau privé virtuel (VPN) ?

6.13 À partir de quels types de données biométriques peut-on développer un mécanisme de contrôle d'accès ?

6.14 Qu'est-ce qu'un mot de passe robuste ?

6.15 Quels sont les différents niveaux de sécurisation d'une infrastructure de télécommunication ?

Solutions

6.1 Non, le protocole TCP ne permet pas d'offrir des services de sécurité contribuant à la disponibilité, l'intégrité, la confidentialité des données ou d'authentification des émetteurs/récepteurs. Il autorise seulement une certaine qualité de service du fait qu'il fonctionne en mode connecté alors que le protocole IPv4 fonctionne en mode non connecté de paquets et qu'il ne permet pas de réaliser l'authentification de la source ou de la destination des paquets, ni la confidentialité des données véhiculées, ni un contrôle d'intégrité, ni la non-répudiation des transactions.

6.2 La **version 6 du protocole IP** (IPv6 [RFC 2460]) répond aux besoins d'intégrer en mode natif, dans le protocole, des capacités (a) qui permettent de développer des services de sécurité (support de procédures d'authentification et de chiffrement, *via* des en-têtes à options et capacité à créer des réseaux IP virtuels) ; (b) d'étendre l'espace des adresses IP disponibles (support d'un adressage étendu et hiérarchisé). Les adresses sont codées sur 128 bits (16 octets) et non plus sur 32 bits (4 octets) comme dans la version 4 et (c) de pouvoir faire de l'allocation dynamique de bande passante pour le support d'applications multimédias.

Dans cette version, les adresses IP sont représentées en nombres hexadécimaux séparés par des deux-points tous les deux octets et non plus en notation décimale pointée.

L'utilisation d'IPv6 impose, entre autres, la modification du schéma d'adressage, de gestion des adresses, la mise en place dans tout l'environnement Internet de systèmes supportant cette nouvelle version du protocole, des systèmes fonctionnant avec les deux versions, la synchronisation à grande échelle de la migration des versions, etc.

6.3 **IPv6** supporte toutes les facilités décrites dans la réponse de l'exercice 6.2, tandis que IPSec fait référence uniquement aux en-têtes de sécurité ESP et AH du protocole IPv6. La mise en œuvre d'**IPSec** nécessite le protocole IPv4 pour transporter les paquets IPSec (ce qui n'est pas le cas de IPv6). Outre le fait que IPv6 constitue la nouvelle génération du protocole **IPv4** et IPSec une version intermédiaire entre les deux qui évite de devoir modifier l'adressage des systèmes et tables de routage des routeurs.

6.4 **L'authentification et l'intégrité des paquets IP** échangés entre deux entités peuvent être réalisées *via* le protocole IPSec et notamment en utilisant l'en-tête d'authentification (AH).

Après que l'émetteur et le destinataire se sont mis d'accord sur les différents paramètres de l'association de sécurité (SA) qu'ils utiliseront, la source et le récepteur partagent une clé secrète qu'ils sont seuls à connaître. L'algorithme utilisé pour la vérification est également spécifié par l'association de sécurité. Cet algorithme n'est autre qu'une fonction de *hashage* comme par exemple HMAC-MD5 ou HMAC-SHA-1. Cette fonction est alors appliquée sur le message et prend la clé secrète comme paramètre. Le résultat de cette fonction est une valeur de contrôle d'intégrité (ICV). Elle est intégrée dans l'en-tête du paquet transmis. À sa réception, la même fonction de *hashage* est exécutée. Si le résultat correspond à l'ICV envoyé par la source alors l'authenticité ainsi que l'intégrité du message sont vérifiées, sinon le paquet est rejeté.

6.5 La **gestion de clés de chiffrement du protocole IPSec** peut invoquer des protocoles d'échanges de clés comme par exemple *Oakley Key Determination Protocol*, ISAKMP (RFC 2408) et IKE (RFC 2409) ; ce dernier est une implémentation pratique de ISAKMP. Ces protocoles présentent des faiblesses surtout lors de la génération et de la distribution de la première clé de chiffrement. De plus, les mécanismes employés par ces protocoles sont basés sur la cryptographie classique et sur des fonctions mathématiques à sens unique (*one-way functions*). Ces mécanismes ne sont pas inconditionnellement sécurisés et leur fragilité a été prouvée par divers cryptographes, notamment pour ce qui est de l'algorithme Diffie-Hellman (sur lequel se basent ces mécanismes pour assurer la distribution et la génération de clés) et des fonctions de *hashage* telles que SHA-1, qui est largement utilisé dans les mécanismes de signature électronique. L'apport du quantique dans la distribution des clés de chiffrement a été démontré et son usage devrait s'intensifier dans le futur.

6.6 Le mode « **transport** » du protocole IPSec permet de sécuriser uniquement la partie « données » et non l'en-tête du protocole. Cela peut être suffisant pour assurer la confidentialité des données mais non celle du flux. Encapsuler un paquet IP dans un paquet IPSec lui-même encapsulé dans un autre paquet IP, en utilisant un mode « **tunnel** », permet de masquer toutes les informations y compris celles d'adressage du paquet initial et ainsi de créer un canal de communication sûr *via* l'usage d'un canal sécurisé dont les extrémités ont été authentifiées (notion de réseaux privés virtuels).

6.7 Les principaux **risques sécuritaires liés au routage** des paquets au travers du réseau Internet sont liés aux menaces d'attaques passives ou actives dont les conséquences peuvent être les suivantes :

Détournement des données par infection ou modification des tables de routages ayant une origine criminelle (virus, programmes malveillants) ou accidentelle (défaut lors de la programmation des logiciels des routeurs, mauvaises configurations, variation inattendue du courant électrique alimentant les routeurs).

Atteintes à la confidentialité et à l'intégrité des données par destruction, modification et copies des données : étant donné que les informations contenues dans les paquets IP sont véhiculées en clair et sans contrôle d'intégrité, il est toujours possible de les altérer ou simplement de les écouter et de copier lors de leur acheminement.

Déni de service : un refus de service peut être occasionné par la saturation de la mémoire d'un routeur ou par une surcharge de requêtes. Cela entraîne des dysfonctionnements pouvant conduire à l'arrêt des routeurs et à l'indisponibilité de l'infrastructure. La perte des données en transit est alors possible. L'inondation d'un réseau peut avoir lieu si certaines fonctions des routeurs sont activées comme la fonction de *broadcasting* (diffusion) des messages d'information (ICMP) ou même par les messages de configuration des routes. Ce nombre de messages, s'il dépasse un certain seuil, diminue l'efficacité des routeurs et réduit la bande passante du réseau puisque celle-ci est alors utilisée pour l'échange de messages de signalisations.

6.8 Il est impératif de pouvoir **protéger physiquement les serveurs de noms et d'assurer la sécurité des données et des processus de traitement** qu'ils supportent. En effet, il s'agit de systèmes cruciaux dans la réalisation et la mise en œuvre non seulement des communications mais aussi de la sécurité.

Les serveurs de noms, annuaires électroniques ou DNS (*Domain Name Server*) constituent une famille d'outils indispensables et incontournables dans la mesure où ils permettent la réalisation de la plupart des applications et des services Internet et des services liés à la gestion des certificats numériques, à l'authentification, à la gestion des profils d'utilisateurs par exemple. Du fait que les serveurs de noms peuvent mémoriser des données sensibles, les identifications et les adresses des entités et des utilisateurs du réseau, les accès à ces serveurs doivent être contrôlés, certaines informations peuvent être chiffrées, des processus de surveillance et d'enregistrement des actions à des fins de traçabilité et d'imputation doivent également être assurées. Protéger un serveur de noms de l'entreprise est primordial si l'on désire garantir un certain niveau de sécurité.

Des procédures de chiffrement, de contrôle d'accès, d'authentification sont donc à mettre en place. Le positionnement du serveur de noms dans l'architecture du réseau et plus particulièrement par rapport aux pare-feu, comme sa configuration, sont également très importants. Sa gestion, notamment *via* le protocole de gestion SNMP, doit satisfaire à des contraintes d'authentification forte.

6.9 La mise en œuvre de **certificats numériques** pour effectuer le contrôle d'accès aux ressources trouve ses limites dans la validité des informations contenues dans le certificat (véracité, authentification de l'information, durée de vie de la certification) et également dans le fait qu'il puisse exister de « vrais-faux » certificats (vol, falsification de certificats).

6.10 Le contrôle d'accès réalisé à partir de **données biométriques** des utilisateurs nécessite (a) d'enregistrer et de stoker la signature biométrique des individus sous forme numérique afin d'avoir un échantillon de comparaison ; (b) de prélever et de collecter à chaque demande d'accès un échantillon des données biométriques. Cela pose divers problèmes relevant notamment du caractère numérique, donc fragile de l'échantillon de référence (qui est à protéger comme un secret), du caractère vivant et évolutif des données prélevées (la variabilité ne permet pas de garantir la fiabilité du système). Il est erroné de penser qu'un système basé sur la biométrique est sûr. Selon les systèmes, la probabilité d'avoir des faux positifs ou des faux négatifs peut être importante. Cette probabilité dépend de la technique et de la qualité d'enregistrement des données biométriques.

6.11 Pour pouvoir effectuer le contrôle d'accès aux ressources, il faut au préalable avoir effectué **l'identification des utilisateurs et leur avoir affecté leurs droits d'accès** (ou permissions). Ainsi, la gestion des droits et le contrôle d'accès passent par la gestion des identités des utilisateurs. Cela peut être parfois compris dans ce que certains dénomment la gestion des profils des utilisateurs.

6.12 La création d'un réseau virtuel sur Internet (VPN) qui offre une connexion sécurisée dont les deux extrémités sont authentifiées est possible *via* la mise en œuvre du IPSec.

6.13 En fait, il est possible de développer des mécanismes de contrôle d'accès biométrique à partir de caractéristiques morphologiques uniques, qui permettent de distinguer, de différencier des personnes, comme par exemple : l'empreinte digitale, l'empreinte vocale, l'empreinte rétinienne, la forme de la main, la taille et la forme du visage ou des oreilles.

6.14 Un mot de passe robuste est un mot de passe qui ne cède pas facilement à des tentatives de découvertes par des attaques par dictionnaire ou par la récolte d'informations sur l'utilisateur. Un tel mot de passe devrait normalement être long et intégrer des caractères spéciaux.

6.15 Les infrastructures de télécommunication peuvent être sécurisées à plusieurs niveaux en passant par la sécurité physique des locaux et des matériels sensibles à la sécurité logique. La sécurité logique peut être réalisée à différents niveaux protocologiques (protection du signal de transmission, chiffrement aux niveaux Liaison, Réseau, Transport et Application) mais aussi *via* des mécanismes de contrôle d'accès et de sécurité des plates-formes logicielles (système d'exploitation, programmes et données).

LA SÉCURITÉ DES RÉSEAUX SANS FIL

7

PLAN

OBJECTIFS

- 7.1 Mobilité et sécurité
- 7.2 Réseaux cellulaires
- 7.3 Sécurité des réseaux GSM
- 7.4 Sécurité des réseaux GPRS
- 7.5 Sécurité des réseaux UMTS
- 7.6 Réseaux locaux sans fil 802.11
- 7.7 Réseaux personnels sans fil

► Présenter les principaux problèmes de sécurité posés par l'usage des réseaux sans fil ainsi que les techniques et services de sécurité offerts pour y remédier¹.

7.1 MOBILITÉ ET SÉCURITÉ

Les réseaux qui autorisent la mobilité des utilisateurs tout en communiquant sont ceux qui s'appuient sur une interface radio pour transmettre des données à partir ou vers les systèmes utilisateurs. Parmi les réseaux sans fil, les **réseaux cellulaires**, les **réseaux locaux sans fil de type 802.11** (réseau Wi-Fi, *Wireless Fidelity*) ainsi que les **réseaux personnels** utilisant la technologie **Bluetooth** sont les plus répandus.

L'usage de l'interface radio induit deux problèmes de sécurité typiques des réseaux sans fil :

- l'écoute, l'interception du trafic sur le lien radio ;
- le déni de service, l'indisponibilité du réseau, la sensibilité au brouillage ;
- l'utilisation des ressources radio par des utilisateurs non autorisés.

Les mesures de sécurité mises en œuvre dans les réseaux sans fil ont pour objectif de permettre d'atteindre un niveau de sécurité similaire à celui existant dans les réseaux filaires.

1. Ce chapitre est réalisé avec la collaboration de Thi Mai Trang Nguyen.

7.2 RÉSEAUX CELLULAIRES

Le découpage de la surface géographique en **cellules** pour une utilisation efficace de la ressource radio a donné naissance aux réseaux cellulaires. Les réseaux cellulaires ont évolué en trois temps :

- Les systèmes de première génération étaient analogiques et n'ont plus cours.
- Les systèmes de deuxième génération sont numériques, dédiés essentiellement au transfert de la voix et fonctionnent en commutation de circuit. Il s'agit du **réseau GSM** (*Global System for Mobile*). Le **réseau GPRS** (*General Packet Radio Service*) est considéré comme étant un réseau de génération deux et demie.
- Les systèmes de troisième génération (3G, 3G+ pour des débits plus importants et 4G pour le haut débit²) sont basés sur la commutation de paquets IP. Le **réseau UMTS** (*Universal Mobile Telecommunication System*) offre un accès large bande pour les services voix, données et multimédia.

Dans un réseau cellulaire, l'espace géographique est divisé en cellules. Chaque cellule est desservie par une **station de base (BTS, Base Transceiver Station)** qui permet aux terminaux mobiles situés dans la cellule de communiquer. Afin d'optimiser l'usage des fréquences radio et ainsi d'augmenter le nombre d'utilisateurs potentiels, une bande de fréquence utilisée dans une cellule peut être réutilisée dans une autre cellule non adjacente.

Les stations de base (BTS) sont connectées à d'autres éléments du réseau cellulaire par les moyens filaires pour offrir les services de la mobilité et des accès aux réseaux fixes. Ces éléments sont spécifiques au type de réseau cellulaire.

Dans le réseau **GSM**, plusieurs stations de base sont connectées à un **contrôleur (BSC, Base Station Controller)** qui contrôle l'allocation des canaux radio, prend la décision de changement de cellule (**handover**) du terminal, et concentre les trafics venant des stations de base vers le centre de commutation (MSC, *Mobile Switching Centre*).

Le **MSSC** (*Mobile Services Switching Center*) est un commutateur qui connecte le réseau GSM au réseau téléphonique fixe, et gère la communication entre un mobile et un autre centre de commutation (MSC).

Pour permettre l'accès au réseau et gérer la mobilité d'un utilisateur, deux types de bases de données sont utilisés :

- le **HLR** (*Home Location Register*), qui mémorise les informations des abonnés du réseau GSM d'un opérateur ;
- le **VLR** (*Visitor Location Register*), qui contient des informations des abonnés actuellement présents dans une zone géographique gérée par un ou plusieurs centre(s) de commutation (MSC) d'un opérateur. Il peut s'agir des abonnés de l'opérateur ou d'abonnés d'un autre opérateur (lors du *roaming*).

2. Le passage à la 4G ou à la 5G est coûteux et s'inscrit dans une évolution des infrastructures des opérateurs sur le long terme. Le sigle LTE (*Long Term Evolution*) est souvent associé à la 4G dont le déploiement en France a débuté dans certaines grandes villes en 2013 / 2014 et se poursuit.

Dans la phase 2+ du GSM, l'ETSI (*European Telecommunications Standards Institute*) a ajouté une fonction **GPRS** permettant l'utilisation des réseaux de données en plus de l'utilisation du réseau téléphonique fixe. Dans un réseau GSM intégrant la fonction GPRS, un contrôleur de station de base (BSC) est également connecté à un noeud de support de GPRS, le **SGSN** (*Serving GPRS Support Node*).

Une unité **PCU** (*Packet Control Unit*) est associée au BSC pour le transfert des données en mode paquet. Un mobile GPRS envoie des données en mode paquet, qui sont alors transmises vers le SGSN, et un appel téléphonique en mode circuit vers le MSC. Le SGSN est un routeur qui gère les terminaux dans une zone donnée. L'ensemble des SGSN est connecté à une **passerelle GGSN** (*Gateway GPRS Support Node*) qui relie le réseau GPRS à un réseau de données comme Internet. Le SGSN possède un rôle équivalent à celui d'un MSC/VLR dans le réseau GSM.

En revanche, le réseau cellulaire de **troisième génération UMTS** fonctionne en mode paquet. Le **node-B** correspond au BTS dans l'architecture GSM. L'élément **RNC** (*Radio Network Controller*) joue un rôle équivalent à celui d'un BSC dans l'architecture GSM.

7.3 SÉCURITÉ DES RÉSEAUX GSM

Dans un réseau GSM, les **services de sécurité** ainsi que les moyens de les réaliser sont les suivants³ :

- la confidentialité de l'identité de l'abonné par l'attribution d'une identité temporaire ;
- l'authentification de l'identité de l'abonné par la mise en œuvre d'un processus d'authentification basé sur une technique de « *challenge-response* » ;
- la confidentialité des données des utilisateurs et de certaines informations de signalisation par chiffrement.

7.3.1 Confidentialité de l'identité de l'abonné

Lors de la souscription au service, l'opérateur fournit à l'abonné une **carte SIM** (*Subscriber Identity Module*) qu'il faut adjoindre au terminal pour pouvoir communiquer. Il s'agit d'une carte à puce qui contient l'identité de l'abonné sous la forme d'un **IMSI** (*International Mobile Subscriber Identity*) qui est unique. L'IMSI est utilisé par le réseau pour identifier un abonné.

Le numéro de téléphone est un numéro **MSISDN** (*Mobile Station ISDN Number*)⁴. La correspondance IMSI-MSISDN est stockée dans le **HLR**. En cas de perte ou de vol de la carte SIM, l'opérateur peut bloquer l'IMSI et la carte SIM ne sera plus utilisable. Une autre carte SIM (*i.e.* une autre identité IMSI) sera allouée à l'abonné, qui pourra conserver son numéro de téléphone (le même MSISDN).

3. ETSI, *Recommendation GSM 02.09*, 1993.

4. ISDN, *Integrated Services Digital Network*.

Pour que l'identité de l'abonné soit **confIDENTIELLE**, l'IMSI ne doit pas être intercepté par des entités non autorisées lorsqu'elle est transmise dans les messages de signalisation. La solution retenue consiste à limiter le plus possible l'envoi de cette identité sur le lien radio et d'utiliser une identité temporaire, le **TMSI** (*Temporary Mobile Subscriber Identity*). Ainsi, l'IMSI n'est envoyé qu'une seule fois, quand le terminal s'allume pour s'attacher au réseau. Il lui est ensuite attribué un TMSI, qui a seulement une signification locale entre le terminal et le MSC/VLR. Le TMSI est attribué par le réseau et envoyé à la **station mobile** (*MS, Mobile Station*) en mode chiffré. De plus, du fait de la signification locale du TMSI sa taille est inférieure à celle d'un IMSI, ce qui contribue à réduire la taille des messages de signalisation transmis sur le lien radio.

Chaque fois que le terminal change de **VLR**, une autre identité temporaire TMSI est attribuée. La correspondance IMSI-TMSI est gérée au niveau du VLR (figure 7.1).

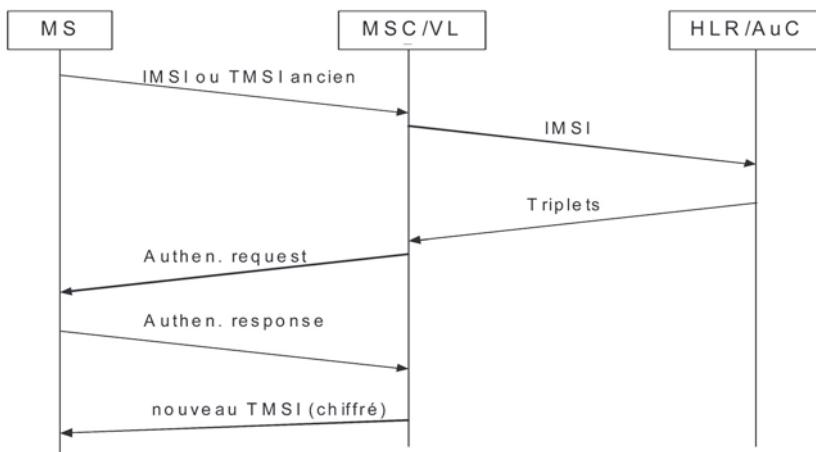


Figure 7.1 – Allocation de TMSI.

Quand la station mobile se connecte au réseau, elle envoie son IMSI au MSC/VLR.

Si la station mobile possède déjà un TMSI et change de MSC/VLR (en cas de *handover*), la valeur du TMSI est envoyée au nouveau MSC/VLR à la place de l'IMSI.

Le MSC/VLR contacte le HLR/AuC (*Home Locator Register/Authentication Center*) pour l'authentifier et obtenir une clé de chiffrement. Le MSC attribue un TMSI et le transmet à la station mobile en mode chiffré.

7.3.2 Authentification de l'identité de l'abonné

L'**authentification** de l'identité d'un abonné contribue à le prévenir d'une facturation abusive et à protéger également l'opérateur contre un usage non autorisé de ses ressources.

Le processus d'authentification est en partie basé sur une **clé secrète d'authentification** (**Ki**). Cette dernière est attribuée à la station mobile lors de la souscription de l'abonné et est stockée dans la carte SIM. Du point de vue du réseau, la clé (**Ki**) est stockée dans un centre d'authentification (AuC, *Authentication Center*) qui peut être implémenté avec le HLR. Cette clé **Ki** n'est jamais transmise sur le réseau, elle ne peut donc pas être interceptée.

Le MSC est l'entité qui authentifie directement les stations mobiles. La procédure d'authentification est la suivante (figure 7.2)⁵.

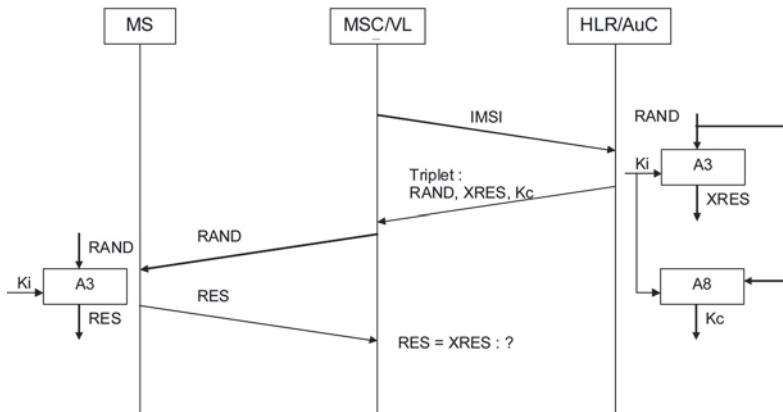


Figure 7.2 - Authentification de l'identité de l'abonné dans le réseau GSM.

Lorsqu'une station mobile a besoin d'être authentifiée, le MSC envoie l'identifiant IMSI de la station au HLR/AuC. Puis, le centre d'authentification (AuC) :

- génère un nombre aléatoire (RAND) ;
- calcule une réponse (XRES) à partir de ce nombre aléatoire (RAND), de la clé (Ki) et d'un algorithme d'authentification (A3) ;
- génère une clé de chiffrement (Kc, qui sera utilisée pour chiffrer les données à transmettre) à partir du nombre (RAND), de la clé (Ki) et d'un algorithme (A8) ;
- envoie au MSC/VLR le triplet [RAND, XRES, Kc].

À la réception du triplet, le MSC/VLR envoie le RAND comme un challenge à la station mobile.

La station mobile calcule alors à partir de ce nombre RAND reçu et de la clé Ki qu'elle possède et de l'algorithme (A3) qui est également intégré dans la carte SIM, une réponse (RES) qui est transmise au MSC/VLR.

Le MSC/VLR vérifie si la réponse (RES) reçue possède la même valeur que celle envoyée par le HLR/AuC (XRES) dans le triplet. Si oui, la station mobile est authentifiée.

5. ETSI, *Recommendation GSM 03.20*, 1992.

Transmettre un triplet d'authentification et non une clé d'authentification permet de réaliser le ***roaming*** entre opérateurs différents. En effet, les algorithmes d'authentification sont présents uniquement dans la carte SIM et dans le HLR/AuC mais pas au niveau du MSC/VLR. De ce fait, ce dernier n'a pas besoin :

- de supporter un algorithme d'authentification identique à celui de l'opérateur auprès duquel l'usager est inscrit (chaque opérateur peut avoir son propre algorithme d'authentification spécifique) ;
- de connaître la clé d'authentification (K_i).

Seule la connaissance du nombre aléatoire (RAND) et la réponse (XRES) dans le triplet suffisent pour authentifier une station selon le mode « *challenge-response* ».

7.3.3 Confidentialité des données utilisateur et de signalisation

La **confidentialité** des données de l'utilisateur, et de certaines informations de signalisation comme les numéros d'appelé et d'appelant, l'identité du terminal, l'identité de l'abonné, est réalisée par leur chiffrement à partir de la clé de chiffrement (K_c) précédemment obtenue et de l'algorithme de chiffrement (A5).

Le processus d'obtention de la clé (K_c) à partir de la clé d'authentification (K_i), du nombre aléatoire (RAND) et de l'algorithme (A8) est dénommé ***key setting*** (établissement de la clé) et peut être invoqué soit par la procédure d'authentification soit par le réseau à n'importe quel moment (figure 7.3).

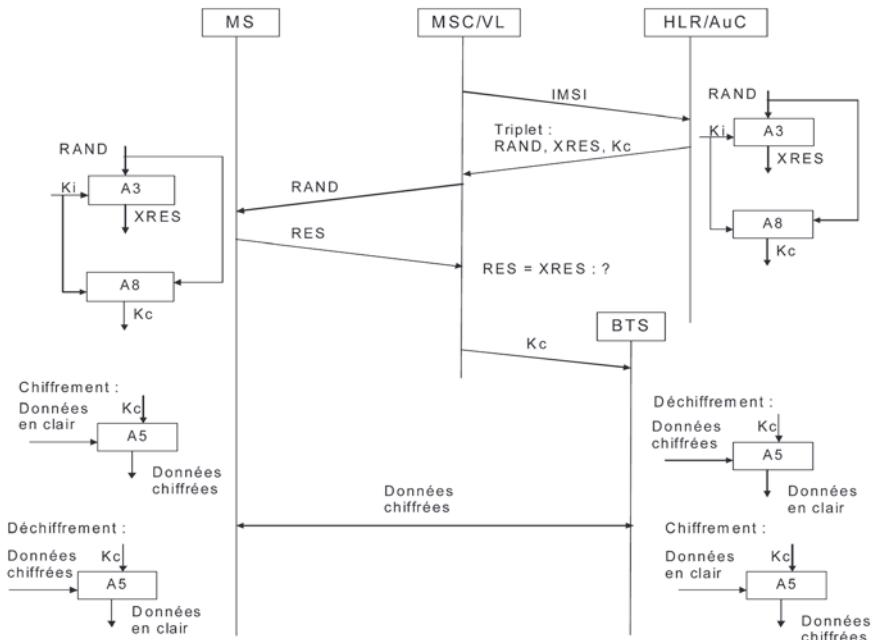


Figure 7.3 - Établissement de la clé de chiffrement et chiffrement des données dans un réseau GSM.

Une fois la station mobile authentifiée, le MSC/VLR envoie la clé de chiffrement (K_c) au BTS. Le chiffrement des **données de l'utilisateur** et des **données de signification** est réalisé par le BTS pour assurer leur confidentialité uniquement sur le lien radio. Dans la partie fixe du réseau, les données sont envoyées en clair.

7.3.4 Limites de la sécurité GSM

Bien que le réseau GSM soit considéré comme étant sécurisé (et cela uniquement sur la partie sans fil) les limitations de la sécurité GSM sont essentiellement liées aux points suivants :

- leurre des systèmes est possible ;
- le triplet d'authentification est envoyé en clair ;
- les algorithmes d'authentification et de cryptographie A3, A5, A8 sont confidentiels et non publics, et leur robustesse n'a pas été démontrée par des techniques classiques de cryptanalyse.

7.4 SÉCURITÉ DES RÉSEAUX GPRS

Les services de sécurité disponibles dans le réseau GSM comme la confidentialité de l'identité de l'abonné, l'authentification de l'abonné et la confidentialité des données sont également supportés par le réseau **GPRS**.

7.4.1 Confidentialité de l'identité de l'abonné

Comme dans le GSM, l'identité de l'abonné, l'**IMSI**, est rarement envoyé sur le lien radio. Une identité temporaire, le **P-TMSI** (*Packet-Temporary Mobile Subscriber Identity*), est utilisée⁶ pour identifier un abonné à des fins de gestion par le **GMM** (*GPRS Mobility Management*) lors les procédures d'attachement et de détachement du mobile au réseau. La correspondance IMSI-P-TMSI est gérée dans la base de données associée à chaque nœud **SGSN** (*Serving GPRS Support Node*).

Le rôle de P-TMSI est identique à celui du TMSI dans un réseau GSM. Une fois alloué, le P-TMSI est envoyé chiffré à la station mobile. Une autre identité temporaire, dérivée du P-TMSI, est utilisée dans le GPRS pour identifier un mobile particulier au niveau du lien radio (niveau LLC, *Logical Link Control*). Il s'agit du **TLLI** (*Temporary Link Layer Identity*).

7.4.2 Authentification de l'identité de l'abonné

De manière similaire au processus d'authentification du GSM, une **authentification basée sur le mode « challenge-response »** est utilisée entre le SGSN et la station mobile. L'entité qui authentifie le mobile est le **SGSN** et non le MSC (figure 7.4).

6. R. J. B. Bates, GPRS (*General Packet Radio Service*), McGraw-Hill, 2002.

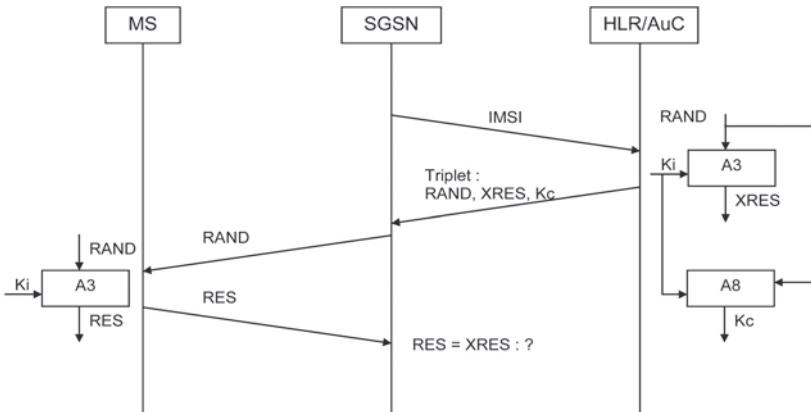


Figure 7.4 – Authentification de l’identité de l’abonné dans un réseau GPRS.

Le SGSN transmet l’IMSI de l’abonné au HLR/AuC. L’AuC génère un nombre aléatoire (RAND) qui va être utilisé comme un challenge pour la station mobile. Le nombre (RAND) et la clé d’authentification (Ki) permettent de calculer via l’algorithme (A3) la réponse (XRES). Le nombre (RAND) et la clé d’authentification (Ki) sont passés à l’algorithme (A8) pour générer la clé de chiffrement (Kc). Les trois valeurs **RAND**, **XRES**, et **Kc** forment un triplet qui est envoyé au SGSN pour valider l’authentification de la station mobile.

7.4.3 Confidentialité des données de l’utilisateur et de signalisation

La **confidentialité des données de l’utilisateur et de signalisation** est assurée par le chiffrement de données entre la station mobile et le SGSN.

L’algorithme de chiffrement est **l’algorithme GEA** (*GPRS Encryption Algorithm*) dérivé de l’algorithme A5 dont plusieurs variantes existent (GEA0, GEA1, GEA2, GEA3). La clé de chiffrement (Kc) est générée à partir de la clé d’authentification (Ki), du nombre aléatoire (RAND) et de l’algorithme (A8) (figure 7.5). Les données peuvent alors être chiffrées et transmises entre la station mobile et le SGSN (figure 7.6). Le principe du chiffrement du GPRS est identique à celui du GSM mais y est associé en plus, la direction de la trame.

L’algorithme de chiffrement du GEA prend la clé de chiffrement (Kc), une information de la trame et la direction comme entrée pour générer une séquence de bits qui est fournie avec les données en clair comme opérandes d’une opération logique de OU exclusif (XOR)⁷ pour former les données chiffrées. Pour le déchiffrement, l’algorithme prend aussi la clé de chiffrement (Kc), une information de la trame et la direction comme entrée pour générer la séquence qui avec les données chiffrées

7. Le résultat de l’opération logique OU exclusif (XOR) de l’algèbre de Boole, est vrai si l’une ou l’autre des opérantes est vraie (mais pas les deux à la fois).

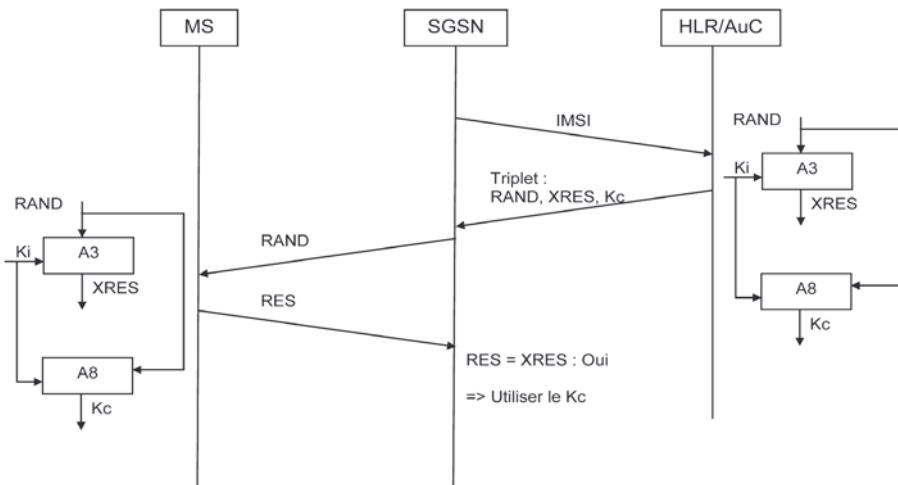
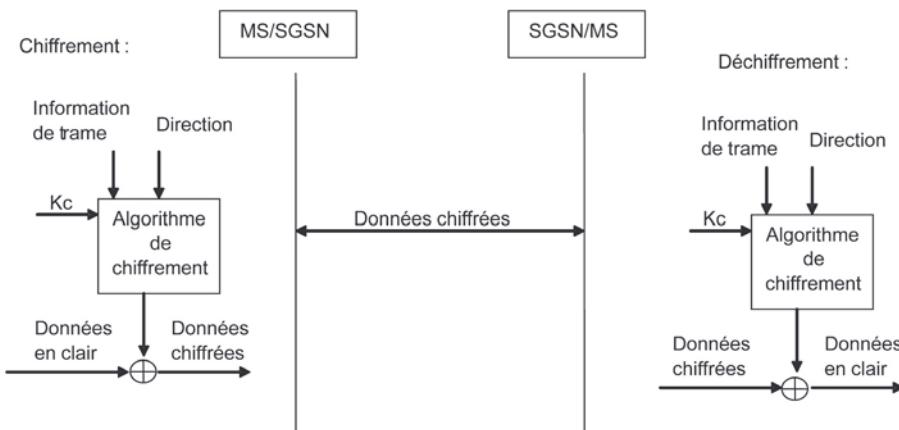
Figure 7.5 – Établissement d'une clé de chiffrement K_c .

Figure 7.6 – Chiffrement et déchiffrement de données dans un réseau GPRS.

seront les opérandes de l'opération de OU exclusif afin de restituer les données en clair. L'information de trame utilisée par l'algorithme de chiffrement dépend du type de trame. Ça peut être un numéro de trame ou une valeur établie pendant l'établissement de la connexion LLC (*Logical Link Control*).

7.4.4 Sécurité du cœur du réseau GPRS

L'opérateur d'un réseau GPRS a la responsabilité de la sécurité du « cœur » de son réseau GPRS. Il s'agit de **protéger le réseau** des écoutes illicites et de la modification des informations de l'utilisateur ou de signalisation. Pour cela, on utilise les techniques de *tunelling*, d'adressage IP privé et on met en place des systèmes pare-feu.

7.5 SÉCURITÉ DES RÉSEAUX UMTS

Les services de sécurité offerts dans un réseau **UMTS** sont⁸ :

- la confidentialité de l'identité de l'abonné ;
- l'authentification mutuelle ;
- la confidentialité et l'intégrité des données utilisateurs et de la signalisation.

7.5.1 Confidentialité de l'identité de l'abonné

Une identité temporaire **P-TMSI** est attribuée à l'utilisateur pour limiter l'échange de l'identité IMSI. L'allocation d'un P-TMSI est faite par le **3G-SGSN** (*Third Generation (UMTS) -Serving GPRS Support Node*) comme le montre la figure 7.7.

Le centre 3G-SGSN, à la réception d'un IMSI (ou d'un ancien P-TMSI) envoyé par la station mobile, contacte le HLR/AuC pour obtenir des vecteurs d'authentification. Si l'authentification se termine avec succès, une valeur P-TMSI est attribuée et envoyée chiffrée au mobile. La correspondance P-TMSI-IMSI est maintenue au niveau du 3G-SGSN.

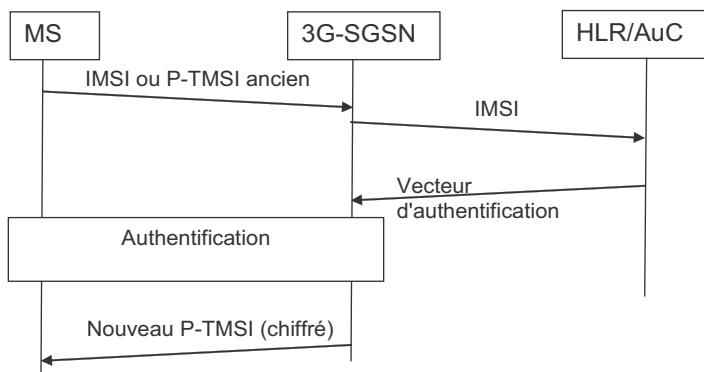


Figure 7.7 – Allocation de P-TMSI.

7.5.2 Authentification mutuelle

Une **authentification mutuelle** entre l'abonné et le réseau est possible dans un réseau UMTS. D'une part, l'authentification de l'abonné permet au réseau de vérifier si le mobile est autorisé à utiliser ses ressources. D'autre part, l'authentification de réseau offre à l'abonné la possibilité de vérifier s'il est servi par un réseau autorisé par le réseau de son opérateur et de valider s'il est connecté à une entité « réseau » légale.

8. 3GPP, *TS 33.102 3G Security : Security architecture (Release 6)*, 2004.

La procédure d'authentification est présentée par la figure 7.8. Elle se base sur une **clé d'authentification** (K) de 128 bits qui réside dans la carte SIM (USIM, *Universal SIM*) et dans l'AuC. Cette clé n'est jamais transmise.

Le 3G-SGSN envoie tout d'abord l'identité de l'abonné, son IMSI au HLR/AuC. L'AuC génère un nombre aléatoire (RAND, *random*) qui sera utilisé comme « *challenge* » pour le mobile. Le nombre (RAND) et la clé d'authentification (K) servent d'entrées à l'algorithme (f2) pour obtenir la réponse (XRES).

L'AuC construit la **clé de chiffrement** (CK) utilisée ultérieurement pour assurer la confidentialité de données et la **clé d'intégrité** (IK) pour vérifier l'intégrité des données de signalisation en utilisant respectivement les algorithmes (f3) et (f4).

Pour l'authentification de réseau, l'AuC utilise deux algorithmes (f5) et (f1) pour construire l'**AUTN** (*Authentication Number*). L'*authentication number* est constituée à partir :

- du nombre (RAND) ;
- de la clé d'authentification (K) ;
- d'un numéro de séquence (SQN, *Sequence Number* [une valeur maintenue par l'AuC et le mobile]) ;
- du champ AMF (*Authentication Management Field*) ;
- d'un champ qui peut être utilisé pour indiquer l'algorithme d'authentification au cas où plusieurs algorithmes sont supportés.

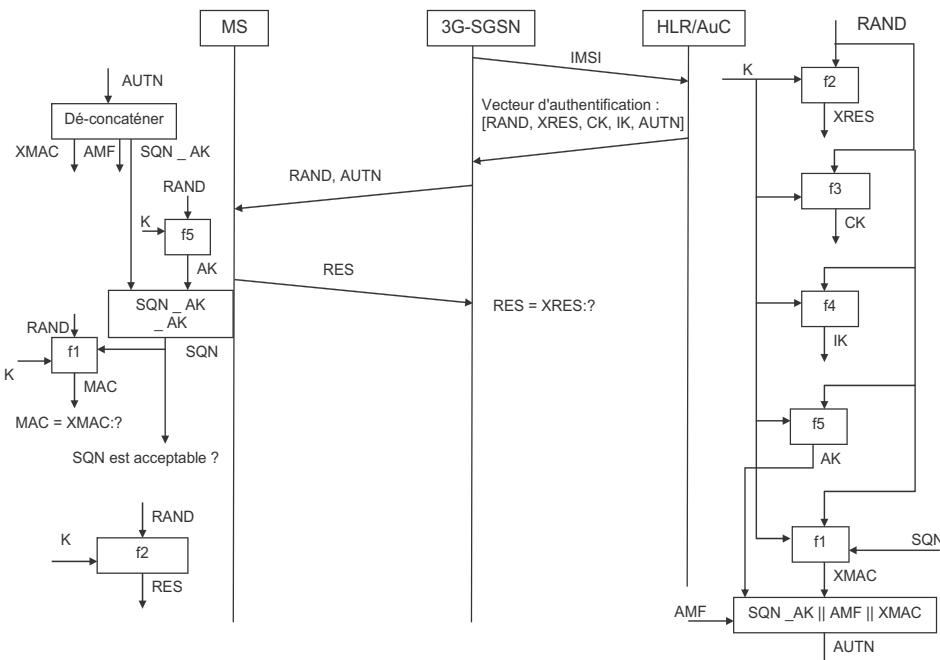


Figure 7.8 - Authentification mutuelle dans un réseau UMTS.

Les cinq valeurs [RAND, XRES, CK, IK, et AUTN] forment le **vecteur d'authentification** qui est envoyé au 3G-SGSN pour réaliser l'authentification mutuelle entre le 3G-SGSN et la station mobile.

À la réception du vecteur d'authentification, le 3G-SGSN envoie au mobile le nombre (RAND) pour l'**authentification de l'abonné** et l'AUTN pour l'**authentification de réseau**. Le mobile vérifie d'abord si la valeur de l'AUTN est dans la plage de valeurs qu'il attend. Si oui, le 3G-SGSN est authentifié. C'est-à-dire qu'il est autorisé par l'AuC à servir le mobile. Dans ce cas, le mobile utilise le nombre (RAND) et la clé d'authentification (K) pour générer la réponse (RES) en utilisant l'algorithme (f2).

La réponse (RES) est envoyée au 3G-SGSN pour l'authentification de l'abonné. Si la réponse RES reçue du mobile et la valeur XRES dans le vecteur d'authentification sont identiques, l'abonné est authentifié.

Dans le cas où l'AUTN ne tombe pas dans la plage de valeurs attendues par le mobile, ce dernier arrête l'authentification et envoie une notification à l'AuC.

Pour permettre au mobile d'authentifier le réseau, l'AUTN est basé sur une valeur de **numéro de séquence** (SQN) qui est synchronisée entre l'USIM (*Universal SIM*) et l'AuC. Un algorithme est utilisé pour assurer que la valeur (SQN) est augmentée pour chaque authentification. L'USIM peut vérifier que la valeur de SQN reçue n'est pas encore apparue et qu'elle tombe dans la plage de valeurs prévues (elle est récente).

Le mécanisme de génération de la valeur (SQN) est **spécifique à l'opérateur**. Le mécanisme le plus simple est d'avoir un numéro de séquence (SQN) individuel pour chaque abonné et de l'incrémenter de 1 pour chaque authentification. Un autre mécanisme est de générer le SQN en se basant sur un compteur global (par exemple, basé sur le temps). Une autre manière de procéder est de générer le numéro de séquence (SQN) avec une partie statique, qui est individuelle pour chaque abonné, et une partie dynamique, qui est basée sur un compteur global.

Pour protéger la valeur (SQN) lors de sa transmission le long du chemin de l'AuC vers le mobile, deux fonctions (f5) et (f1) sont utilisées. La fonction (f5) prend le nombre (RAND) et la clé (K) pour générer la valeur (AK) (*Anonymity Key*) qui est utilisée pour masquer la valeur SQN lors de la transmission. La valeur (AK) et la valeur SQN sont les opérandes d'une opération logique de OU exclusif (XOR) dont le résultat est transmis au mobile via la valeur AUTN. Cela assure que seul le mobile qui possède la clé (K) peut extraire la valeur SQN de l'AUTN.

La fonction (f1) prend le RAND, le SQN et la clé (K) pour calculer un MAC (*Message Authentication Code*) noté (XMAC). Cette valeur XMAC assure à l'USIM que l'entité qui génère la valeur SQN est celle qui a la clé (K), i.e. l'AuC.

La valeur SQN masquée (opération XOR avec la clé AK), le XMAC et un champ administratif (AMF) sont concaténés pour former l'AUTN qui est envoyé au mobile.

À la réception du numéro d'authentification (l'AUTN), le mobile utilise le nombre aléatoire (RAND) et la clé (K) comme entrées pour l'algorithme (f5) afin d'obtenir la clé anonyme (AK) qui est ensuite utilisé pour extraire le numéro de séquence (SQN).

Les valeurs SQN, RAND et la clé (K) sont utilisées pour calculer le code d'authentification du message (le MAC) avec l'algorithme (f1).

Le MAC est alors comparé avec le XMAC reçu via l'AUTN pour vérifier si la valeur SQN est bien générée par l'AuC. Si le résultat est identique, MAC = XMAX, le mobile vérifie si la valeur SQN est dans sa plage de valeurs pour assurer qu'elle est récente. Si la valeur SQN est acceptable, le réseau est authentifié.

7.5.3 Confidentialité des données utilisateurs et de signalisation

Une fois que le mobile et le réseau se sont authentifiés, les communications peuvent être sécurisées par le **chiffrement des données des utilisateurs et de signalisation**. La clé de chiffrement (CK) est calculée par l'algorithme (f3) à partir de la clé d'authentification (K) et du nombre (RAND). La figure 7.9 présente les mécanismes d'obtention de la clé de chiffrement (CK), les processus de chiffrement et de déchiffrement dans un réseau UMTS. L'UMTS utilise la technique de **chiffrement par flot (stream cipher)**.

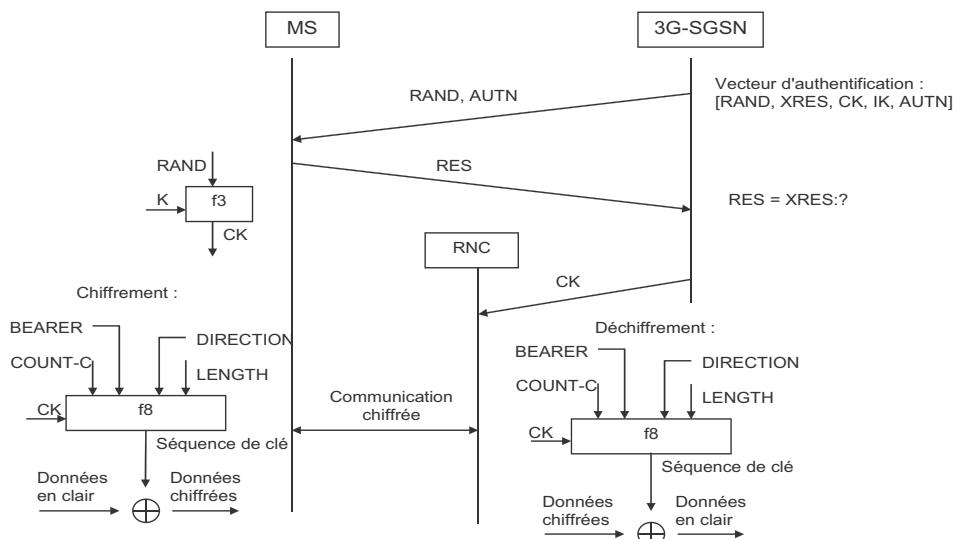


Figure 7.9 – Obtention de la clé de chiffrement et chiffrement de données dans l'UMTS.

Le chiffrement et le déchiffrement sont réalisés entre le mobile et le **RNC** (*Radio Network Controller*). La clé (CK) est envoyée du 3G-SGSN (3^e génération du *Serving GPRS Support Node*) vers le RNC.

L'algorithme (f8) prend la clé (CK), une valeur de compteur (COUNT-C), le numéro du canal logique de transport (ou *bearer*), la direction de la transmission (*uplink/downlink*), et la longueur du bloc de la séquence de la clé générée comme des entrées pour générer une séquence de clé. Cette séquence de clé est utilisée pour

effectuer une opération de OU exclusif (XOR) bit par bit avec les données en clair pour constituer les données chiffrées.

Pour le déchiffrement, les mêmes entrées sont utilisées par l'algorithme (f8) pour générer la même séquence de clé. Cette séquence de clé et les données chiffrées sont des opérandes de l'opération logique de OU exclusif afin de restituer les données en clair.

L'avantage de ce mécanisme est que les séquences de clé peuvent être calculées en avance, et dès que les données arrivent seule l'opération XOR est effectuée. Ceci permet d'augmenter la rapidité du traitement car il n'est pas nécessaire d'attendre que les données soient reçues pour effectuer une partie du déchiffrement car les paramètres d'entrée sont connus et peuvent être prétraités.

Cependant, comme la séquence de clé est indépendante des données à chiffrer, les paramètres d'entrée de l'algorithme (f8) doivent être différents pour chaque génération de séquence de clé. En effet, le paramètre **COUNT-C** est un compteur très grand qui assure que la valeur utilisée n'est pas réinitialisée pendant la durée d'utilisation d'une clé (CK) jusqu'à l'authentification suivante. L'authentification sera aussi suffisamment fréquente pour changer la valeur de clé de chiffrement (CK). Comme chaque *bearer* maintient un compteur indépendant, l'identité du *bearer* est utilisée comme paramètre d'entrée pour éviter la répétition des valeurs COUNT-C appartenant à différents *bearers*. Le paramètre *Direction* indique la voie montante ou descendante. Le paramètre *Length* indique la longueur des données à chiffrer avec la séquence de clé générée.

7.5.4 Intégrité des données de signalisation

Les procédures d'authentification assurent l'identité des entités seulement durant le temps de l'authentification. Un attaquant peut capter les messages et les délivrer jusqu'à ce que l'authentification soit terminée. Ensuite, il peut manipuler les messages pour contrôler les ressources radio. Pour contrer cette attaque de type *man in the middle*, l'UMTS utilise un service d'intégrité pour authentifier chaque message de contrôle de ressources radio (RRC, *Radio Resource Control*). Comme les messages sont protégés individuellement, les faux messages de contrôle peuvent être détectés et éliminés.

La clé d'intégrité (IK) est dérivée par l'algorithme (f4) à partir d'un nombre aléatoire (RAND) et de la clé d'authentification (K) pendant la procédure d'authentification. La figure 7.10 schématisé la dérivation de la clé (IK) ainsi que la fonction d'intégrité.

La protection de l'intégrité est basée sur le calcul d'un **MAC-I** (*Message Authentication Code – Integrity*). L'algorithme d'intégrité (f9) est une fonction à sens unique. Il prend la clé (IK), le contenu du message RRC (*Radio Ressources Control*), un compteur d'intégrité (COUNT-I), la direction et une valeur aléatoire nouvelle (FRESH) produite par le RNC afin de générer un MAC-I de 32 bits. Le MAC-I est envoyé au récepteur avec le message RRC. À la réception, un MAC-I' est calculé selon la même procédure et est comparé avec le MAC-I reçu.

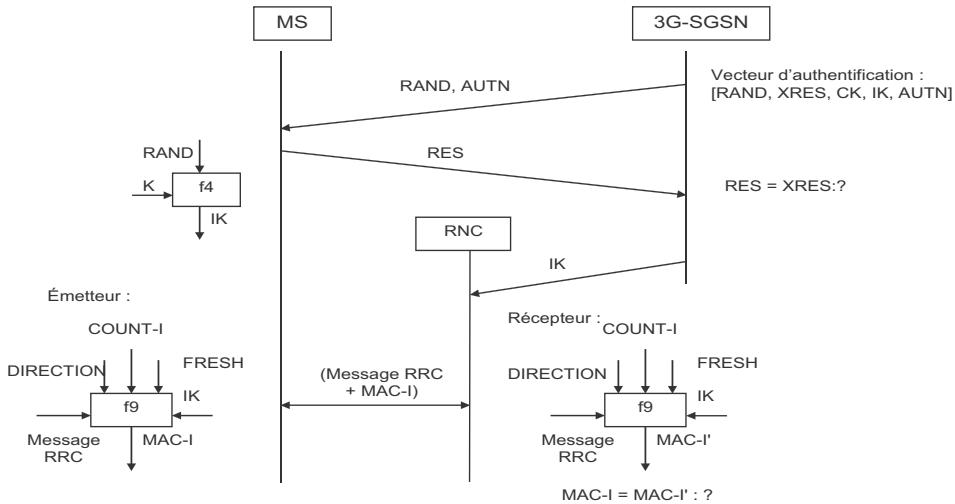


Figure 7.10 – Clé d'intégrité et protection d'intégrité dans l'UMTS.

Afin d'éviter les **attaques de type rejet** (*replay attacks*), les paramètres d'entrée de l'algorithme (f9) assurent que les entrées sont suffisamment différentes pour chaque calcul de MAC. À côté du compteur COUNT-I, qui joue un rôle similaire à celui du compteur COUNT-C dans le chiffrement, un nombre FRESH est généré par le RNC et envoyé au mobile au moment de l'établissement d'une connexion RRC en utilisant le **mode de commande sécurisé** (*secure command mode*). S'il n'y a pas cette valeur, un attaquant peut leurrer le réseau en se faisant passer pour un abonné (*mascarade*) et envoyer une fausse valeur COUNT-I initiale au réseau. Ce fait peut influencer le choix de valeur COUNT-I initiale qui peut être faible et l'attaquant aura ainsi plus de facilité pour faire des attaques de type rejet.

7.6 RÉSEAUX LOCAUX SANS FIL 802.11

7.6.1 Principes de base

Les **réseaux locaux sans fil de type 802.11** sont utilisés dans les entreprises ou dans des lieux publics pour la réalisation de points d'accès à Internet (points d'accès « **hot spots** », dans des gares aéroports, hôtels, cafés, salles de conférences, etc.). Le nom commercial de Wi-Fi (*Wireless Fidelity*) désigne à la fois les équipements qui intègrent une carte réseau permettant un accès sans fil à Internet et le mode de transmission des données. Le Wi-Fi utilise une bande de fréquence étroite, entre 2,41 et 2,484 GHz, dite « industrielle, scientifique et médicale » (ISM).

Les **stations mobiles**, les **points d'accès** et le **système de distribution** sont les éléments constitutifs d'un réseau local sans fil en mode infrastructure. Les stations mobiles envoient et reçoivent des données via des points d'accès par le lien radio.

Différents points d'accès sont reliés par le système de distribution, permettant aux stations mobiles attachées à différents points d'accès de communiquer. Outre le mode infrastructure, la norme 802.11 autorise également des **réseaux dits *ad hoc*** dans lesquels les stations mobiles communiquent directement entre elles sans passer par des points d'accès et un système de distribution.

Comme dans les réseaux cellulaires, le lien radio présente un point critique pour la sécurité du réseau. Afin de protéger les informations envoyées sur le lien radio contre les écoutes illégales et de protéger le réseau contre les utilisations de ressources radio par les personnes non autorisées, les normes 802.11 et 802.11i définissent des mécanismes pour réaliser l'authentification et la confidentialité.

7.6.2 Sécurité 802.11

La **norme 802.11⁹** définit deux services de sécurité pour les réseaux locaux sans fil qui permettent d'assurer l'authentification et la confidentialité des données de l'utilisateur.

L'utilisateur est authentifié afin de lui permettre d'accéder ou non au réseau. Comme il s'agit d'une authentification au niveau liaison, seuls deux équipements directement reliés par un lien physique peuvent s'authentifier.

Dans un réseau sans fil en **mode infrastructure**, une station mobile s'authentifie auprès d'un point d'accès. Lorsqu'il s'agit d'un réseau 802.11 **en mode *ad hoc***, deux stations mobiles directement reliées par le lien radio peuvent s'authentifier.

L'authentification de bout en bout ou d'utilisateur à utilisateur n'est pas proposée dans la norme 802.11. Pour cela, des mécanismes d'authentification additionnels doivent alors être implantés.

Un **algorithme de chiffrement, WEP** (*Wired Equivalent Privacy*), est utilisé pour chiffrer les données avant qu'elles soient envoyées sur le lien radio.

Authentification

Deux types d'authentification sont définis : l'authentification dans un système ouvert et l'authentification à clé partagée.

L'**authentification dans un système ouvert** permet à un équipement (un point d'accès dans le mode infrastructure ou une station mobile dans le mode *ad hoc*) d'accepter tous les utilisateurs dans sa zone de couverture. Ce type d'authentification de système ouvert est souvent utilisé pour donner gratuitement accès à Internet dans certaines zones géographiques. Tout portable équipé d'une carte 802.11 peut alors accéder à Internet. La figure 7.11 présente l'authentification entre une station mobile et un point d'accès.

L'**authentification dite à clé partagée** se base sur une clé secrète possédée par la station mobile et le point d'accès, et sur un algorithme de chiffrement symétrique, selon un mode « *challenge-response* » (figure 7.12).

9. Norme IEEE 802.11 (ISO/IEC 8802-11).

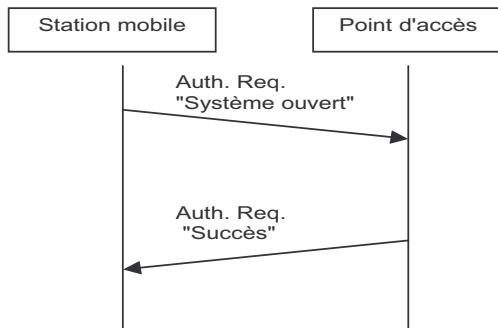


Figure 7.11 - Authentification dans un système ouvert.

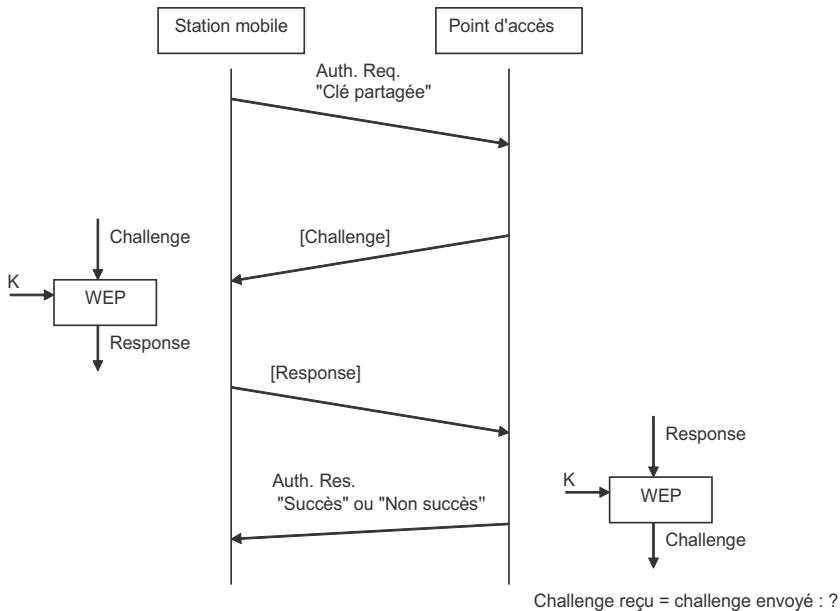


Figure 7.12 - Authentification à la clé partagée entre une station mobile et un point d'accès.

Quand le point d'accès reçoit une requête d'authentification, il envoie un *challenge* à la station mobile. L'utilisateur chiffre le *challenge* avec l'algorithme de chiffrement symétrique WEP et sa clé secrète puis transmet le résultat (la réponse – *response*) au point d'accès. Le point d'accès déchiffre la réponse à l'aide de la même clé secrète et du même algorithme et compare la valeur obtenue (*challenge* reçu) avec celle du *challenge* envoyé. Si les deux valeurs sont identiques, l'utilisateur est authentifié.

Confidentialité

L'**algorithme WEP** permet de chiffrer les données à transmettre sur le lien radio dans un réseau 802.11 (figure 7.13). Il est basé sur l'algorithme de chiffrement symétrique (RC4) à clé secrète, dont l'abandon est recommandé depuis 2015 du fait de sa faiblesse.

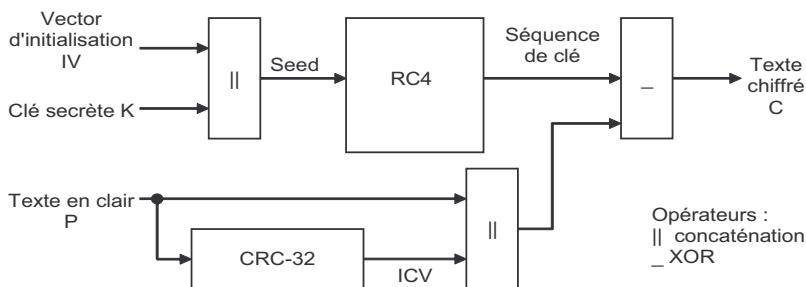


Figure 7.13 - Procédure de chiffrement WEP.

Les éléments à l'entrée du processus de chiffrement sont le **vecteur d'initialisation** (IV, *Initialization Vector*), la **clé secrète partagée** (K), et le **texte en clair** (P) à chiffrer.

Le vecteur d'initialisation de 24 bits est concaténé avec la clé secrète de 40 bits pour former une sous-clé ou *seed* de 64 bits. Ce *seed* est utilisé par l'algorithme RC4 pour générer une séquence de clé. De plus, afin d'assurer l'intégrité du texte en clair, une **valeur d'intégrité ICV** (*Integrity Check Value*) de 32 bits est calculée sur le texte en clair (P) en utilisant l'algorithme CRC-32. La valeur de l'ICV est concaténée au texte en clair et constitue avec la séquence de clé obtenue, les opérandes de l'opération logique OU exclusif (XOR) pour obtenir le texte chiffré (C) qui est envoyé au récepteur. Le vecteur d'initialisation (IV) est transmis en clair avec le message dans son en-tête pour que le destinataire puisse l'utiliser lors du déchiffrement (figure 7.14).

Le récepteur calcule la valeur d'intégrité du texte en clair reçu (ICV') et le compare à l'ICV reçu. Si les deux valeurs sont équivalentes, le texte sera considéré comme ayant été non modifié.

7.6.3 Renforcer la sécurité (norme 802.11i)

La norme 802.11 comporte plusieurs points faibles concernant la sécurité. En effet, l'algorithme WEP notamment n'est pas robuste. Pour renforcer la sécurité des réseaux 802.11, la **norme 802.11i**¹⁰ a introduit les concepts de **RSN** (*Robust Security Network*) et d'association de sécurité **RSNA** (*Robust Security Network Association*) ainsi que deux nouveaux algorithmes de chiffrement **TKIP** (*Temporal Key*

10. ANSI/IEEE, Standard 802.11i, 2004.

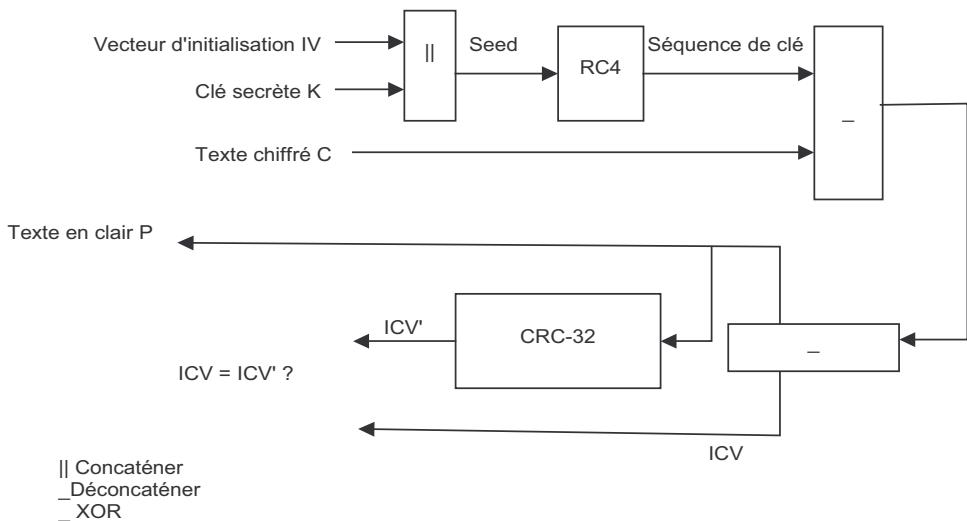


Figure 7.14 - Procédure de déchiffrement WEP.

Integrity Protocol) et **CCMP** (*Counter with CBC-MAC Protocol*). Cette nouvelle version est le plus souvent connue sous l'appellation **WPA** (*Wi-Fi Protected Access* – version 2 WPA2).

Trois services de sécurité sont proposés par la norme 802.11i : le contrôle d'accès *via* le port 802.1X, l'authentification et la confidentialité des données.

Association de sécurité

Un **réseau sans fil** qualifié de **robuste** (RSN, *Robust Security Network*) est défini comme un réseau dans lequel les stations communiquent d'une manière sécurisée au travers d'associations de sécurité dénommées **RSNA** (*Robust Security Network Association*). Une association RSNA est basée sur l'architecture **IEEE 802.1X** (figure 7.15).

Chaque station utilise un port 802.1X pour la transmission des données. Ce concept de port défini dans la norme IEEE 802.1X est utilisé pour fournir le contrôle d'accès dans 802.11i. Le port 802.1X est plus précisément un **IEEE 802.1X PAE** (*Port Access Entity*). Dans un réseau 802.11 en mode infrastructure, le PAE implanté dans une station mobile est de type *supplicant* tandis que le point d'accès supporte un PAE de type *authenticator*¹¹.

La communication entre les deux ports *supplicant* et *authenticator* se réalise *via* le **protocole EAP** (*Extensible Authentication Protocol*)¹².

11. IEEE, *Standard 802.1X*, 2004.

12. B. Aboba, L. Blunk, J. Vollbrecht, J. Carlson, and H. Levkowetz, *Extensible Authentication Protocol (EAP)*, RFC 3748, June 2004.

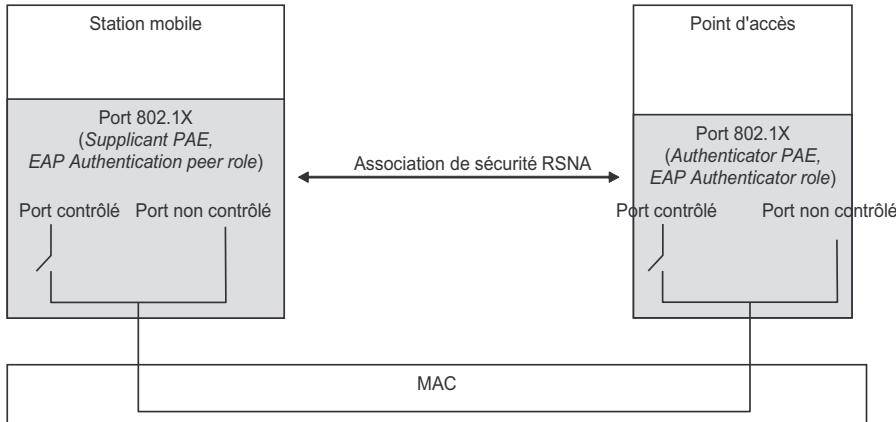


Figure 7.15 – Association de sécurité RSNA pour la mise en œuvre du contrôle d'accès.

Chaque port 802.1X se compose d'un port contrôlé et d'un port non contrôlé. Le port non contrôlé est utilisé pour passer les données d'authentification et le port contrôlé est utilisé pour passer d'autres types de trafic. Le port contrôlé est bloqué jusqu'à ce que la procédure d'authentification via le port non contrôlé soit complétée.

Une association de sécurité RSNA est établie entre deux ports 802.1X de deux entités du réseau. La figure 7.16 présente une association de sécurité entre un port 802.1X d'une station mobile et un port 802.1X d'un point d'accès. En fait, quatre types d'association de sécurité existent :

- **L'association PMKSA (Pairwise Master Key Security Association)** est une association de sécurité établie entre un *supplicant* et un *authenticator* (entre une station mobile et un point d'accès) qui supporte la clé primaire PMK (*Pairwise Master Key*) et d'autres informations comme la durée d'utilisation de la clé primaire, l'adresse MAC de l'*authenticator*, le protocole d'authentification et de gestion de clé, etc. La clé primaire est utilisée pour dériver les clés temporaires utilisées pour le chiffrement des données.
- **L'association PTKSA (Pairwise Transient Key Security Association)** est une association de sécurité établie entre un *supplicant* et un *authenticator* qui contient la clé temporaire PTK (*Pairwise Transient Key*) et d'autres informations comme l'algorithme de chiffrement des données. Ce type d'association est utilisé pour sécuriser les trafics *unicast* entre le *supplicant* et l'*authenticator*.
- **L'association GTKSA (Group Temporal Key Security Association)** est une association de sécurité établie entre les membres d'un groupe de stations. Dans un réseau 802.11 en mode infrastructure, une GTKSA est établie entre un point d'accès et des stations mobiles et supporte la clé temporaire GTK (*Group Temporal Key*) et d'autres informations nécessaires pour le chiffrement des trafics *broadcast* ou *multicast* envoyés du point d'accès vers les stations mobiles. Dans

un réseau 802.11 en mode *ad hoc*, chaque station établit une GTKSA avec chaque voisin pour pouvoir chiffrer les trafics *broadcast* ou *multicast*.

- **L'association STAKeySA** (*Station Key Security Association*) est une association de sécurité établie entre deux stations mobiles qui sont associées à un même point d'accès. Une STAKeySA contient un STAKey (*Station Key*) permettant le chiffrement de données directement envoyées entre ces deux stations.

Authentification

L'authentification de type système ouvert est utilisée pour les réseaux ouverts au public et pour l'établissement d'une association de sécurité RSNA afin de pouvoir associer une station mobile à un point d'accès et négocier les mécanismes d'authentification et de gestion de clé.

Deux autres types d'authentification sont également possibles : l'authentification 802.1X et l'authentification à clé secrète partagée.

Dans **l'authentification 802.1X**, un serveur d'authentification est utilisé. Le lien entre le serveur d'authentification et l'*authenticator* est supposé sécurisé. L'authentification 802.1X est basée sur le protocole EAP (*Extensible Authentication Protocol*). La procédure d'authentification 802.1X est illustrée par la figure 7.16.

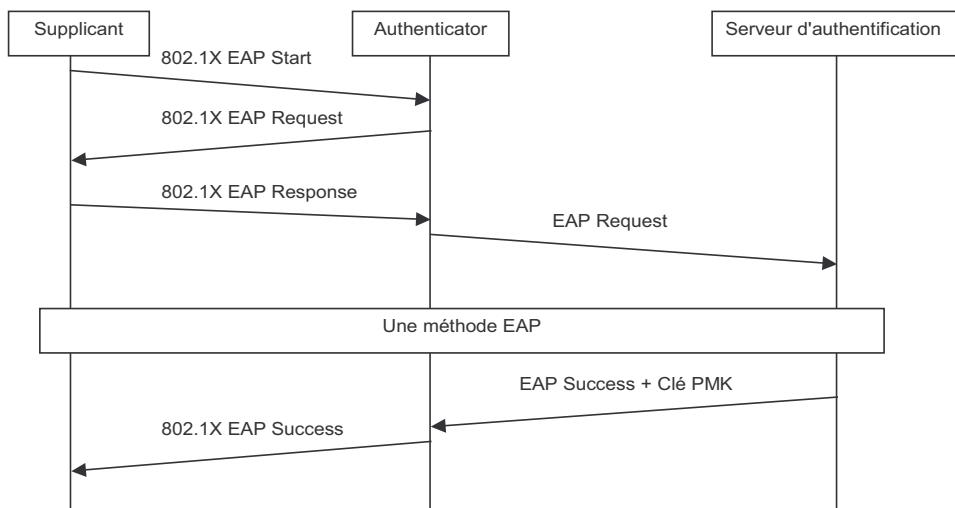


Figure 7.16 - Authentification 802.1 X.

Le fait que l'authentification soit mutuelle ou non dépend de la méthode EAP utilisée. La méthode EAP-TLS permet une authentification mutuelle tandis que l'EAP MD5-CHALLENGE ne permet que l'authentification du *supplicant* auprès du réseau.

Dans l'**authentification à clé partagée**, il n'y a pas de serveur d'authentification. Une clé d'authentification est configurée dans la station mobile et le point d'accès. Un mécanisme de mot de passe associé à une fonction *hash* peut être utilisé pour générer la clé (l'utilisateur doit se souvenir uniquement du mot de passe).

Confidentialité

Le standard 802.11i introduit deux nouveaux protocoles pour le chiffrement des données, les **protocoles TKIP** (*Temporal Key Integrity Protocol*) et **CCMP** (*Counter with CBC-MAC Protocol*).

• *Le protocole TKIP*

Le **protocole TKIP** (*Temporal Key Integrity Protocol*) est une amélioration de l'algorithme WEP. Les équipements supportant le WEP nécessitent une mise à jour logicielle pour supporter le protocole TKIP. Ce dernier est considéré comme une solution temporaire pour la transition vers le protocole CCMP.

TKIP est basé, comme le WEP, sur l'algorithme RC4. Les améliorations portent :

- sur l'utilisation d'un numéro de séquence TSC (*TKIP Sequence Counter*) associé à chaque MPDU (*MAC Protocol Data Unit*) afin de pallier les attaques de type rejet ;
- sur la vérification de l'intégrité au niveau des unités de données MSDU (*MAC Service Data Unit*) via un paramètre MIC (*Message Integrity Code*) ;
- sur des clés composées.

L'intégrité d'une unité de données (MSDU) est protégée par une **valeur MIC** calculée sur les adresses destination et source, la priorité du MSDU, et les données en clair. Ce MIC est ajouté aux données en clair.

• *Le protocole CCMP*

Le **protocole CCMP** (*Counter with CBC-MAC Protocol*) est basé sur l'algorithme de chiffrement AES (*Advanced Encryption Standard*) en mode CCM (*Counter with CBC-MAC*)¹³ (figure 7.17).

Le chiffrement en mode CCM de l'algorithme AES a besoin de quatre entrées : un **AAD** (*Additional Authenticated Data*), un **Nonce** (une valeur unique), des **données en clair** et la **clé de chiffrement** pour chiffrer les données et calculer le MIC (*Message Integrity Code*).

L'AAD est utilisé pour authentifier l'en-tête MAC d'un MPDU.

Le *Nonce* est une valeur qui doit être unique pour chaque chiffrement utilisant la même clé. Pour construire le *Nonce*, le protocole CCMP concatène la priorité de la trame, le champ d'adresse A2 du MPDU, et le numéro de paquet (PN, *Packet Number*). Le numéro de paquet (PN) est un numéro géré par CCMP, incrémenté

13. D. Whiting, R. Housley and N. Ferguson, *Counter with CBC-MAC (CCM)*, RFC 3610, September 2003.

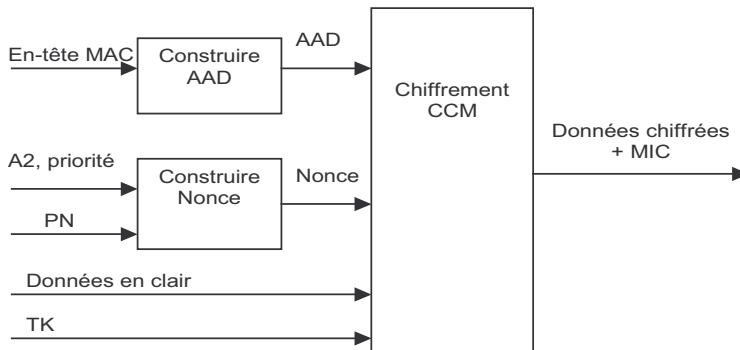


Figure 7.17 - Chiffrement CCMP.

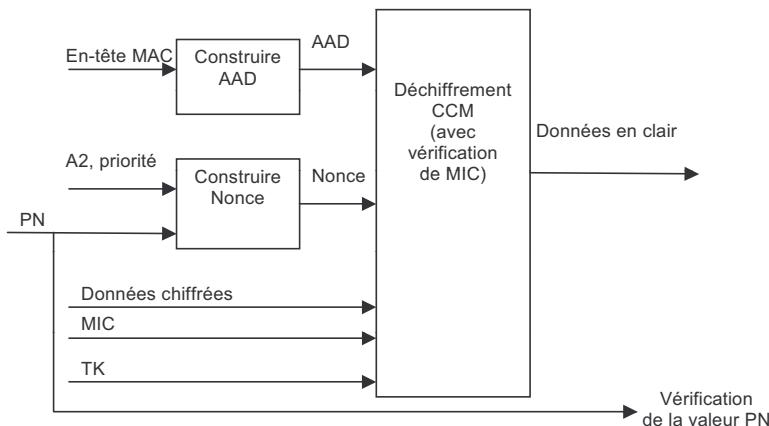


Figure 7.18 - Déchiffrement CCMP.

pour chaque MPDU afin de fournir une valeur de *Nonce* unique pour chaque chiffrement utilisant la même clé (TK) (*Temporal Key*). La clé de chiffrement (TK) est dérivée de la clé (PTK) obtenue au cours de la procédure d'authentification. La procédure de déchiffrement CCMP est illustrée dans la figure 7.18.

Le récepteur reproduit la donnée AAD à partir de l'en-tête MAC du MPDU reçu. Le *Nonce* est reconstruit à partir des valeurs A2, Priorité et (PN) dans le MPDU reçu. Une vérification de la valeur (PN) permet de détecter des attaques de type rejet. Le récepteur maintient un compteur qui est réinitialisé pour chaque changement de clé (TK) et est mis à jour avec la valeur (PN) du dernier MPDU accepté. Comme la valeur (PN) est incrémentée pour chaque chiffrement d'un MPDU, une valeur de (PN) reçue égale ou inférieure à la valeur du compteur concerne une attaque de type rejet. Les données chiffrées et leur MIC sont déchiffrés pour obtenir les données en clair et vérifier l'intégrité des données et l'intégrité de l'AAD.

7.7 RÉSEAUX PERSONNELS SANS FIL

Les réseaux personnels sans fil (**WPAN**, *Wireless Personal Area Network*) permettent de relier, *via* des ondes hertziennes (bande de fréquences 2,4 GHz)¹⁴, des équipements (souris, clavier, imprimantes, oreillettes, téléphone portable, PDA (*Personal Digital Assistant*), appareil photo, équipement GPS (*Global Positionning System*), etc. et des systèmes sur une distance faible comprise entre une dizaine de mètres et au maximum cent mètres. La distance est directement liée à la puissance d'émission et à la sensibilité de réception des équipements.

La technologie Bluetooth, permettant l'interopérabilité d'équipements différents, initialement conçue par Ericson en 1994, doit son nom à un roi viking, Harald II, père de l'unification des pays scandinaves ayant vécu vers le milieu du X^e siècle, surnommé « la dent bleue » du fait de son goût pour les myrtilles. Cette technologie a été ensuite normalisée par le groupe d'intérêt spécial *Bluetooth Special Interest Group* (SIG), qui compte plusieurs milliers de membres dont Ericsson, IBM, Intel, Microsoft, Motorola, Nokia, ou Toshiba. La série des normes 802.15.x de l'IEEE, qui spécifient des débits variant de 1 à 20 Mbits/sec, sont équivalentes.

Les équipements Bluetooth peuvent être classés selon trois niveaux de sécurité. Le niveau 1 indique qu'aucun service de sécurité n'est intégré, l'équipement n'est pas protégé et accepte toutes les connexions tandis que les niveaux 2 et 3 offrent des services de sécurité respectivement au niveau applicatif et au niveau de la liaison de données (connexion avec authentification et chiffrement au moyen d'une clé).

Comme toute technologie, celle-ci peut faire l'objet de détournement et d'**attaques passives et actives** qui exploitent les failles matérielles et logicielles des équipements Bluetooth et les vulnérabilités humaines.

Ainsi par exemple, des dénis de services, du spam, des virus, des intrusions, des écoutes, la prise de contrôle à distance des équipements, des vols ou des modifications de données dans des téléphones portables, oreillettes, agendas électroniques, ordinateurs, etc., le détournement de session, les leurre, le cassage de code PIN, peuvent exister. Des équipements compromis par un programme (logiciel espion) et commandés à distance à l'insu de leurs propriétaires peuvent être bloqués, les données peuvent être copiées, modifiées, détruites, ou des nouvelles données (photos, sms, carnet d'adresses, etc.) peuvent aussi être introduites et des écoutes environnementales sont par ailleurs possibles.

Outre des atteintes à la confidentialité de ses données, l'utilisateur peut également voir sa facture de téléphonie exploser et devoir supporter les coûts induits par un **usage abusif** et non autorisé de son équipement Bluetooth.

Le détournement de trafic fait partie des attaques courantes dans la mesure où il est possible de désactiver le signal d'un point d'accès pour le neutraliser (*via* un déni de service) ou d'en émettre un plus puissant (*via* une antenne de plus forte puissance) afin que l'attaquant se substitue au point d'accès légitime (attaque du type « *Man in the middle* ») et détourne à son profit tous les trafics.

14. Norme IEEE 802.16, nom commercial **WiMax**.

Bien que la sécurité des équipements Bluetooth ait été progressivement renforcée, certains restent toutefois très vulnérables. Parmi les principales raisons retenons les suivantes : implémentations défaillantes, existence de **portes dérobées** (*backdoors*), protocole Bluetooth toujours activé (même si cela n'est pas nécessaire), valeur des codes PIN toujours par défaut (0000 ou 1234), acceptations inconsidérées des demandes de connexion, etc.

Résumé

Ce chapitre a présenté les services et les techniques de sécurité supportés dans les réseaux cellulaires GSM, GPRS et UMTS (WWAN, *Wireless Wide Area Network*) et dans les réseaux locaux sans fil 802.11 (WLAN, *Wireless Local Area Network*). Le principe de la sécurité de ces réseaux est de chiffrer les données pour la confidentialité des données envoyées sur le lien radio et d'authentifier l'utilisateur (ou l'abonné) pour éviter les utilisations de ressources radio non autorisées. Les réseaux cellulaires offrent la confidentialité de l'identité de l'abonné *via* l'utilisation d'une identité temporaire.

Les nouvelles générations des réseaux cellulaires et des réseaux locaux sans fil disposent d'une authentification mutuelle permettant à l'utilisateur d'authentifier le réseau qui le sert.

La sécurité physique et logique des points d'accès au réseau local sans fil est primordiale tout comme le fait de mettre en œuvre des protocoles cryptographiques afin de se protéger des écoutes passives.

La faiblesse du protocole WEP (*Wired Equivalent Privacy*) au regard des besoins de confidentialité et d'intégrité a été démontrée. Une clé de chiffrement WEP est cassable facilement et les outils disponibles pour le faire existent sur Internet. De plus, une même clé WEP est commune à tous les utilisateurs d'un réseau partagé Wi-Fi. Pour pallier cette limite, le protocole WPA (*Wi-Fi Protected Access*) tend à remplacer le WEP et est l'objet de la norme IEEE 802.11.i. Celle-ci est connue sous le sigle de WPA 2 et se base sur l'algorithme de chiffrement AES (*Advanced Encryption Standard*) avec des clés de 128 bits et un vecteur d'initialisation de 48 bits.

Il est également possible de créer des réseaux privés virtuels *via* l'implantation d'IPSec pour sécuriser un échange de données en Wi-Fi.

Exercices

7.1 Dans un réseau GSM, expliquez comment l'identité d'un abonné, l'IMSI, est rendue confidentielle ?

7.2 Dans un réseau GPRS, expliquez comment l'entité SGSN peut authentifier un abonné sans connaître la clé d'authentification (celle-ci étant gérée au niveau du centre d'authentification, AuC) dans la base de données HLR. Est-ce que l'authentification

dans un réseau GPRS suit le même principe d'authentification que dans un réseau GSM ?

7.3 Comment le réseau UMTS renforce-t-il la sécurité des messages de contrôle des ressources radio RRC ?

7.4 Quel est le principal point faible de l'algorithme WEP de la norme 802.11 ?

7.5 Quelle est la différence fondamentale, pour ce qui concerne la confidentialité des données utilisateur, entre l'algorithme WEP défini par la norme 802.11 et l'algorithme CCMP défini par la norme 802.11i ?

7.6 Pourquoi la norme 802.11i définit-elle en plus de l'algorithme CCMP, l'algorithme TKIP ?

7.7 Comment le protocole TKIP corrige-t-il le principal point faible de l'algorithme WEP tel que défini dans l'exercice 7.4 ?

7.8 Quelles sont les principales vulnérabilités d'un réseau Wi-Fi et les principales recommandations en matière de sécurité ?

7.9 Quels sont les rôles des protocoles WAP et WPA ?

7.10 Est-il vraiment possible de protéger l'accès à un réseau sans fil ?

Solutions

7.1 La confidentialité de l'identité d'un abonné d'un réseau GSM, l'**IMSI** (*International Mobile Subscriber Identity*), est basée sur l'utilisation d'une identité temporaire, le **TMSI** (*Temporary Mobile Subscriber Identity*), et sur le fait que l'échange de l'**IMSI** est limité le plus possible sur le lien radio. Lorsqu'un mobile se connecte au réseau et envoie son identité **IMSI**, le réseau attribue un numéro **TMSI** qui sera utilisé pour toutes les communications ultérieures entre le mobile et le réseau. Le numéro **TMSI** est envoyé au mobile en mode chiffré et il est toujours chiffré avant d'être envoyé sur le lien radio. La correspondance **IMSI-TMSI** est maintenue dans la base de données **VLR** associée au **MSC** qui sert le mobile.

7.2 Dans un **réseau GPRS**, l'entité **SGSN** (*Serving GPRS Support Node*) peut authentifier un abonné sans connaître la **clé d'authentification** grâce au triplet envoyé par l'**AuC** (*Authentication Center*). L'**AuC** calcule les valeurs **RAND** et **XRES** en se basant sur la clé d'authentification de l'abonné et envoie ces résultats au **SGSN** via le triplet. Le **SGSN** envoie la valeur **RAND** au mobile et attend la réponse du mobile. Si la réponse du mobile et la valeur **XRES** sont identiques, le mobile obtient la clé d'authentification de l'abonné. En fait, les principes d'authentification GPRS et GSM sont similaires.

7.3 En plus du chiffrement, l'**UMTS** fournit une **protection d'intégrité des messages de contrôle des ressources radio RRC** (*Radio Resource Control*) via le calcul d'une valeur **MAC** de chaque message. Le **MAC** est calculé en se basant sur

le contenu du message RRC, sur la clé d'intégrité IK qui est connue par le mobile et le réseau, sur l'identificateur de la direction, sur une valeur d'un compteur et sur un nombre aléatoire FRESH. Cette valeur MAC est envoyée avec le message de contrôle RRC sur le lien radio. Le récepteur va recalculer la valeur MAC en se basant sur le contenu du message reçu et sur la clé d'intégrité IK. Si le résultat du calcul et la valeur MAC du message reçu sont identiques, cela signifie que le contenu du message n'a pas été modifié et que l'entité est authentifiée car elle obtient la clé IK. Les autres valeurs (*i.e.* la direction, le compteur et la valeur FRESH) ont pour objectif d'éviter les attaques de type rejet.

7.4 Le principal point faible de l'**algorithme WEP** est que le vecteur d'initialisation (IV) qui est transmis en clair sur le lien radio est utilisé directement comme une partie du *Seed WEP* (clé WEP). L'algorithme WEP peut être cassé par l'interception des communications.

7.5 La différence fondamentale entre l'**algorithme WEP** (*Wired Equivalent Privacy*, défini par la norme 802.11) et l'**algorithme CCMP** (*Counter with CBC [Cipher Block Chaining]-MAC Protocol*, défini par la norme 802.11i pour renforcer la confidentialité des données utilisateur) est que WEP est basé sur l'algorithme de chiffrement RC4 tandis que le protocole CCMP est basé sur l'algorithme AES, qui est beaucoup plus difficile à casser.

7.6 Comme l'implémentation du protocole CCMP demande une mise à jour au niveau du matériel (*hardware*), la norme 802.11i a défini le **protocole TKIP** comme une solution temporaire, compatible avec les cartes réseau WEP, pour la transition vers le protocole CCMP. En effet, le support du protocole TKIP nécessite uniquement une mise à jour logicielle des équipements configurés avec le protocole WEP.

7.7 Le **protocole TKIP corrige le point faible de l'algorithme WEP** (envoi en clair du vecteur d'initialisation [IV] sur le lien radio), par la constitution d'une clé par mixage (mélange de clé en deux phases). Le TSC (*TKIP Sequence Counter*), qui est équivalent au vecteur d'initialisation (IV) dans le protocole WEP, est aussi envoyé en clair, mais il n'est pas directement utilisé comme élément constitutif du *Seed WEP*. Le TSC est mixé en deux phases avec la clé secrète partagée entre le mobile et le réseau pour former le *Seed WEP* (figure 7.19). Cela assure qu'un espion, qui ne possède pas la clé secrète, ne peut pas utiliser directement le TSC comme une partie du *Seed WEP*.

7.8 La facilité de déploiement, le faible coût d'installation comme la mobilité autorisée par un **réseau Wi-Fi**, sont des avantages qui toutefois peuvent être de peu d'utilité dans la mise en œuvre de services de sécurité efficaces. En effet, comme dans toute transmission sans fil, les données émises peuvent être interceptées ou écoutes. Il existe des possibilités de déchiffrer les données véhiculées par le protocole WEP (*Wired Equivalent Privacy*), des logiciels de cassage sont disponibles sur Internet, ou en vente dans le Dark web. De plus, il est difficile de maîtriser le périmètre radio (réflexion, diffusion des ondes, brouillage, usurpation des bornes, tous les équipements connectés à une borne reçoivent les données...). Le réseau peut

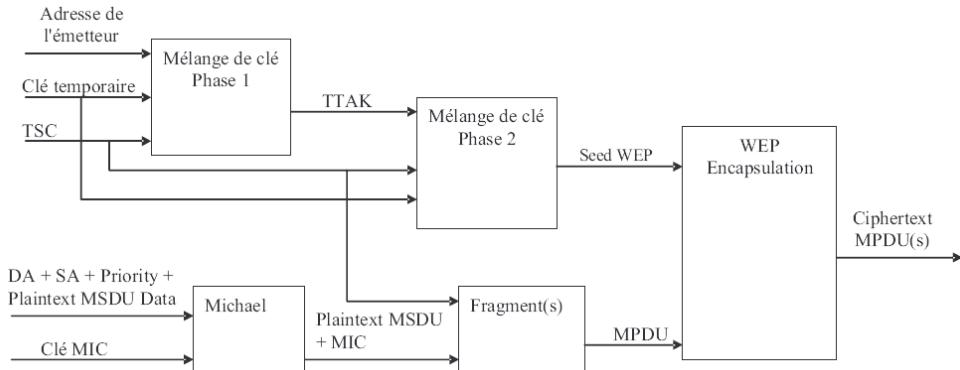


Figure 7.19 - Le chiffrement TKIP.

faire l'objet d'intrusion, de vol ou de détournement de session. L'obtention et l'usage illicite des mots de passe peuvent également mettre à mal la sécurité des systèmes raccordés.

Les points d'accès au réseau peuvent faire l'objet de destruction physique, de dénis de service par une surcharge volontaire des trames transmises et inondation du réseau, occasionnant ainsi l'indisponibilité du service réseau. De plus, un malveillant peut se substituer à un point d'accès en émettant un signal plus puissant que celui du point d'accès. En fait, différentes attaques connues mettant en défaut les critères de confidentialité, d'intégrité et d'authentification sont possibles.

Parmi les possibilités existantes pour renforcer la sécurité d'un réseau Wi-Fi, citons les suivantes :

- de configurer et d'activer les options de sécurité des points d'accès ;
- d'utiliser les protocoles cryptographiques qui permettent de réaliser la confidentialité et l'intégrité des données ainsi que l'authentification des clients ;
- de réaliser la sécurité physique des points d'accès ;
- de ne pas utiliser des mots de passe par défaut ;
- de désactiver les services disponibles non utilisés ;
- d'installer les correctifs de sécurité au fur et à mesure de leur disponibilité ;
- de gérer, surveiller, auditer le réseau et les activités ;
- d'analyser régulièrement les journaux d'activité afin de comprendre la nature des incidents survenus pour les corriger ;
- de sensibiliser et de responsabiliser les utilisateurs aux besoins et mesures de sécurité.

7.9 Le protocole WAP (*Wireless Application Protocol*) est un protocole d'accès à Internet pour des équipements mobiles (périphériques sans fil, comme des téléphones par exemple) possédant des capacités d'affichage, de traitement et d'autonomie réduites, par rapport à un poste de travail fixe). Tandis que le protocole WPA (*Wi-Fi Protected Access* [WPA et WPA2]) permet de renforcer la sécurité des réseaux Wi-Fi (norme IEEE 802.11.i) en remplacement du protocole WEP.

7.10 Oui et non. S'il est possible d'authentifier des clients d'un réseau sans fil, l'authentification mutuelle (y compris celle du point d'accès) n'est pas toujours mise en œuvre. La protection des accès à un réseau sans fil passe également par une protection physique, ce qui est difficilement réalisable dans un lieu public. Diverses attaques existent pour leurrer ou détourner les mécanismes de sécurité. Aussi, les notions de protection et de sécurité, quelle que soit la technologie employée, sont toujours relatives.

LA SÉCURITÉ PAR PARE-FEU ET LA DÉTECTION D'INCIDENTS

8

PLAN

- 8.1 Sécurité d'un intranet
- 8.2 Principales caractéristiques d'un pare-feu
- 8.3 Positionnement d'un pare-feu
- 8.4 Système de détection d'intrusion et de prévention d'incidents (IDS)

OBJECTIFS

- Mettre en évidence les besoins de sécurité liés au contrôle d'accès et au cloisonnement d'environnements Internet-intranet.
- Présenter et analyser les fonctions et caractéristiques d'un système pare-feu (*firewall*).
- Présenter et analyser les fonctions et caractéristiques d'un système de détection d'intrusion (IDS).

8.1 SÉCURITÉ D'UN INTRANET

Un **Intranet** est un réseau « Internet » privé, interne à une organisation, qui offre à ses employés des services mettant en œuvre les technologies d'Internet afin de contribuer à réaliser ses objectifs. Le plus souvent raccordé à l'Internet public, l'intranet d'une institution doit être spécialement protégé pour qu'il reste privé et non accessible au reste du monde.

8.1.1 Risques associés

Les services offerts par un intranet nécessitent le plus souvent une évolution de la capacité de transmission de l'infrastructure du réseau pour supporter les flux additionnels générés par l'usage de l'intranet. La migration de l'architecture du réseau de l'entreprise pour tenir compte des nouveaux besoins de contrôle d'accès et de cloisonnement des environnements est incontournable. En fait, ce n'est pas uniquement le réseau, mais c'est tout le système d'information qui doit être préalablement bien préparé au déploiement d'applications intranet (infrastructure, contrôle, routage, logiciels clients, serveurs adaptés, etc.).



Le premier risque de sécurité relatif à la mise en place d'un **intranet** est lié à l'incapacité de l'infrastructure de communication existante à prendre en compte de nouveaux trafics (risque d'indisponibilité des ressources).

On attachera une importance particulière à ne pas **dégrader les performances globales du système d'information** et à intégrer correctement les applications intranet, en veillant particulièrement à ne pas introduire de nouvelles brèches de sécurité.

Le premier stade de la **sécurité d'un intranet** passe donc par un bon **dimensionnement** et une bonne **gestion du réseau**. Des vulnérabilités supplémentaires ne doivent pas être créées en autorisant de manière incohérente l'interconnexion de l'intranet à l'Internet. En effet, l'ouverture des systèmes intra-organisation sur un environnement externe, *a priori* hostile, facilite toutes sortes d'attaques informatiques et de malveillances (intrusions, fuite de données, prise de contrôle à distance des ressources, etc.) dont les conséquences peuvent être dramatiques pour l'organisation.

8.1.2 Éléments de sécurité d'un intranet

La mise en place d'un intranet doit s'accompagner de la mise en œuvre de mesures et de procédures de sécurité spécifiques pour notamment contrôler l'accès aux ressources informatiques internes d'une organisation et les flux entrant et sortant entre son intranet et Internet. Il faut donc développer une véritable politique de contrôle des accès aux ressources et de contrôle des flux entre les environnements privé et public, afin d'autoriser exclusivement ceux qui sont légitimes, dans un sens et dans l'autre. Les exigences de sécurité exprimées dans la politique de sécurité de l'organisation doivent se traduire, au niveau du réseau, par des mesures architecturales appropriées.

Cette démarche peut faire appel :

- aux différents **services de l'entreprise** (expression des besoins) ;
- au **responsable de la sécurité** (gestion globale, intégration des différents impératifs de sécurité) ;
- au **directeur informatique** ou au **responsable réseau** (qui eux connaissent les véritables capacités du réseau existant à supporter des flux Internet-intranet sans pour autant fragiliser l'édifice en place) ;
- au **responsable juridique** (si nécessaire déclaration de fichiers nominatifs auprès de la CNIL pour la France, respect des contraintes juridiques liées à l'usage du chiffrement, etc.). En France, l'usage du chiffrement est libre, c'est l'achat et la vente de solutions de chiffrement qui sont soumis à déclaration ou à autorisation (de la part de l'ANSSI) ;
- au **responsable des ressources humaines** (diffusion, acceptation de la charte de sécurité, sensibilisation à une certaine éthique d'utilisation des ressources, ratification par le personnel de clauses de sécurité, les autorisations d'accès ne devant être accordées qu'après la responsabilisation des utilisateurs concrétisée par la signature d'une charte d'utilisation).

En fait, les outils de la sécurité d'un intranet sont peu différents de ceux permettant de réaliser la sécurité des télécommunications au sens large. Ils sont basés sur l'adoption d'un ensemble de mesures cohérentes de sécurité qui reposent sur le contrôle d'accès, le filtrage, l'authentification, le chiffrement, l'exploitation, la surveillance et la gestion et le cloisonnement d'environnements.

Ainsi, la **sécurité d'un intranet** s'appuie sur l'installation d'un ou plusieurs systèmes **pare-feu**, dits encore **coupé-feu** ou *firewalls*, séparant, pour le protéger, l'environnement privé de l'organisation du réseau non protégé Internet. La mise en place d'un pare-feu tend à créer un sas de sécurité isolant physiquement et/ou logiquement Internet du reste du système d'information (figure 8.1). On sépare ainsi les infrastructures interne (privée) et externe (publique). Il peut s'agir de séparation physique (pare-feu matériel, machine dédiée avec une interface spécifique à chaque partie du réseau à cloisonner) ou logique des environnements (pare-feu logiciel, programme de filtrage).



Figure 8.1 – Rôles d'un système pare-feu (*firewall*).

Pour rendre l'environnement informatique de l'entreprise complètement opaque, on masque également toutes les adresses IP internes de l'entreprise *via* des systèmes pare-feu proxy, afin que depuis l'extérieur on ne puisse les connaître et les utiliser pour détourner les règles de filtrage du pare-feu.

L'implantation et la configuration d'un **pare-feu** résultent d'un choix d'architecture de réseaux pour répondre aux besoins de sécurité et de contrôle des entités d'un système d'information. Le pare-feu constitue un des outils de réalisation de la politique de sécurité et n'est qu'un des composants de sa mise en œuvre. En effet, un pare-feu ne suffit pas à bien protéger le réseau et les systèmes d'une organisation. Il doit être également accompagné d'outils, de mesures et de procédures répondant à des objectifs de sécurité préalablement déterminés par la politique de sécurité. De plus, si l'utilisateur malveillant se trouve déjà dans le périmètre protégé par le coupe-feu, celui-ci ne peut le voir. L'efficacité d'un pare-feu dépend essentiellement de son positionnement par rapport aux systèmes qu'il doit protéger, de sa configuration et de sa gestion.

La **sécurité d'un intranet** est principalement :

- un **problème organisationnel** lié à l'adoption d'un mode de travail collaboratif, d'une culture de partage et de communication particulière qui reflète l'évolution

des besoins et de l'organisation des entreprises, et du contexte économique dans lequel elles s'intègrent ;

- un **problème d'architecture de réseau** (positionnement du/des pare-feu dans l'architecture du réseau, dimensionnement du réseau et des systèmes, configuration, paramétrage et gestion, capacité d'évolution pour supporter l'évolution des flux, etc.) ;
- un **problème de choix organisationnels, techniques et procéduraux** pour réaliser une politique de sécurité bien déterminée.

Sans vouloir être exhaustif, voici quelques **recommandations** contribuant à sécuriser un environnement intranet :

- un pare-feu doit être protégé et sécurisé contre des accès non autorisés (notion de système de confiance possédant un système d'exploitation sécurisé, souvent un LINUX ou un UNIX BSD renforcé) ;
- tous les trafics (entrants et sortants) doivent passer par le pare-feu (pas de contournement possible du pare-feu) ;
- un pare-feu ne peut pas protéger l'environnement à sécuriser contre des attaques ou des accès illicites qui ne passent pas par lui ; il n'est d'aucune efficacité en ce qui concerne des délits perpétrés depuis l'intérieur de l'entreprise, par des personnes habilitées à accéder aux données ;
- seul le trafic défini par la politique de sécurité comme étant valide et autorisé peut traverser le pare-feu ;
- configurer le pare-feu de telle sorte que tout ce qui n'est pas explicitement autorisé soit interdit ;
- un pare-feu ne peut pas également être le serveur web de l'entreprise ;
- si les données du réseau interne sont vraiment sensibles, il faut alors accéder à Internet par des machines détachées de ce réseau interne ;
- un pare-feu n'est pas un antivirus : il faut donc le protéger de manière complémentaire contre des infections virales. Dans l'absolu, un antivirus devrait résider sur tous les systèmes, serveurs et postes de travail des utilisateurs, mais attention aux performances !

8.2 PRINCIPALES CARACTÉRISTIQUES D'UN PARE-FEU

L'objet du réseau est d'offrir un maximum de connectivité et d'accès aux ressources. L'objet de la sécurité est de limiter ces accès. Ces deux objectifs concurrents et contradictoires se trouvent être ceux d'un pare-feu. Pour cela, et afin de satisfaire les objectifs de sécurité attendus du pare-feu, ce dernier implémente quatre fonctions basiques : le **cloisonnement**, le **filtrage**, le **masquage** et le **relais**.

8.2.1 Fonctions de cloisonnement

Dans une architecture de réseau, un pare-feu renforce la sécurité en contrôlant les flux de données qui le traversent (en entrée et en sortie). Un pare-feu est un système

qui permet de **filtrer les communications** qui lui parviennent, de les analyser et de les autoriser si elles remplissent certaines conditions, de les rejeter sinon. Ces conditions sont exprimées selon un certain nombre de règles reflétées par la configuration du pare-feu (figure 8.2).

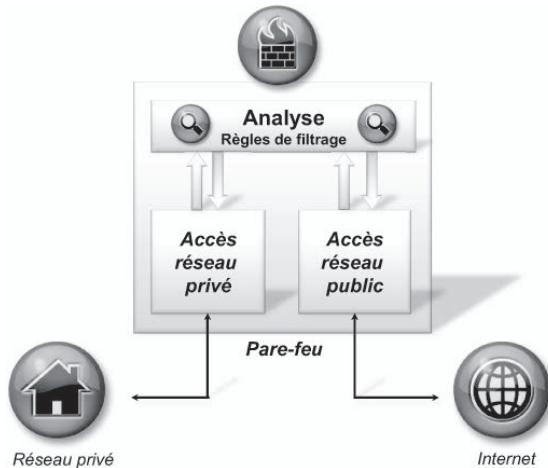


Figure 8.2 – Fonctions de cloisonnement et de filtre d'un pare-feu.

La séparation physique des environnements

En s'interfaisant entre les systèmes du réseau d'une organisation et Internet, un pare-feu permet de cloisonner le réseau et, en principe, de le masquer aux utilisateurs d'Internet.



Cloisonner un réseau revient à le concevoir de telle manière que l'on puisse, en fonction d'impératifs de sécurité, séparer des systèmes afin de mieux les contrôler.

Le principe de cloisonnement repose sur la segmentation du système d'information en composants de sécurité homogènes (domaines de confiance mutuelle). Le contrôle d'accès des flux d'information échangés entre les divers composants du système d'information doit être rigoureux pour garantir la sécurité et la séparation totale et filtrante des entités cloisonnées.

Le cloisonnement d'un réseau permet de constituer des **environnements IP disjoints** en rendant physiquement indépendants les accès des réseaux que l'on désire séparer. Cela permet d'interconnecter deux réseaux de niveaux de sécurité différents. Ainsi l'on peut contrer les flux qui pourraient engendrer la compromission des systèmes et des données (modification, destruction, altération, perte, fuite d'informations), l'atteinte aux critères d'intégrité, de disponibilité et aux performances (déni de service, détournement, prise de contrôle à distance, etc.).

Dans la figure 8.2 par exemple, toutes les demandes d'accès à Internet qui parviennent au pare-feu depuis un système du réseau interne sont préalablement analysées et traitées avant d'être émises sur Internet et inversement, si la politique de sécurité de l'organisation l'autorise.

Ce type de pare-feu possède deux cartes réseau, l'une pour le réseau de l'entreprise, l'autre pour l'accès au réseau Internet. La configuration du pare-feu est telle que les données arrivant sur l'une des cartes ne sont pas transmises directement sur l'autre mais de manière sélective, selon des critères de filtrages déterminés lors de sa configuration. Il n'est pas suffisant de filtrer uniquement les flux entrants (le filtrage doit se faire dans les deux sens).

8.2.2 Fonction de filtre

Selon la nature de l'analyse et des traitements effectués par un pare-feu, différents types de pare-feu existent. Ils se distinguent le plus souvent en fonction du niveau de filtrage des données auquel ils opèrent : **niveau 3** (IP), **niveau 4** (TCP, UDP) ou **niveau 7** (FTP, HTTP, etc.) du modèle OSI (figure 8.3).

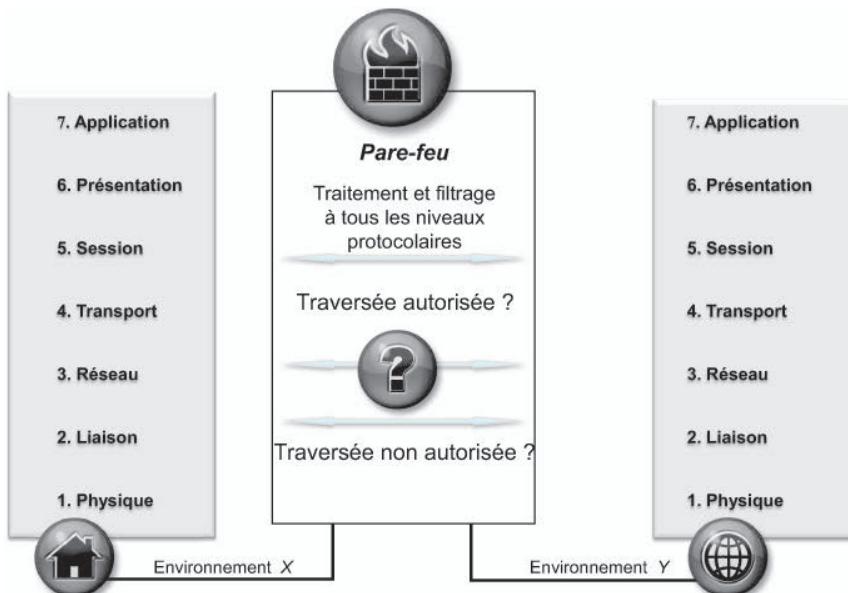


Figure 8.3 – Les différentes possibilités de filtrage d'un pare-feu applicatif.

Stateless packet filtering

Un **pare-feu dit stateless packet** (*stateless packet filtering*) analyse chaque paquet, selon un ensemble de règles déterminées qui constituent le filtre, et les informations contenues dans le paquet (adresses IP [émetteur et récepteur], numéros de ports TCP ou UDP, nature du protocole véhiculé dans le paquet, etc.).

Dans un système, les différents points d'entrée et de sortie des protocoles, pour un processus de communication donné, sont identifiés par des numéros de port codés sur 16 bits. L'adresse IP de l'ordinateur et le numéro de port du processus de communication constituent un identifiant unique. Avec 16 bits, on peut identifier 2^{16} numéros de ports différents. Parmi les ports connus et réservés à certains protocoles (ports de 0 à 1 023 – *Well Known Ports* – attribués par IETF¹), retenons par exemple les suivants : protocole FTP – port 21 ; protocole SMTP – port 25 ; protocole HTTP – port 80 ; protocole PoP 3 – port 110 ; protocole HTTPS – port 443, etc. Les autres numéros de ports correspondent à des ports enregistrés et à des ports qualifiés de dynamiques et/ou privés. Un serveur de communication reçoit une requête de demande de service *via* un port connu en fonction de l'application demandée (FTP, SMTP...), le client reçoit la réponse à sa demande de service sur un numéro de port assigné par son système d'exploitation en fonction de ceux disponibles.

Une fonction de filtrage d'un pare-feu peut être paramétrée en fonction des numéros de ports. Tous les échanges notifiés avec un numéro de port non identifié comme explicitement autorisé devront être bloqués. Ainsi par exemple le port 23, correspondant au protocole Telnet peut être bloqué de manière à empêcher toute connexion externe à un serveur en émulation de terminal.



La performance et la souplesse d'un pare-feu de niveau 3 (sa capacité à être déployé dans presque tout type d'infrastructure) sont les principaux avantages de ce type de pare-feu. En revanche, les flux applicatifs malveillants peuvent ne pas être détectés et bloqués par ce type de *firewall*.

Pour pallier le filtrage individuel des paquets indépendamment les uns des autres (de niveau 3), qui ne tient pas compte du mode de fonctionnement de TCP ou des sessions de travail, les pare-feu peuvent effectuer un filtrage sur les niveaux 3 et 4 simultanément, c'est-à-dire un filtrage du flux entre un client et un serveur (*stateful packets filtering*, notion de filtrage de paquets avec état, *stateful inspection*).

Stateful packet filtering

Un pare-feu dit **stateful packet** permet de filtrer les paquets en se basant sur la couche transport du modèle OSI (filtrage au niveau des ports de communication TCP-UDP). Il maintient une table d'état des connexions correspondant aux ports logiques du niveau 4 et sur tous les ports dont le numéro est supérieur à 1 024 (les ports utilisés par les applications de l'utilisateur) pour un meilleur suivi des communications. Ainsi, si une connexion est autorisée, tous les paquets constitutifs de l'échange seront implicitement acceptés. Certains attaquants savent détourner ce mode de fonctionnement et exploiter les failles dues aux applications communiquantes.

1. Internet Engineering Task Force (www.ietf.org), voir notamment la RFC 6335 (<http://tools.ietf.org/html/rfc6335>).

8.2.3 Fonctions de relais et de masque

Un **pare-feu applicatif** joue un rôle de filtre des flux applicatifs. Pour le paramétrier correctement, il faut connaître l'ensemble des applications qui le traverseront. Il peut également jouer le rôle de passerelle applicative, de **proxy** (serveur proxy, pare-feu proxy). Il établit en lieu et place de l'utilisateur le service invoqué par celui-ci en masquant certaines informations et en validant chaque contenu, ce qui nécessite des ressources et des temps de traitements plus longs (figure 8.4).

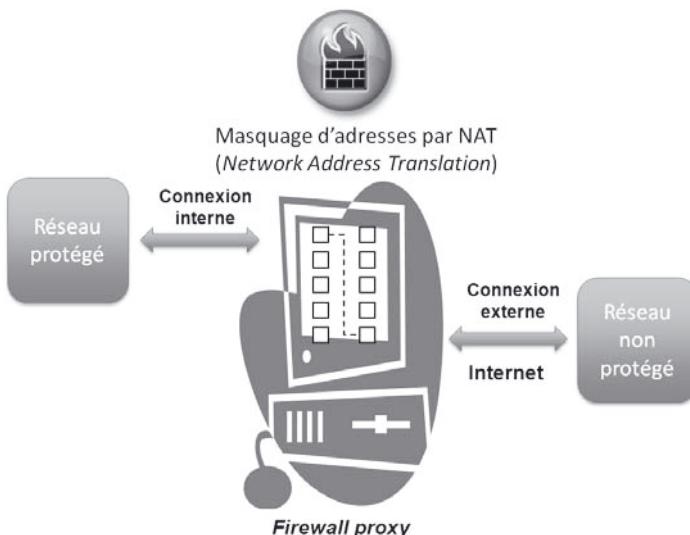


Figure 8.4 - Fonctions de relais et de masque d'un pare-feu proxy.

L'objectif d'un système qualifié de proxy est de réaliser un **masquage d'adresse** par relais applicatif, et de rendre transparent l'environnement interne de l'organisation. Il est censé constituer un point de passage obligé pour toutes les applications qui nécessitent un accès Internet. Cela suppose qu'une application « relais » soit installée sur le poste de travail de l'utilisateur et sur le pare-feu (figure 8.5).

Ainsi, à chaque demande de connexion Internet, le fait de lancer un navigateur active également ce programme relais qui demandera au proxy de réaliser la connexion externe à sa place. Le proxy contacte alors le serveur externe sollicité sur Internet, avec sa propre adresse et non pas avec celle du système de l'utilisateur final, et effectue les échanges de données nécessaires. Le proxy cache de la sorte toute l'infrastructure du réseau interne et ne dévoile en aucun cas les adresses des systèmes. Il agit comme une passerelle applicative. Ce type de serveur est systématiquement mis en œuvre lors de l'utilisation d'un plan d'adressage privé NAT (*Network Address Translation*), ce qui permet de palier l'insuffisance d'adresses IPv4 par des adresses « non routables »².

Une alternative pour effectuer un masquage d'adresse est de le réaliser au « fil de l'eau », au fur et à mesure que les paquets arrivent au pare-feu. Depuis le poste de

2. Address Allocation for Private Internets (IETF-Rfc 1918).

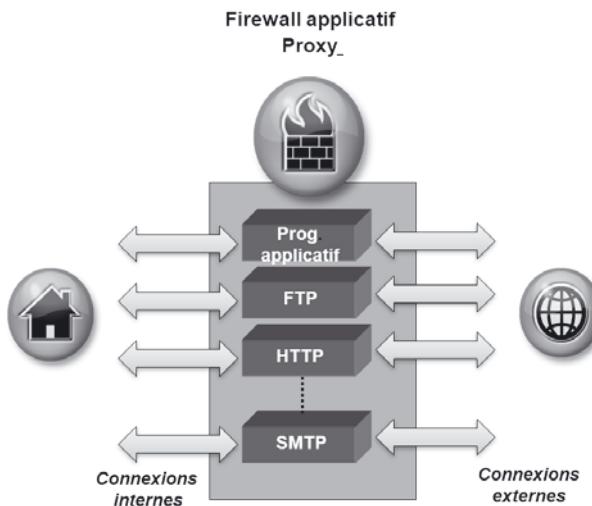


Figure 8.5 – Exemple de pare-feu proxy.

travail de l'utilisateur final les paquets de données sont transmis au pare-feu, qui retire alors l'adresse source du paquet en transit pour la substituer et y mettre soit sa propre adresse soit une adresse issue d'un pool d'adresses IP libres.

Par ailleurs, certains pare-feu réalisent également des fonctions de répartition et d'équilibrage de charge entre les systèmes qu'ils desservent.

8.2.4 Critères de choix d'un pare-feu

Les façons de configurer un pare-feu et de le gérer sont tout aussi importantes que les capacités intrinsèques qu'il possède. Toutefois, lorsque le choix s'impose, on prendra en considération, entre autres, les **critères** suivants :

- la nature, le nombre des applications appréhendées (FTP, messagerie, HTTP, SNMP, RealAudio, VDO Live, vidéoconférence, etc.) ;
- le type de filtres, le niveau de filtrage (niveau applicatif, niveau TCP, niveau IP, possibilité de combiner ces niveaux) ;
- les facilités d'enregistrement des actions à des fins d'audit, login complet des paramètres de connexion, l'existence d'outils d'analyse, d'audit actif et de détection d'activités suspectes ;
- les outils et facilités d'administration (interface graphique ou lignes de commandes, administration distante après authentification du gestionnaire, etc.) ;
- la simplicité du système, proxy facile à comprendre et à vérifier (facilité de configuration, etc.) ;
- la capacité à supporter un tunnel chiffré permettant de réaliser, si nécessaire, un réseau privé virtuel (VPN, *Virtual Private Network*) ;
- la disponibilité d'outils de surveillance, d'alarmes, d'audit actif ;
- la possibilité d'effectuer de la répartition et de l'équilibrage de charge avec un autre coupe-feu ;

- l'existence dans l'organisation de compétences en matière d'administration du système d'exploitation du pare-feu.
- Le pare-feu est comme tout système sujet à des **menaces**. Parmi elles, retenons :
- les **intrusions** dans un pare-feu avec, pour conséquences, la modification de sa configuration, des accès, l'effacement ou la modification des traces de journalisation ou encore l'infection virale ;
- toute **opération inappropriée** réalisée d'une manière accidentelle ou par négligence.

Vu l'importance et le rôle critique des pare-feu dans la réalisation de la sécurité des réseaux, la communauté internationale a proposé une évaluation de ce type de fonction et de système. L'organisation des Critères Communs³ propose notamment **deux profils de protection**, à savoir :

- **Pare-feu à exigences réduites**, qui est accessible sur le site des Critères Communs. Ce profil de protection permet l'obtention du niveau d'assurance quatre augmenté (EAL4 +).
- **Pare-feu à exigences élevées**, qui permet l'obtention du niveau d'assurance cinq augmenté (EAL5 +).

8.3 POSITIONNEMENT D'UN PARE-FEU

8.3.1 Architecture de réseaux

Plusieurs architectures et configurations de réseaux intégrant des pare-feu peuvent être mises en place en fonction des besoins, du type et du nombre de ressources à protéger ou de l'architecture du système d'information.

Un pare-feu pourra par exemple être placé en amont de serveurs sur lesquels des services indispensables (serveurs de noms, de messagerie, etc.) sont implantés. Un pare-feu peut être précédé d'un **routeur filtrant** qui s'assure que les paquets entrants à partir d'Internet sont exclusivement à destination du pare-feu (et non à destination des serveurs). Le routeur n'admettra du réseau interne que les paquets IP provenant du pare-feu (figure 8.6).

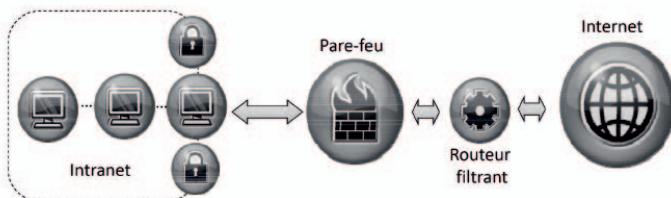


Figure 8.6 – Exemple de configuration de réseau intégrant un routeur filtrant, un pare-feu applicatif et un système bastion.

3. www.commoncriteriaportal.org

Le pare-feu effectue les fonctions de filtre, de proxy, d'authentification. Ainsi, on réalise deux mécanismes complémentaires de filtrage, l'un au niveau du routeur, l'autre au niveau du pare-feu. Toutefois, si le routeur est compromis, une brèche de sécurité importante est alors ouverte. Pour pallier cet inconvénient, on implante dans les serveurs **deux accès réseau distincts** (*dual-homed bastion*).



En augmentant le nombre et la nature des systèmes à pénétrer, de *firewalls* à traverser, avant d'accéder au réseau interne de l'organisation, on augmente la sécurité de celui-ci. Cela demande au malveillant de posséder des connaissances sur ces divers systèmes et donc un effort supplémentaire qui pourra être éventuellement rédhibitoire.

8.3.2 Périmètre de sécurité

Il est parfois nécessaire de réaliser, au sein de l'architecture du réseau interne, un **périmètre de sécurité**, notion de **zone démilitarisée** (**DMZ**, *DeMilitarized Zone*) (figure 8.7). Toutes les machines internes, y compris le pare-feu dénommé alors « *screened host gateway* », sont alors complètement masquées.

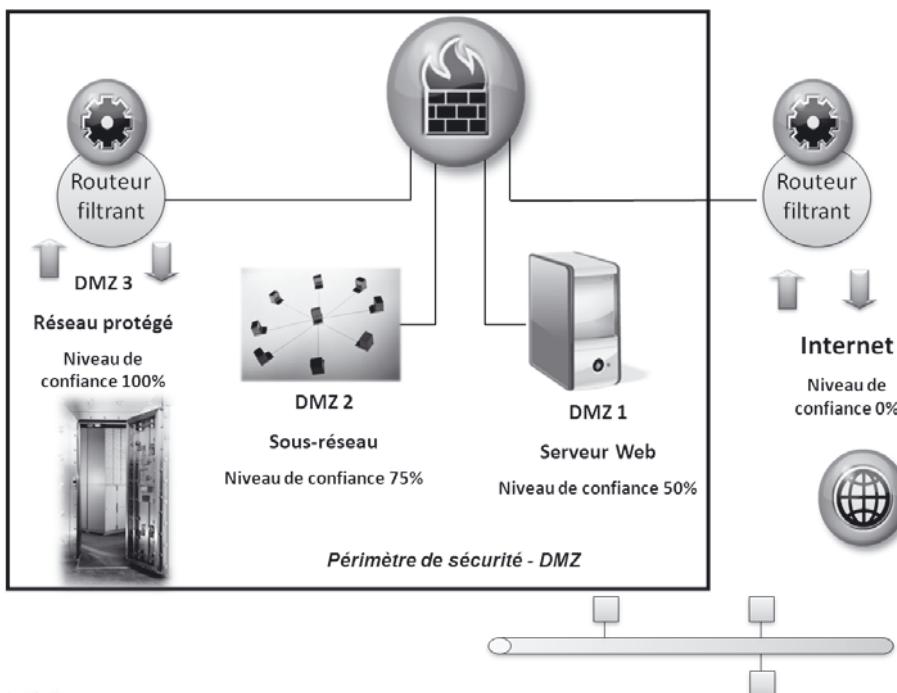


Figure 8.7 – Exemple de périmètre de sécurité.

Cela permet de créer un sous-réseau isolé relativement sûr. Le réseau interne est invisible d'Internet et les systèmes de l'entreprise ne peuvent accéder directement à Internet. On pourra configurer les systèmes en interdisant toute forme de routage automatique entre Internet et le réseau interne ou encore par exemple n'utiliser pour

Chapitre 8 • La sécurité par pare-feu et la détection d'incidents

le réseau de l'entreprise que des adresses IP à usage interne (de signification locale), telles que définies par la RFC 1918 (*Address Allocation for Private Internets*). En principe, aucun routeur ne devrait transmettre des paquets ayant pour origine ou destination de telles adresses.

Le périmètre de sécurité ne vaut que si on l'utilise. Il faut donc faire en sorte qu'il ne puisse être contourné *via* des technologies sans fil par exemple et qu'un utilisateur ne puisse établir des connexions directes à Internet. Il est donc nécessaire de définir une **politique d'usage des équipements personnels et des connexions externes** dans l'entreprise de manière rigoureuse et réalisable. En effet, en particulier avec les technologies du sans-fil et les clés USB, le système d'information d'une organisation peut être vu comme un aéroport où les menaces atterrissent directement en son cœur, plutôt que comme un château fort, où l'entrée est protégée par le coupe-feu.

La localisation d'un serveur web, dans l'architecture de réseau de l'entreprise, dépend du degré de protection et d'interaction avec les autres éléments du système d'information que l'on souhaite obtenir. Diverses **configurations** sont envisageables, les plus courantes sont résumées ci-après :

- Dans la **configuration dite de « l'agneau sacrifié »**, le serveur web est placé entre le pare-feu et le point d'accès au réseau Internet. Il n'a de ce fait aucune interactivité directe avec le reste des ressources informatiques de l'entreprise. Si cela offre un bon isolement des environnements, cela pose, entre autres, des problèmes de gestion des contenus, des mises à jour, du partage de fichiers et d'intégration des traitements. Le serveur web a toutes les chances d'être défiguré par des attaques venant de l'extérieur. Cette configuration est peu retenue par les organisations. C'est sur ce modèle de « rendre attractif » un système pour leurrer des malveillants que se base le principe du système ***honey pot*** (« pot de miel »), afin de diriger les attaques potentielles sur le système sacrifié et non sur les systèmes plus critiques de l'organisation.
- Une possibilité est de placer le **serveur « derrière » le pare-feu**, entre le réseau de l'entreprise et le pare-feu visible d'Internet. L'exploitation, le suivi et la mise à jour sont facilités, et le serveur web est bien protégé des attaques externes mais pas du tout de celles provenant de l'intérieur de l'entreprise. De plus, une prise de contrôle du serveur permet de s'en servir comme relais pour une attaque ultérieure. Pour pallier cet inconvénient, on isole les ressources de l'entreprise du serveur web, par un pare-feu interne. Un serveur web peut résider dans l'enceinte d'un périmètre de sécurité (zone dématérialisée et politique de sécurité appropriée).

Une application logicielle offrant des services de pare-feu personnel, implantée sur un poste de travail, peut également définir un périmètre de sécurité en analysant, par exemple, les demandes d'accès au réseau/aux applications à l'insu de l'utilisateur et limiter la prise de contrôle des systèmes par des entités malveillantes.

8.4 SYSTÈME DE DÉTECTION D'INTRUSION ET DE PRÉVENTION D'INCIDENTS

8.4.1 Définitions

Des systèmes de détection d'intrusion ou d'une manière générique de détection d'incidents (IDS) ou de **prévention d'incidents** (IPS) sont nécessaires afin de renforcer la robustesse des environnements informatiques, en identifiant au plus tôt de leur survenue des événements non sollicités, des **incidents**, pouvant porter atteinte à la sécurité des systèmes informatiques.

Une **erreur** peut être à l'origine d'un incident. Si l'erreur se répète parce qu'aucun dispositif n'a été mis en place pour la corriger, il ne s'agira plus d'une erreur mais d'une **faute** imputable à une personne. Une **anomalie** est une exception, elle peut induire un fonctionnement anormal du système et conduire à une violation de la politique de sécurité. Elle peut être d'origine accidentelle (par exemple une erreur de configuration) ou volontaire (une attaque ciblée du système d'information). Une **intrusion** résulte de la pénétration non autorisée dans un système, elle constitue généralement la première phase d'une cyberattaque et peut être considérée comme un incident ou une anomalie délibérée.



Incidents, anomalies et intrusions doivent si possibles être évités, sinon détectés et identifiés au plus tôt de leur survenue et maîtrisés et corrigés afin d'assurer le fonctionnement normal des systèmes et leur sécurité.

La **détection d'intrusion** est définie comme étant l'ensemble des pratiques et des mécanismes utilisés qui permettent de détecter des problèmes pouvant conduire à des violations de la politique de sécurité (la notion d'intrusion étant à considérer au sens large).

L'étude des intrusions dans les systèmes s'est beaucoup développée à partir des années 1980 où l'accent a d'abord été mis sur l'importance et la nécessité de l'automatisation des analyses et des réponses. Actuellement, de nombreux produits commerciaux mettent en œuvre les concepts, méthodes et procédés alors énoncés et ceux issus de l'intelligence artificielle.

À la détection d'intrusion certains préfèrent des systèmes de prévention d'intrusion (SPI) mais il semble que cette vue ne soit pas partagée par certains qui considèrent que les **systèmes de prévention d'intrusion** sont simplement des outils pour la détection d'intrusion. Un système de détection d'intrusion travaille de manière complémentaire à celle d'un pare-feu. Les mesures architecturales en tiennent compte. Un IPS peut être considéré comme un IDS qui sert à quelque chose, parce qu'il peut réagir à une attaque, alors qu'un IDS ne peut que la signaler.

8.4.2 Fonctions et mode opératoire

Un **système de détection d'intrusion** (IDS, *Intrusion Detection System*) analyse les données pour détecter celles qui pourraient conduire à des incidents ou à des

intrusions. Selon la localisation (sur l'infrastructure réseau ou dans un système hôte) et le champ d'action, les systèmes de détection d'intrusion se distinguent en deux types :

- **IDS_Réseaux** (N-IDS, *Network Based Intrusion Detection System*), qui constituent des sondes de manière assez similaire aux *sniffers* ;
- **IDS_Hôtes** (H-IDS, *Host Based Intrusion Detection System*) qui sont fonction des systèmes d'exploitation, et qui peuvent analyser le trafic entrant et les données enregistrées dans les journaux.

Un IDS se compose généralement de trois blocs fonctionnels essentiels :

- la collecte des informations ;
- l'analyse des informations récupérées ;
- la détection des intrusions et les réponses à donner à la suite d'une intrusion décelée.

Collecte des informations

La **collecte des informations** et des événements à une date précise est la fonction principale d'un système de détection d'intrusion. Cette collecte est réalisée à deux niveaux : au niveau de la machine hôte et/ou au niveau du réseau du système d'information.

Les informations obtenues **au niveau de la machine hôte** le sont généralement par le biais de son système d'exploitation. La plupart des systèmes d'exploitation actuels réalisent des fonctions d'audit des événements et les enregistrent : au niveau du noyau et au niveau des applications de l'utilisateur. Ces informations ne sont généralement pas exploitables par d'autres programmes que le système d'exploitation lui-même, ce qui constitue un problème de compréhension de ces informations. Toutefois, certaines applications sont commercialisées afin d'enregistrer et d'exploiter les informations sur les machines hôtes. Les données enregistrées par ces programmes sont, par exemple, l'identification de l'objet responsable d'un événement et tout autre objet lié à celui-ci, du processus qui a lancé l'événement, de l'utilisateur associé à cet événement, la date de l'événement et parfois certaines données issues directement du noyau du système d'exploitation comme les variables et les arguments d'entrée et de sortie. L'audit au niveau de la machine hôte permet d'observer directement le comportement d'un système et les événements qui surviennent. Il peut être efficace même si les applications sont chiffrées. La difficulté essentielle réside dans le déploiement d'une telle solution. En effet, il faudrait pour une efficacité optimale, installer ce système de collecte d'informations dans chaque machine du réseau. Or, une telle application est spécifique à un système d'exploitation donné. Elle n'est pas multi-plate-forme puisqu'elle opère à bas niveau, directement sur le noyau du système d'exploitation. Enfin, ces programmes d'audit généralement affectent les performances des machines hôtes du fait des ressources nécessaires à leur exécution.

 Les antivirus sont un exemple de système de collecte d'informations fonctionnant sur les machines hôtes. Ils collectent des informations et détectent celles possédant un potentiel de malveillance préalablement déterminé.

La majorité des systèmes de détection d'intrusion réalise la **collecte des informations au niveau du réseau**. Le système de détection d'intrusion est un point de contrôle obligé (notion de *check point*) par lequel transitent toutes les données, qui sont alors enregistrées dans le système. L'audit des données au niveau du réseau permet de détecter certaines attaques qui ne sont pas visibles par les systèmes de détection installés sur les machines hôtes.

Un système IDS de niveau réseau n'est généralement pas un routeur et sa localisation dans l'architecture de réseau dépend de la topologie de ce dernier.



Par exemple, dans une topologie en étoile, le système de détection doit impérativement être situé dans le nœud central, tandis que dans un réseau de topologie en bus sa localisation est moins importante.

La collecte des informations au niveau du réseau ne pose pas de problème particulier de performance dans la mesure où le système de détection lit simplement les données au moment où elles lui parviennent de manière indépendante des autres systèmes connectés au réseau, ce qui n'affecte pas leurs performances. Le système de collecte des informations au niveau réseau est transparent à l'utilisateur interne du réseau, totalement invisible depuis l'extérieur, et il ne constitue pas une cible attractive pour des attaquants potentiels.

La maintenance et le coût de déploiement de ce type de système de détection d'intrusion sont relativement bas, ce qui favorise leur mise en place au sein des réseaux d'entreprise. Les points faibles des systèmes de détection d'intrusion sont notamment relevés dans des architectures de réseau intégrant des commutateurs, supportant des données chiffrées, et dans les cas de trafics élevés. Ceci restreint donc le champ d'application des IDS de niveau réseau et en limite l'usage à des configurations de réseau particulières.

Méthodes d'analyse

La phase d'**analyse des données** et des événements fait suite à celle de leur collecte. L'analyse dans le contexte de détection d'intrusion est relative à l'organisation, au classement et à la caractérisation des informations afin d'identifier certaines activités suspectes. Ces activités peuvent alors être isolées au moment où elles se produisent ou ultérieurement. Dans certains cas, d'autres examens sont effectués afin d'affiner les résultats des analyses. Deux catégories de méthode d'analyse sont distinguées : celles basées sur les signatures et celles basées sur les profils.

- *Méthodes basées sur les signatures*

Les méthodes d'analyse des événements collectés **basées sur des signatures d'intrusion** consistent à les comparer à des scénarios d'attaques déjà connus. L'analyseur parcourt les données et les transforme en une suite d'actions selon un modèle particulier. Une fois la transformation accomplie, une étape de comparaison est alors effectuée pour identifier les événements connus par l'analyseur. Cette méthode est rapide, facile à implanter et de nombreux systèmes de détection d'intrusion l'utilisent. Le nombre de fausses alertes est relativement faible voire nul. Son

défaut majeur réside dans la nécessité de mettre à jour, comme pour un antivirus, sa base de signatures régulièrement afin de faire face aux nouvelles attaques. Cette méthode est inefficace pour contrer des attaques dont la signature n'a pas été précédemment enregistrée dans le système de détection d'intrusion.

Le fait de disposer d'un IDS ne garantit pas une protection absolue, totalement efficace contre les attaques, puisque celles non reconnues ne sont pas identifiées par le système, ce qui ne certifie pas qu'elles n'existent pas. De manière identique, un antivirus, non comportemental, ne détecte que les virus qu'il connaît.

• *Méthodes basées sur les profils*

Les méthodes de détection d'intrusion sont **basées sur la comparaison des événements collectés par rapport à des profils de comportements normaux** associés à des utilisateurs ou à des applications. Comme dans la méthode précédente, les événements enregistrés sont convertis en une série d'actions particulières et comparés à des profils prédéfinis. En se basant sur une méthode statistique et sur les profils identifiés comme normaux (c'est-à-dire autorisés), le système de détection évalue chaque comportement et parvient à distinguer les actions ou les traitements étranges qui se distinguent des profils enregistrés.

Ces systèmes n'ont pas besoin de maintenance coûteuse et aucune connaissance antérieure des attaques n'est requise. Néanmoins, ce type de système génère un nombre assez important d'alarmes qui se révèlent dans la plupart des cas de fausses alertes. La phase d'apprentissage des comportements est indispensable et doit être réalisée dans un environnement stable et non hostile. Cette méthode ne peut pas être mise en place dans un environnement dynamique où les systèmes, les utilisateurs et les applications changent fréquemment.

La pertinence et l'efficacité de la méthode d'analyse reposent sur la qualité et sur la justesse de la définition des profils d'actions autorisées. Ainsi, le système de détection d'intrusion agit comme un filtre qui doit laisser passer exclusivement les événements reconnus comme étant habituels. Si la taille du filtre est trop grande, des intrusions ne seront pas détectées (notion de **faux négatif** : un incident, pouvant engendrer des problèmes de sécurité, n'est pas identifié). Si le filtre est trop restrictif, de fausses alertes seront générées (notion de **faux positif** : une anomalie est identifiée alors que l'événement qui l'a déclenchée ne porte pas préjudice à la sécurité).

Réponses aux intrusions détectées

Suite à la collecte des informations sur les systèmes hôtes ou au niveau du réseau et à l'analyse qui a conduit à la détection d'une intrusion, une réponse est donnée. Plusieurs considérations entrent en jeu au moment de la mise en place des réponses aux intrusions et tiennent compte des choix de sécurité exprimés dans la politique de sécurité.

Les réponses des systèmes de détection d'intrusion peuvent être classées selon deux types non exclusifs de réponses : les réponses actives ou passives.

Les **réponses actives** impliquent une action à entreprendre par le système suite à une détection d'intrusion. Ces actions se regroupent en trois catégories :

- **Entreprendre une action aggressive contre l'intrus** : ceci vise à le traquer, à contre-attaquer en le localisant et en l'intimidant ou en endommageant son environnement informatique dans l'optique de faire cesser l'attaque (**notion de sécurité offensive**). Quoiqu'illégale, sauf dans certaines conditions, autorisée pour des organismes définis, en France, par la loi de programmation militaire 2014-2019, cette mesure peut éventuellement être mise en œuvre en dernier recours.
- **Restructurer l'architecture du réseau**, isoler le système attaqué, modifier les paramètres d'environnement qui ont permis à l'intrusion d'avoir lieu. C'est probablement la réponse la plus répandue actuellement et la plus efficace pour stopper la propagation d'une attaque et en limiter les impacts.
- **Surveiller le système attaqué**, collecter des informations additionnelles pour tenter de comprendre l'origine et la finalité de l'intrusion, identifier l'auteur de la malveillance, la démarche utilisée et les failles des mesures de sécurité en place. L'obtention d'un maximum d'informations relatives à l'intrusion permet éventuellement d'améliorer l'IDS en y intégrant des mesures pour contrer des tentatives d'intrusion semblables. De plus, cela facilite l'investigation des services de police, si l'organisation dépose une plainte.

Les **réponses passives** sont celles qui présentent toutes les informations récoltées et qui ont conduit à la détection de l'intrusion, à la personne en charge de la gestion des incidents. Il s'agit généralement de l'administrateur ou du responsable de la sécurité du système, qui entreprend ensuite des mesures qui lui semblent pertinentes. Aux débuts des systèmes de détection d'intrusion, toutes les réponses étaient passives. De nos jours, la plupart des IDS intègrent des fonctions automatiques de réponse active ou encore une réponse active assistée par une personne, et sont des IPS. Certains, toutefois, ne fonctionnent qu'en mode passif par le biais de génération d'alarmes (fenêtres d'attention, alarme sonore, etc.) et de notifications à l'administrateur par l'envoi d'un message électronique ou d'un SMS par exemple.

Les systèmes de prévention d'intrusion sont censés détecter et prévenir les intrusions de sorte qu'elles n'aient pas lieu. Si un début d'intrusion est identifié, les données sont bloquées. L'analyse et l'arrêt des données peuvent être effectués à différents niveaux protocolaires : au niveau Application s'il s'agit d'un programme malveillant, ou par exemple au niveau Transport si des ports interdits par la politique de sécurité sont utilisés. Le filtrage et le blocage peuvent également être effectués au niveau Réseau.

Les IDS peuvent être perçus comme étant à la fois un pare-feu et un système de détection d'intrusion. Néanmoins, leur efficacité n'est pas démontrée dans la mesure où le nombre de faux positifs est considérable et que leur mode opératoire, basé sur le blocage des communications ou des accès, les rendent peu performants.

8.4.3 Attaques contre les systèmes de détection d'intrusion

Les **systèmes de détection d'intrusion** sont, comme tous les autres systèmes informatiques, la cible d'attaques qui exploitent leurs vulnérabilités.

Outre les attaques tirant parti des possibilités de faux positifs induits par les défaillances des méthodes d'analyse, les **dénis de service** sont les principales attaques contre les systèmes de détection d'intrusion. Les malveillants visent non seulement à pénétrer dans les systèmes mais aussi à effacer leurs traces en inondant les ressources du système de détection d'intrusions.

Par exemple, en portant atteinte aux capacités de traitement du processeur central de l'IDS, soit à l'aide d'un programme malveillant, soit en intensifiant le trafic : le processeur ne sera plus capable d'analyser le trafic de manière suffisamment rapide, ce qui permettra à l'attaquant de disposer d'un laps de temps pendant lequel il ne pourra pas être détecté.

Si le système n'arrive plus à collecter les données qui transitent dans le réseau, ce qui peut être occasionné par une modification des tables de routages ou par une attaque directe aux interfaces réseau du système de détection d'intrusion, ce dernier n'est plus efficace.

Les systèmes de détection d'intrusion utilisent de la **mémoire volatile** afin de stocker les états des événements qui sont en train de se réaliser et des données utiles à la détection comme les signatures ou les profils normaux. Si cette mémoire est saturée, l'IDS est alors dans l'incapacité d'analyser correctement les événements. De plus, des supports de mémorisation (disques, supports de stockage secondaire) sont également sollicités pour sauvegarder les fichiers de journalisation des événements collectés. Si cet espace mémoire est insuffisant ou non disponible, les données sont alors perdues et aucun historique des actions et des faits ne pourra plus être réalisé.

Résumé

L'usage généralisé du Web et les services en lignes ont contraint les organisations à ouvrir leur système d'information à Internet. Il est alors devenu impératif de protéger l'infrastructure informatique et télécom privée de l'organisation et de rendre accessibles les ressources strictement nécessaires aux supports des services web.

Isoler des environnements, masquer des ressources, filtrer les flux entrants et sortants qui les traversent, autoriser ou non des accès ou services, sont les fonctions essentielles d'un système pare-feu.

Placé judicieusement dans l'architecture du réseau de l'entreprise, un pare-feu permet de renforcer la protection des systèmes internes en réalisant des périphériques de sécurité. Par ailleurs, il faut identifier au plus tôt les accès non autorisés qui sont de véritables intrusions dans le système d'information des organisations. Bien que différents types de systèmes de détection d'intrusion existent, leur efficacité n'est jamais totale. Si les systèmes pare-feu ou de détection d'intrusion contribuent à réaliser certains services de sécurité, ils ne suffisent pas à eux seuls à accomplir la protection des ressources informationnelles.

Exercices

- 8.1** Qu'est-ce qu'un pare-feu (*firewall*) ? Quels sont ses rôles, fonctions et services offerts ? Proposez un schéma de structure fonctionnelle d'un pare-feu.
- 8.2** Un pare-feu est un outil de sécurité nécessaire mais pas suffisant, pourquoi ?
- 8.3** Sur quels paramètres peut s'effectuer le filtrage de paquets IP ?
- 8.4** Qu'apporte le filtrage effectué au niveau applicatif ?
- 8.5** Comparez les systèmes de détection d'intrusion dont la collecte d'informations est basée sur les machines hôtes (*host based*) et sur le réseau (*network based*).
- 8.6** Quels sont les avantages et les inconvénients d'un système de détection d'intrusion utilisant la méthode d'analyse par signature ?
- 8.7** Quels sont les services de sécurité offerts par un système de détection d'intrusion ? À quels critères de sécurité un système de détection d'intrusion répond-il ? Peut-on avoir confiance en un système de détection d'intrusion ?
- 8.8** Pourquoi qualifie-t-on un système pare-feu de « mesure de sécurité architecturale » ?
- 8.9** Est-ce qu'un système pare-feu peut offrir un service de répartition de charge ?
- 8.10** Quels sont les points communs entre un système pare-feu et un système de détection d'intrusion (IDS) ?
- 8.11** Quel est l'intérêt principal de masquer les adresses IP internes à une organisation ? Quel type de système permet de le faire ?

Solutions

- 8.1** Un **pare-feu** (*firewall*) est une entité matérielle et logicielle (les *appliances*) ou simplement logicielle qui permet de contrôler les données qui le traversent en les filtrant selon des paramètres (critères, règles de filtrage) fixés lors de sa configuration, et implémentant la politique de sécurité de l'organisation.

Un système pare-feu contribue à réaliser la protection des environnements informatiques en réalisant une sécurité périphérique. Il permet de masquer, séparer, isoler des ressources en servant d'intermédiaire dans la réalisation des connexions internes et externes.

Le **rôle principal** d'un pare-feu est de créer un sas de sécurité permettant de séparer et d'isoler certaines entités, de définir des zones de confiance dans lesquelles des ressources verront leur accès contrôlé par des pare-feu. La définition, par des

systèmes pare-feu, d'un **périmètre de sécurité** ou **zone démilitarisée (DMZ)** permet d'isoler des systèmes et de masquer des ressources.

Pour assurer ce rôle, un pare-feu peut supporter des fonctions de filtrage, de relais et de masquage.

La fonction de **filtre** analyse les communications passant par le pare-feu et ceci dans les deux sens (sortant ou entrant). Cette fonction de filtrage peut être assurée à tous les niveaux du modèle OSI, pour tout type de protocole.

Les fonctions de **relais** et de **masque** sont généralement associées dans un pare-feu qualifié de proxy qui masque les ressources internes du système d'information. Chaque application passe alors par le pare-feu proxy et envoie sa requête non pas au serveur qu'elle désire atteindre mais au pare-feu, qui la retransmettra. Inversement, les communications émises depuis Internet à destination des systèmes internes ne les atteignent pas directement mais sont préalablement traitées par pare-feu. On parle alors de *reverse proxy*.

La structure fonctionnelle d'un pare-feu est présentée par la figure 8.8.

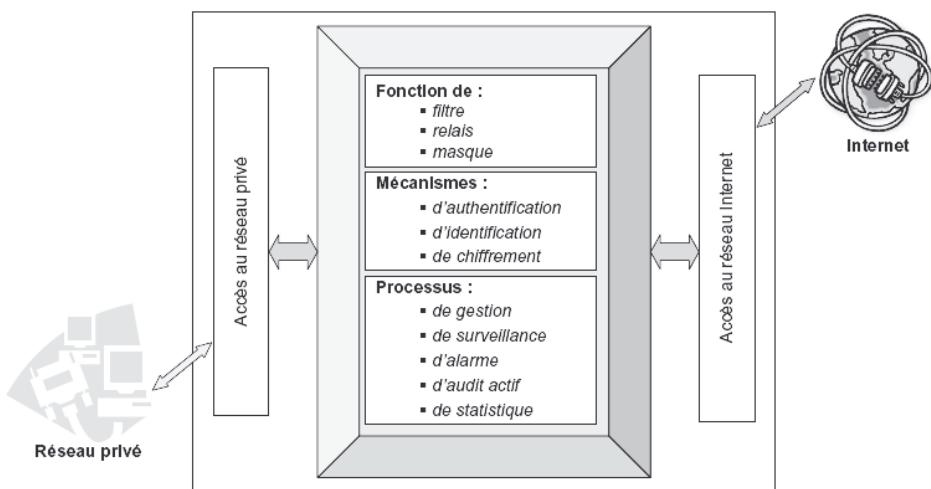


Figure 8.8 – Structure fonctionnelle d'un pare-feu.

8.2 Un pare-feu est un outil de sécurité **nécessaire mais pas suffisant** dans la mesure où, à lui seul, il ne peut réaliser l'ensemble des mesures de sécurité identifiées dans une politique de sécurité. Il peut contribuer à effectuer un contrôle d'accès aux ressources d'un système d'information et à en limiter la visibilité mais il ne peut en aucun cas se substituer à des mesures de chiffrement de données, ou de vérification d'intégrité par exemple. Comme tout autre outil de la sécurité, il doit être utilisé de manière cohérente et complémentaire pour satisfaire des objectifs de sécurité

préalablement déterminés dans une politique de sécurité résultant de l'analyse des risques liés au système d'information.

Un pare-feu unique constitue un point de passage obligé pour toutes les communications entrantes et sortantes et, comme il ne doit pas être contourné, il peut dégrader considérablement les performances du réseau. Il peut également constituer un point central de vulnérabilité (*single point of failure*). Dans un réseau, le fait de disposer comme seule mesure de sécurité des pare-feu peut introduire un faux sentiment de sécurité, préjudiciable à la protection réelle des systèmes et des données.

8.3 Le **filtrage de paquets IP** s'effectue sur toutes les données contenues dans l'en-tête du protocole (typiquement adresses IP source et destination, type de protocole encapsulé, options, etc.) et non sur le contenu des paquets.

8.4 Contrairement à un filtrage de niveau IP, le **filtrage effectué au niveau applicatif** permet d'analyser et éventuellement de bloquer des flux applicatifs ne répondant pas aux critères autorisés. Toutefois, des applications de messagerie instantanée (ICQ...) ou de partage de fichiers en point à point (Napster, gnutella...) peuvent ne pas être filtrées par un pare-feu. En encapsulant ce type de communication dans des protocoles applicatifs autorisés, on peut créer un tunnel applicatif invisible par le pare-feu.

8.5 La **collecte d'informations** est primordiale pour les systèmes de détection d'intrusion (IDS) afin qu'ils puissent identifier les événements qui relèveraient d'une tentative d'intrusion. Cette récupération des données peut s'effectuer soit au niveau des machines hôtes, soit au niveau du réseau.

La collecte d'informations directement sur les machines s'opère *via* le système d'exploitation, ce qui permet d'observer le comportement et les événements d'un système particulier et peut être efficace même si les données sont chiffrées. Cette solution de collecte d'informations est difficile à déployer surtout pour des grands environnements informatiques. De plus, les performances et l'espace disque des **machines hôtes** sont affectés par ce traitement additionnel. La collecte d'informations **au niveau du réseau** consiste à récupérer les données lors de leur transit. Cela permet d'être indépendant du système d'exploitation des systèmes, de surveiller le trafic, de détecter certaines attaques impossibles à déceler par la collecte d'informations au niveau des machines hôtes (attaques basées sur les paquets mal formés et certains dénis de service par exemple). La maintenance d'une telle solution ainsi que le coût de déploiement sont relativement bas comparés à ceux des IDS basés sur la collecte d'informations au niveau des machines hôtes. Néanmoins, cette solution reste inefficace si les données transitant sont chiffrées ou s'il s'agit d'un réseau commuté ou fortement segmenté.

8.6 Les systèmes de détection d'intrusion **basés sur la méthode d'analyse par signature** permettent d'identifier des attaques et des événements d'une manière rapide voire en temps réel. Cette méthode autorise un nombre de fausses alertes relativement faible et ce type d'IDS est relativement facile à déployer. Les inconvénients de cette

méthode d'analyse par signature sont identiques à ceux des logiciels antivirus. Comme eux, ils ne détectent que les événements dont la signature est préenregistrée. Les nouveaux scénarios d'attaques, les nouvelles formes d'intrusion, les nouveaux virus ne sont pas repérés. De ce fait, des mises à jour de la base de données de signatures doivent être effectuées fréquemment afin d'augmenter le degré d'efficacité des IDS, qui de toute manière seront impuissants pour détecter une attaque de signature inconnue.

8.7 Un **système de détection d'intrusion** contribue à réaliser la disponibilité, l'intégrité des ressources et la confidentialité des données en évitant la destruction, la modification, le vol de données, l'infection virale, la mise en place de chevaux de Troie ou la prise de contrôle des systèmes par exemple. Cela renforce les critères de disponibilité, d'intégrité, de confidentialité. Il est toutefois difficile de faire totalement confiance aux systèmes de détection d'intrusion, du fait de leur mode de fonctionnement, ils peuvent être détournés et aucune garantie n'est donnée sur leur efficacité absolue. Il est impératif de surveiller leur fonctionnement, d'auditer leurs logs afin de valider leur adéquation aux besoins ou de les adapter pour qu'ils soient toujours performants.

8.8 On qualifie un système pare-feu de « mesure de sécurité architecturale » parce que l'implantation et la configuration du pare-feu résultent d'un choix d'architecture de réseau en fonction des besoins de sécurité. Son efficacité dépend de son positionnement par rapport aux systèmes qu'il doit protéger, de sa configuration, de sa gestion et des outils, mesures et procédures qui l'entourent.

8.9 Il est possible d'utiliser un système pare-feu, notamment les pare-feu applicatifs et proxy, pour, en plus de leur fonction initiale, répondre aux besoins de répartition et d'équilibrage de charge des serveurs sollicités. Des offres commerciales existent dans ce sens.

Un responsable de réseau devrait choisir alors si une telle configuration est appropriée ou s'il serait plus judicieux de séparer les fonctions et d'avoir des systèmes dédiés à la gestion de charge.

8.10 Les principaux points communs sont la collecte des données qui les traversent, l'analyse de données et le filtrage avec blocage éventuel des données selon des critères préalablement définis.

8.11 Le masquage des adresses IP internes à une organisation à l'avantage de cacher au monde extérieur ces informations qui pourraient être utilisées pour réaliser des attaques, accéder à des ressources, pour leurrer des systèmes (y compris les pare-feu), détourner les mesures de sécurité.

Si une organisation n'est visible sur Internet que par une seule adresse IP, et ne laisse rien deviner de son plan d'adressage privé ou de ses adresses IP du fait de l'usage de systèmes proxy bien configurés, elle dresse un rempart entre son environnement informatique et Internet, plus facile à surveiller et à défendre. On parle ici de NAT (*Network Address Translation*).

LA SÉCURITÉ DES APPLICATIONS ET DES CONTENUS

9

PLAN

- 9.1 Messagerie électronique
- 9.2 Protocoles de messagerie sécurisés
- 9.3 La sécurité de la téléphonie Internet
- 9.4 Mécanismes de sécurité des applications Internet
- 9.5 Sécurité du commerce électronique et des paiements en ligne
- 9.6 Sécurité des documents XML
- 9.7 Marquage de documents et droits numériques
- 9.8 Le BYOD, les réseaux sociaux et la sécurité

OBJECTIFS

- Présenter les outils, les mécanismes et les mesures de protection pour la messagerie électronique, ainsi que pour le support de diverses applications Internet.
- Aborder certains aspects de la sécurité de la téléphonie Internet.
- Examiner les problèmes et les éléments de solution de la sécurité du commerce électronique et des paiements en ligne.
- Considérer la sécurité des documents XML et des contenus.
- Traiter de la sécurité sous l'angle de la gestion des droits et des politiques électroniques.
- Aborder la sécurité des nouvelles pratiques liées aux réseaux sociaux et à l'informatique personnelle.

9.1 MESSAGERIE ÉLECTRONIQUE

9.1.1 Une application critique

Bien que les messages électroniques (e-mail, courriel) circulent généralement en clair sur le réseau, ce qui devrait en limiter l'usage au transfert de données non confidentielles et dont l'authenticité et l'intégrité ne sont pas garanties, la messagerie électronique est un outil de travail indispensable et une application critique pour les organisations. Dans ce contexte, il est impératif qu'elle soit disponible, performante, fiable et sûre.

9.1.2 Risques et besoins de sécurité

Les **risques de sécurité** encourus par l'usage d'un système de messagerie sont principalement liés à :

- la perte, l'interception, l'altération, la destruction de messages (des messages peuvent être introduits, rejoués, mélangés, supprimés, retardés) ;
- la divulgation d'informations confidentielles ;
- l'infection des systèmes par le biais de messages contenant des codes malveillants (virus, vers ou cheval de Troie) ;
- l'inondation de messages (*junk mail*, spam, etc.) ;
- l'usurpation d'identité, le harcèlement des utilisateurs ;
- le refus de service par défection d'un élément de la chaîne du système de messagerie ;
- la répudiation (un acteur du système nie avoir envoyé ou reçu un message).

À ceux-ci on associe également tous les risques liés aux réseaux et à leurs modes de fonctionnement (attaques au niveau du routage, des serveurs de noms, etc.). À ces risques intrinsèques, sont associées les nuisances liées à la messagerie elle-même. Des **messages non sollicités** (spam, pourriel) peuvent surcharger les boîtes aux lettres électroniques des utilisateurs, être le support d'escroqueries et d'arnaques de toute sorte, de campagnes de marketing agressif ou promouvant des produits interdits ou contrefaçons. De plus, le spam par envoi massif de messages infectés peut contribuer à la propagation rapide de programmes malveillants (virus, cheval de Troie, *spyware*, etc.). Des **codes malveillants** (virus et dérivés) peuvent infecter les systèmes par le biais de la messagerie et porter atteinte à la confidentialité, à l'intégrité, à la disponibilité et aux performances des ressources. De plus, bien souvent, une attaque en phishing commence par un message qui propose de cliquer sur un lien conduisant à télécharger un malware ou à entrer des paramètres dans un formulaire situé sur le Web de l'attaquant.

Les impératifs de sécurité des systèmes de messagerie s'expriment en termes :

- de confidentialité et d'intégrité des messages ;
- de non-répudiation (preuve de l'émission, preuve de la réception, signature, certification des messages) ;
- d'authentification de l'identité de tous les acteurs du système de messagerie (utilisateurs, éléments intermédiaires, mémoire de messages, agents de transfert de messages, etc.).



9.1.3 Mesures de sécurité

Une parade à mettre en place consiste à installer de manière complémentaire, sur les serveurs et les postes de travail, des antispams et des **antivirus**¹ afin d'identifier et d'éliminer les messages/programmes non sollicités.

1. Toutefois, un antivirus ne détecte que les virus pour lesquels il a été conçu et ne protège pas contre de nouvelles formes d'infection. Par ailleurs, un antivirus augmente les temps de traitement des données et dégrade considérablement les performances des systèmes. De plus, les nécessaires mises à jour des logiciels d'antivirus demandent un effort de gestion non négligeable.

Un serveur de messagerie de désincubation, qui examine systématiquement tous les messages et leurs pièces jointes, peut également être mis en place. Plusieurs antivirus peuvent alors s'exécuter simultanément et augmenter ainsi la probabilité de détection d'un message infecté. Le filtrage du spam est réalisé avec plus ou moins d'efficacité au niveau des fournisseurs d'accès Internet ou des serveurs de messagerie.

Le principe de base du filtrage du spam consiste à filtrer et à analyser chaque message électronique, selon des critères particuliers préalablement fixés par le responsable du service de messagerie. Si le message correspond au critère de filtrage, il est alors considéré comme étant « polluant » et potentiellement indésirables, puis traité en conséquence.

9.1.4 Cas particulier du spam

Contexte et nuisances

Au sens large, le spam désigne l'envoi de messages électroniques non sollicités de manière massive et répétée, dans un objectif commercial ou très souvent à des fins malveillantes (phishing, prise de contrôle de l'ordinateur, introduction de programme malveillant [virus, *adware*, *spyware*], déni de service). Le plus souvent, le contenu des messages est illégal, trompeur ou préjudiciable et les adresses des destinataires sont obtenues à l'insu de leur propriétaire (en violation des règles relatives à la protection des données à caractère privé).



De nos jours, le phénomène du spam ne concerne pas uniquement la messagerie électronique, il touche aussi les messageries instantanées et la téléphonie par le biais de la voix sur IP et des SMS.

Au niveau européen, la directive 95/46/CE du 24 octobre 1995 *relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel* donne les standards minimaux en matière de constitution de fichiers et de traitement de données. L'article 10 de cette directive impose que le titulaire connaisse la finalité de la collecte et l'identité du contrôleur. **En France** par exemple, la loi « informatiques et libertés » pénalise l'infraction des atteintes au droit de la personne résultant de l'exploitation des fichiers, des données personnelles ou des traitements informatiques et donc l'utilisation des adresses de messagerie à des fins de spam car ces dernières sont considérées comme des données personnelles. Les citoyens bénéficient de droits spécifiques tels que ceux relatifs au droit à l'information (connaissance des informations qui les concernent), le droit d'accès aux données personnelles, le droit de rectification et d'opposition (vérification de l'exactitude et possibilité de refuser). Les **États-Unis** se sont dotés d'un texte de loi spécifique concernant le spam, permettant de poursuivre les *spammers* (CAN-SPAM Act Controlling the Assault of Non-Solicited Pornography and Marketing, 2003). La collecte des adresses sur des sites web est interdite et sont prohibés les programmes qui génèrent des adresses en combinant aléatoirement des lettres et des chiffres.

Le spam peut également poser un problème du point de vue de la concurrence déloyale quand il est utilisé dans un but publicitaire. En effet, il peut être considéré comme une politique de vente ou de publicité agressive.

Spam, publicité et concurrence déloyale

La publicité sur Internet ne disposant pas d'un cadre légal spécifique, elle se réfère au droit de la publicité en général et doit respecter les règles applicables au commerce « classique » et au e-commerce.

Cela concerne la protection des jeunes internautes, le respect de la personne humaine, le respect d'une publicité loyale, véridique et honnête, le respect de l'intimité numérique des internautes, le confort de la navigation.

Spam et intention criminelle

Lorsque les spameurs agissent avec une intention criminelle, cette dernière peut être placée sur le plan du droit pénal. Même si les messages peuvent revêtir un caractère commercial, le contenu peut faire l'objet de poursuites.

Spam et pornographie

Une grande majorité des messages de spam invitent à visiter des sites pornographiques. Cette action, notamment le fait de rendre accessible de tels contenus à des personnes qui ne le désirent pas ou à des mineurs, est le plus souvent réprimée par le droit pénal des pays.

Spam, escroquerie, virus et vente de produits prohibés

Le spam constitue souvent le moyen d'introduire des programmes malveillants et de prendre le contrôle des systèmes ciblés. L'introduction de virus peut être considérée comme une détérioration de données et est réprimée par le droit pénal, pour autant que ce virus ait provoqué des dégâts (modification, effacement ou mise hors usage des données). De plus, si le spam est le support à une escroquerie, celle-ci est aussi réprimée (délit classique réalisé *via* un nouveau support).

Régulation du spam

Deux visions s'opposent pour la régulation du spam : l'*opt-in* « permission marketing » avec consentement explicite préalable de l'internaute pour recevoir du spam et l'*opt-out* « désinscription », qui est en fait un droit d'opposition *a posteriori* de recevoir de tels courriers électroniques.

En principe, la démarche communautaire européenne, y compris la Suisse, penche vers la solution de l'*opt-in*, se basant sur la directive 2002/58/CE *concernant le traitement des données à caractère personnel et la protection de la vie privée dans le secteur des communications électroniques (directive vie privée et communications électroniques)*, tandis que les États-Unis sont plutôt favorables à l'option *opt-out*.

Seule la complémentarité des approches technico-juridiques permet de lutter contre le phénomène du spam. Un spameur de moins, découragé par une règle de droit ou empêché efficacement par une solution technique, et cela contribue à faire diminuer le nombre de spam circulant sur Internet. Toutefois, remarquons qu'une véritable économie souterraine s'est développée autour du commerce d'adresses e-mail et du profilage des internautes. Sur le Dark web, tout s'achète et tout se vend, les adresses de messagerie exploitées à des fins de spamming ou de relations commerciales B2C (*Business to Consumer*) ou B2B (*Business to Business*) n'échappent pas à la règle.

9.2 PROTOCOLES DE MESSAGERIE SÉCURISÉS

Pour pallier les principales limites sécuritaires inhérentes au mode de fonctionnement de la messagerie, de nouvelles versions de logiciels de messagerie intègrent des capacités de chiffrement et de signatures électroniques pour assurer la confidentialité, l'intégrité et l'authenticité des informations échangées et des correspondants.

Le **protocole initial de messagerie SMTP²** (*Simple Mail Transfer Protocol*) de l'environnement Internet a été enrichi au cours du temps pour supporter, d'une part, des contenus de message multimédia et d'autre part, pour intégrer des mécanismes de sécurité. Plusieurs sont disponibles actuellement, parmi eux, citons :

- **Le protocole S/MIME³** (*Secure Multipurpose Internet Mail Extensions*) est une extension sécurisée, intégrant un processus de certification, du protocole de messagerie MIME, orienté support de messages multimédia.
- **Le protocole PEM⁴** (*Privacy Enhancement for Internet Electronic Mail*) est un standard proposé par l'IETF (*Internet Engineering Task Force*) pour chiffrer des messages électroniques. Il combine l'usage des algorithmes RSA et DES. Assez complexe, ce système est relativement peu utilisé.
- **Le protocole PGP⁵** (*Pretty Good Privacy*) est une solution connue des usagers pour rendre confidentielle la transmission de messages et authentifier l'émetteur. Elle fut développée et mise à disposition sur Internet dès 1991 par son auteur, P. Zimmermann. Cette alternative peut poser le problème de sa compatibilité avec le format des messages du système de messagerie MIME.

9.2.1 S/MIME

Un message est composé d'une enveloppe et d'un contenu. C'est sur l'enveloppe que sont spécifiées toutes les informations nécessaires au transfert du message et à sa remise. Le contenu, quant à lui, est structuré en en-tête dont la fin est précisée par

-
2. Protocole SMTP (RFC 821 - www.ietf.org/rfc/rfc821.txt).
 3. Toutes les RFC relatives à S/MIME sont accessibles à partir du site : www.imc.org/ietf-smime
 4. PEM (RFC 1421, 1422, 1423, 1424) accessible à partir du site de l'IETF (www.ietf.org).
 5. PGP (versions accessibles en freeware à partir de www.pgpi.org/).

une ligne blanche, suivie du corps du message. Un identifiant unique du message (*Message-Id*) est associé à l'en-tête.

À partir de cette définition de format de message a été développé le protocole de messagerie **SMTP** (*Simple Mail Transfer Protocol*).

Les limitations suivantes sont inhérentes au protocole SMTP :

- SMTP ne peut transmettre que des messages « texte » en ASCII 7 bits. Ainsi, les particularités des alphabets de certains langages ne peuvent être véhiculées par des messages SMTP, comme également les fichiers exécutables ou les objets binaires associés à un message ;
- des problèmes de conversions de formats ASCII-EBCDIC et de compatibilité de format des messages SMTP-X.400 peuvent survenir au niveau des passerelles de messagerie ;
- le rejet de message dont la taille est trop importante peut arriver au niveau des serveurs SMTP.

MIME (*Multipurpose Internet Mail Extensions*) répond aux restrictions précédentes (RFC 2045 à 2049), tout en étant compatible avec les spécifications de la RFC 822. Ainsi sont spécifiés :

- cinq nouveaux champs d'en-tête qui permettent de préciser le corps du message ;
- le support de contenus de type multimédia ;
- des facilités de conversion de formats.

S/MIME (*Secure Multipurpose Internet Mail Extensions*) en est une extension sécurisée qui propose, comme PGP d'ailleurs, des services d'authentification par signature et de confidentialité par chiffrement. Ainsi, S/MIME permet de chiffrer tout type de contenu ainsi que les clés de chiffrement à destination de un ou de divers destinataires.

La signature du message est réalisée par chiffrement, *via* la clé privée de l'émetteur (RSA, DSS), d'un résumé du message (*message digest*) créé par une fonction à sens unique MD5, SHA-1 ou MD5. Les clés de session sont générées *via* l'algorithme Diffie-Hellman. Les algorithmes de chiffrement RSA, DES, RC2/40 sont supportés par S/MIME.

9.2.2 PGP

Pour répondre au besoin de confidentialité et d'authentification de la messagerie électronique, certains utilisent les services offerts par **PGP** (*Pretty Good Privacy*). Il s'agit d'une solution s'exécutant sur un grand nombre de plates-formes et disponible gratuitement ou commercialement. Un de ses avantages réside dans le fait qu'elle n'a pas été développée par une agence gouvernementale ou par un organisme de normalisation, ce qui rassure certains internautes. De plus, ses sources sont disponibles, ce qui permet de s'assurer de l'absence de **porte dérobée** (*backdoor*), qui pourrait permettre l'espionnage ou la prise de contrôle à distance.

Cette solution se base sur l'algorithme IDEA pour le chiffrement de messages, sur MD5 pour le *hash* du résumé, sur RSA pour le chiffrement du résumé et pour l'échange de la clé privée nécessaire à IDEA. Cette dernière est générée de façon

aléatoire au moment du chiffrement et utilisée une seule fois. PGP utilise optionnellement la compression (ZIP)⁶ d'un message avant son chiffrement. On mémorise localement la ou les clés secrètes de l'utilisateur, qui sont elles-mêmes chiffrées. Cet ensemble de fonctions est relativement facile à mettre en œuvre et bien documenté.

PGP propose cinq types de services permettant de renforcer la sécurité des messages transférés, à savoir : l'authentification par signature digitale, la confidentialité, la compression ZIP, la compatibilité, ainsi que la segmentation et le rattachement.

Lors de l'authentification par signature digitale, l'émetteur crée un message à partir duquel un résumé (*hash*) d'une longueur de 160 bits est généré en utilisant l'algorithme SHA-1. Ce *hash* est ensuite chiffré avec la clé privée de l'émetteur et l'algorithme RSA. Il est alors transmis au destinataire avec le message. À sa réception, le récepteur décode avec la clé publique de l'émetteur le *hash*. Il génère un nouvel *hash*, par la même fonction à sens unique SHA-1, et le compare avec celui reçu et déchiffré. S'ils correspondent, le message est authentifié.

La confidentialité des messages est assurée par chiffrement. Divers algorithmes de chiffrement symétrique et à clés publiques sont applicables : CAST, IDEA, Triple DES, Diffie-Hellman ou RSA. Les clés de chiffrement symétrique ne sont utilisées qu'une seule fois et pour un seul message.

Pour répondre au problème de la distribution des clés de sessions, on utilise le chiffrement à clé publique. La clé de session est un nombre aléatoire de 128 bits généré par l'émetteur. Elle est chiffrée en utilisant la clé publique du destinataire et RSA. Le message est lui chiffré par l'algorithme CAST-128, IDEA, DES, ou AES par exemple. Le destinataire décode la clé de session avec sa clé privée et cette clé de session est ensuite utilisée pour déchiffrer le message original.

Les services d'authentification et de confidentialité peuvent être associés.

La compression ZIP des données est faite après la réalisation de la signature du message et avant son chiffrement. Certains mécanismes de conversion de formats sont effectués par PGP pour assurer la compatibilité entre systèmes de messagerie. Enfin, des fonctions de fragmentation de message et de rattachement sont mises en œuvre pour une adaptation aux diverses restrictions de taille des messages supportée par les systèmes.

9.2.3 Recommandations pour sécuriser un système de messagerie

Parmi des directives élémentaires qui contribuent à protéger un système de messagerie, retenons :

- **Du côté du serveur :**

- ◊ implanter des logiciels antivirus et antispam ;
- ◊ filtrer les messages sur certains critères paramétrables (taille, fichiers attachés, etc.) ;

6. <http://www.info-zip.org/>

- ◊ configurer correctement le serveur ;
 - ◊ effectuer une gestion efficace pour en assurer la disponibilité ;
 - ◊ éviter les comptes de maintenance par défaut ;
 - ◊ assurer une protection physique du serveur.
- **Du côté de l'utilisateur :**
 - ◊ installer, gérer et imposer l'usage de logiciels antivirus ;
 - ◊ définir des règles d'utilisation de la messagerie (ne pas ouvrir des fichiers exécutables, etc.) ;
 - ◊ sensibiliser suffisamment les utilisateurs aux risques encourus ;
 - ◊ faire s'engager les utilisateurs sur un usage approprié des ressources informatiques (établir, faire connaître et respecter une charte d'utilisation des ressources, programmes de sensibilisation, etc.) ;
 - ◊ configurer correctement le poste de travail de l'utilisateur et son application de messagerie ;
 - ◊ planter des versions de messagerie sécurisées ;
 - ◊ utiliser des procédures de chiffrement pour les messages confidentiels et réaliser l'authentification des sources.

9.3 SÉCURITÉ DE LA TÉLÉPHONIE INTERNET

9.3.1 Contexte et éléments d'architecture

La voix sur IP (**VoIP Voice over IP**) permet à des équipements IP de téléphoner en s'affranchissant des opérateurs téléphoniques classiques, pour communiquer à faible coût (au prix de l'abonnement Internet) même sur les grandes distances et à l'international. Les données vocales sont *paquétisées*, c'est-à-dire mises en paquets IP et ces derniers doivent pouvoir être livrés au destinataire dans le bon ordre et sans perte, avec une certaine qualité de service, pour que la communication puisse se réaliser de manière fluide, sans délais excessifs ni écho. Bien que la téléphonie soit appréhendée par le réseau comme une application supplémentaire, au même titre qu'une autre, elle s'appuie sur des protocoles de session additionnels pour supporter la synchronisation des données et l'interactivité des interlocuteurs en temps réel.

Le plus souvent, cela passe par la mise en œuvre de protocoles d'**établissement de session SIP** (*Session Initiation Protocol*) ou **H.323** tel que défini par l'Union internationale des télécommunications (UIT)⁷. Les protocoles sous-jacents de niveau Transport peuvent être TCP ou UDP. En fait, toute une pile de protocoles intervient notamment dans le contexte d'une architecture H.323, qui correspond à diverses mises en œuvre et caractéristiques, modes de communication (H.245, H.225, H.332, H.246) ou de profiles de sécurité (série H.235) nécessaires à la réalisation de la transmission de la voix.

7. H.323 v7 : H SERIES : *Audiovisual and multimédia systems ; Infrastructure of audiovisual services - Systems and terminal equipment for audiovisual services.*

Des vulnérabilités existent au niveau des protocoles liés à la téléphonie mais aussi à celui des logiciels de gestion des appels et des équipements eux-mêmes (téléphones IP mobiles ou non), ce qui affecte la sécurité des applications de téléphonie sur le réseau Internet. Aux vulnérabilités spécifiques s'ajoutent toutes celles liées aux infrastructures et aux protocoles d'Internet et la malveillance. Ainsi par exemple, les attaques en déni de service, en particulier, impactent la disponibilité des services de gestion des appels et de réalisation des communications, ce qui peut être très graves si l'on considère que la téléphonie doit obligatoirement permettre de joindre les **services d'urgence**.

Non seulement la voix sur IP nécessite du réseau des performances particulières notamment en termes de temps de réponse, délai, synchronisation des données, qualité de service, mais elle impose aussi qu'il puisse être en mesure de supporter les trafics relatifs aux appels vers les numéros d'urgence (pompier, police, etc.). Cela demande une **disponibilité** et une capacité de transport permanente de l'infrastructure (24h/24, 7 jours sur 7), ce qui, théoriquement, n'est pas garanti pour des applications de transmission de données en commutation de paquets IP. De plus, des routeurs, passerelles d'interconnexion ou des systèmes pare-feu peuvent considérablement altérer la qualité de la téléphonie en introduisant des variations de délais (gigue), en retardant les appels, en les bloquant, en détruisant ou perdant certains paquets par exemple. En fait, la téléphonie sur IP nécessite également des systèmes pare-feu ou de détection d'incidents spécialement adaptés à son support.

Des problèmes de performances peuvent survenir du fait que la téléphonie sur IP manipule divers types d'adresses (adresses IP assignées le plus souvent de manière dynamique, adresses MAC, adresses téléphoniques), qu'il existe, dans une architecture IP, des systèmes d'allocation dynamiques des adresses IP (serveur DHCP, *Dynamic Host Configuration Protocol*) et des convertisseurs d'adresses (NAT, *Network Address Translation*).

Du fait du caractère interactif et relativement « temps réel » du dialogue téléphonique entre deux ou plusieurs correspondants simultanément (notion de conférence téléphonique à plusieurs interlocuteurs), le réseau doit être en mesure de supporter ce type de flux apparenté à des flux multimédia.

Comme toutes les applications supportées par Internet, la téléphonie peut elle aussi subir les conséquences d'attaques ou de nuisances touchant l'infrastructure Internet. Le spam affectant la téléphonie sur IP (**SPIT**, *Spam over Internet Telephony*) est désormais courant, tout comme d'ailleurs l'est le spam ciblant les messageries instantanées (**SPIM**, *Spam over Instant Messaging*), pouvant non seulement convoyer des messages publicitaires non sollicités mais aussi des codes malveillants. Contrairement aux filtres antispams qui peuvent bloquer des spams relatifs à la messagerie électronique, il est beaucoup plus difficile de contrer le SPIT du fait de la notion de conversation en « temps réel ». Par ailleurs, les écoutes sont possibles via des analyseurs de protocoles, des outils de capture de paquets IP et des atteintes à l'intégrité des messages peuvent se réaliser par des attaques de type « *man in the middle* », le re-routage de paquets permet également d'intercepter des conversations téléphoniques...

9.3.2 Éléments de sécurité

Le chiffrement des données peut être effectué au niveau du protocole IP (en utilisant IPSec, mais cela ne permet plus de faire de la téléphonie à plusieurs) ou au niveau Transport. En effet, la mise en œuvre de la version sécurisée du protocole RTP (*Real-time Transport Protocol* [RFC 3550]), **Secure Real-time Transport Protocol** (SRTP, RFC 3711), permet le chiffrement des données transmises, l'authentification des messages, l'intégrité et la protection contre les attaques de type « rejet » des paquets IP, pour des flux unicast et multicast, y compris pour des communications sans fil.

Un paquet est rejoué lorsqu'il est stocké puis réinjecté dans le réseau, ce qui peut être évité avec l'authentification du message car chaque SRTP récepteur maintient une liste de paquets déjà reçus.

La version sécurisée du protocole *Real time Transport* (SRTP) peut également renforcer la sécurité du protocole RTCP (*Real-time Transport Control Protocol*, [RFC3350]). SRTP intègre aussi un service de gestion de clés de chiffrement et de génération de clés de session, à partir d'une clé maîtresse, qui peuvent être « rafraîchies » (changées) périodiquement, limitant ainsi la durée de vie d'une clé, ce qui augmente globalement la robustesse du système de chiffrement.

SRTP peut être utilisé pour supporter tous types de session multimédia et d'échanges de données, indépendamment du protocole de session (SIP ou H.323). Son usage n'est donc pas limité à la téléphonie et il existe différents profils de sécurité et variantes de sécurité.

Par ailleurs, l'IETF propose un **mécanisme de gestion de clés de chiffrement**, *Multimedia Internet Keying* (MIKEY [RFC 3830]), qui tient compte des besoins des applications multimédia (*streaming*, temps réel, unicast, multicast) et qui peut être mis en œuvre avec SIP ou STRP. Cela permet d'établir des associations de sécurité, éventuellement multiples, avec une négociation possible des clés de chiffrement et des paramètres de sécurité. MIKEY autorise l'authentification des utilisateurs selon trois options, à savoir : la distribution de clés symétriques, de clés asymétriques ou de signatures digitales via l'algorithme Diffie-Hellman.

Par défaut, ce sont les algorithmes AES/SHA-1 et les certificats X.509v3 qui sont mis en œuvre. La taille de la clé d'authentification est fixée également par défaut à 160 bits.

SIP est un protocole d'application de contrôle de la signalisation, spécifié par l'IETF (RFC 3261) pour créer, modifier et terminer des sessions entre un ou plusieurs participants pour supporter de la téléphonie, la distribution de contenus multimédia ainsi que des conférences multimédia. L'établissement d'une session SIP permet de négocier certains paramètres et passe par des serveurs proxy qui supportent, entre autres, l'enregistrement des utilisateurs, l'établissement des routes entre émetteurs et destinataires, l'authentification des utilisateurs et l'autorisation de l'accès aux services.

Souvent considéré comme plus simple que l'architecture H323, SIP est un protocole de niveau applicatif qui peut s'exécuter au-dessus de TCP, de TLS/SSL, d'UDP

ou de SCTP (*Stream Control Transmission Protocol* [RFC 2960]). TLS peut être mis en œuvre au-dessus de SCTP (RFC 3426) et également au-dessus de IPSec (RFC 3554). La RFC 3261 spécifie également les services de sécurité pour le protocole SIP.

Aux différents points d'une architecture SIP des mécanismes d'authentification peuvent être mis en œuvre, généralement sous la forme d'un « *challenge-response* », qui est une version améliorée du *digest* d'authentification HTTP (RFC 2617 (*HTTP Authentication : Basic and Digest Access Authentication*)). Cela fait intervenir un *nonce* (*number used once*), qui permet de calculer le *digest* (résumé) du mot de passe selon l'algorithme MD5 afin que le mot de passe ne soit jamais transmis en clair sur le réseau. Cela permet également d'éviter les attaques par dictionnaire ou de type rejet.

Les messages SIP peuvent inclure des messages MIME. Aussi la version sécurisée S/MIME peut être utilisée pour offrir des services de confidentialité et d'intégrité des contenus transférés, basés sur l'usage de certificats numériques. Pour protéger en plus les en-têtes SIP, il est proposé que les messages SIP soit véhiculés *via* des « tunnels » S/MIME (*tunneling* des messages SIP), ce qui alourdit considérablement les performances et fait que dans la majorité des usages, aucun service de sécurité n'est mis en œuvre pour supporter les dialogues téléphoniques.

Par ailleurs, des mécanismes additionnels de sécurité continuent à être régulièrement proposés au sein de l'IETF pour renforcer la sécurité des flux multimédia. Le chiffrement des données augmente leur taille et introduit des délais de traitement souvent incompatibles avec les exigences de qualité de service requises par des applications temps réel. Ainsi, force est de constater qu'en pratique, aucune sécurité n'existe, que la prise de contrôle à distance des ordinateurs « clients », comme l'interception des communications ou encore le détournement des capacités des systèmes et des réseaux, est une réalité qu'aucun mécanisme cryptographique ne peut empêcher. En effet, ces derniers peuvent être cassés ou contournés.

9.4 MÉCANISMES DE SÉCURITÉ DES APPLICATIONS INTERNET

9.4.1 *Secure Sockets Layer (SSL) – Transport Layer Security (TLS)*

SSL (*Secure Sockets Layer*) permet d'assurer la sécurité des échanges applicatifs indépendamment du protocole (figure 9.1)⁸. La majorité des navigateurs Internet intègre SSL, dont l'usage est transparent à l'utilisateur ; seul l'icône d'un cadenas fermé figure la mise en œuvre de SSL.

8. Il a été développé par Netscape (en collaboration avec plusieurs acteurs dont notamment Mastercard, Bank of America...).

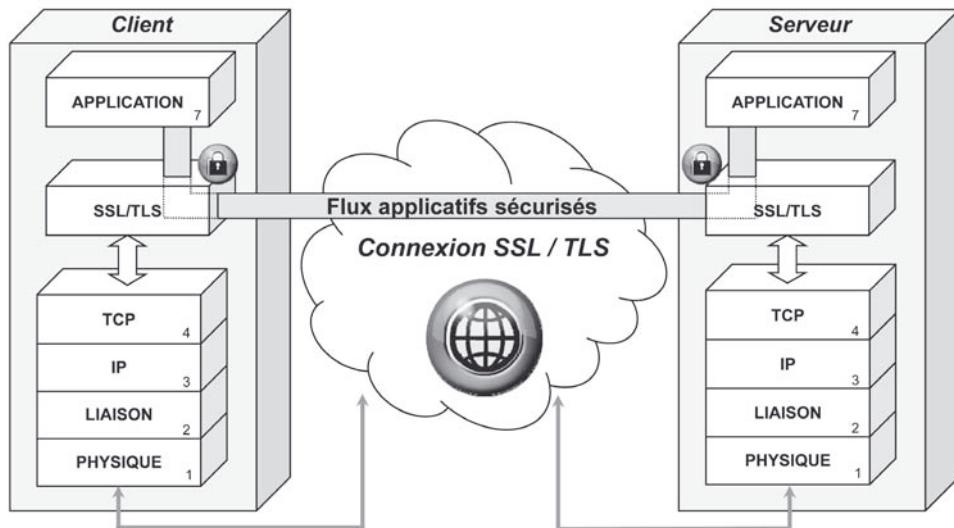


Figure 9.1 – La sécurité des flux applicatifs par SSL.

SSL permet de chiffrer les communications entre deux machines et d'assurer la confidentialité des données, l'authentification de l'utilisateur et du serveur, ainsi que l'intégrité des données par signature électronique (*via* des certificats numériques et la mise en œuvre du chiffrement asymétrique).

Le protocole SSL initialise une connexion logique avec une machine distante par un mécanisme dit de **poignée de main** (*handshake*). Les deux entités communicantes peuvent s'authentifier *via* une procédure et une autorité de certification (cf. chapitre 5). Le niveau de sécurité à appliquer au transfert est fonction des algorithmes de chiffrement et de la longueur des clés supportées par les deux entités communicantes.

Sur requête d'un client, un serveur renvoie un certificat, signé par l'autorité de certification, avec sa clé publique. Le client, en vérifiant la validité du certificat, authentifie le serveur, puis génère une clé de session, la chiffre avec la clé publique du serveur et lui envoie. Client et serveur peuvent alors chiffrer/déchiffrer les données avec la clé de session qu'ils sont seuls à connaître.

Les données transmises sont chiffrées et transmises *via* un canal de communication logique « SSL » qui opère entre les couches Application et Transport. SSL offre ainsi un service d'authentification du serveur (et éventuellement du client avec la version 3), de confidentialité et d'intégrité des données échangées⁹.

L'implantation de SSL a un fort impact du côté du serveur du fait de la certification. Cela implique un dialogue avec une autorité de certification reconnue et

9. Il a été démontré que SSL est vulnérable à des attaques de type « *man in the middle* » qui interceptent l'échange lors de l'établissement de la connexion sécurisée avec substitution du serveur.

demande également que les relais applicatifs des pare-feu supportent le mode de fonctionnement de SSL. La certification est parfois considérée comme un frein au déploiement de SSL.

Bien que SSL soit largement utilisé dans l'environnement web, SSL peut être invoqué indépendamment de celui-ci, ce qui contribue certainement à son adoption. Lors d'une transaction commerciale sur Internet, SSL peut, par exemple, sécuriser la transmission du numéro de carte de crédit entre client et vendeur. L'authentification du numéro de la carte de crédit reste à faire hors Internet.

SSLv3 a été repris et transformé par l'IETF pour donner **TLS** (*Transport Layer Security*)¹⁰. Le protocole **DTLS** (*Datagram Transport Layer Security*) en est l'équivalent en mode datagramme¹¹.

TLS offre des services de sécurité équivalents à ceux de SSLv3. La couche de transport sécurisée met en œuvre deux protocoles : **TLS Record Protocol** et **TLS Handshake** via le protocole TCP.

Le premier offre un service de connexion logique privée entre deux correspondants et sécurisée via un chiffrement symétrique (DES, RC4, etc.). La clé secrète est générée à chaque connexion par le protocole (de poignée de mains) *TLS Handshake*. Le protocole *TLS Record* supporte également un service de vérification d'intégrité via la mise en œuvre de fonction de hachage comme SHA ou MD5 par exemple.

Par ailleurs l'implémentation du **protocole SSH** (*Secure Shell*) autorise également un échange de données chiffrées et l'authentification d'un client et d'un serveur (notion de canal de transport sécurisé).

9.4.2 Secure-HTTP (S-HTTP)

L'extension au protocole HTTP, S-HTTP (*Secure HTTP*), offre un service de sécurité uniquement pour les flux de données HTTP. Il s'agit d'un protocole applicatif et non pas de transport (contrairement à SSL/TLS). Toutefois, **S-HTTP** offre de manière complémentaire, mais au niveau applicatif, les mêmes facilités de sécurité que SSL/TLS, avec les mêmes contraintes de certification. Cette solution, développée par le consortium CommerceNet, peut se trouver également implantée au niveau des navigateurs Internet. Un même serveur web peut supporter les protocoles S-HTTP et SSL/TLS, qui interviennent à différents niveaux de la communication. La sécurité d'une transaction peut alors être augmentée en invoquant les services de S-HTTP et de SSL/TLS, mais attention aux performances !

9.4.3 Authentification des applications

Répondre aux besoins d'**authentification des applications** communicantes via Internet est nécessaire pour effectuer des transactions de manière fiable. Être sûr d'une source et d'un destinataire (d'un client et d'un serveur) permet d'établir la confiance

10. TLS : RFC 2766 – <http://tools.ietf.org/html/rfc2766>

11. DTLS : RFC 5746 – <http://tools.ietf.org/html/rfc5746>

nécessaire à la réalisation d'une communication. Des protocoles cryptographiques, comme l'usage de certificats numériques, permettent de répondre à ce besoin.

9.5 SÉCURITÉ DU COMMERCE ÉLECTRONIQUE ET DES PAIEMENTS EN LIGNE

9.5.1 Contexte du commerce électronique

La question du **commerce électronique** (e-commerce) peut être envisagée sous l'angle de la problématique du commerce avec les **consommateurs** (*Business-to-Consumer*, B2C), ou celle **interentreprise** (*Business-to-Business*, B2B). On classera également dans la même catégorie les variantes associées par exemple à la **cyberadministration (e-administration)**. On parlera ainsi de commerce électronique entre le citoyen et les institutions publiques. Cette distinction peut avoir son importance, d'une part au niveau juridique puisque le droit commercial différencie en général les transactions interentreprises de celles opérées avec le consommateur et, d'autre part, au niveau de la problématique, car les transactions sont en général structurées différemment. Dans tous les cas, la sécurité est primordiale.

Le commerce électronique pose des problèmes de sécurité informatique semblables à ceux rencontrés avec les applications stratégiques d'une entreprise. Leurs résolutions emprunteront les mêmes voies méthodologiques, organisationnelles et techniques. De plus, il doit également être tenu compte du risque élevé de fraude. Des mesures anti-fraudes, qui peuvent être sous-traitées par des sociétés spécialisées, accompagnent généralement la mise en place de solutions de commerce en ligne.

9.5.2 Protection des transactions commerciales

La **protection des transactions commerciales** sur Internet repose sur une **démarche globale de gestion de la sécurité**, de protection des valeurs de l'entreprise et du consommateur, **de la maîtrise des risques**, et sur la mise en place de procédures et d'outils de sécurité du côté des clients et des marchands. Elle exige aussi la sécurisation du transfert de données entre le client et le serveur. La difficulté de mise en œuvre de solutions efficaces de sécurité provient du fait qu'elles doivent être à la fois d'ordre technologique, procédural, réglementaire, organisationnel, humain et managérial. Ces multiples facettes sont donc à intégrer de façon cohérente et doivent être acceptées et gérées efficacement par l'ensemble des acteurs intervenant dans une opération commerciale ou financière. Ces derniers sont nombreux, voire répartis au niveau international.

À l'heure actuelle, les technologies de la sécurité permettent de contribuer au déroulement correct d'une **transaction commerciale**, en assurant aux systèmes informatiques les capacités à :

- pouvoir être utilisés (disponibilité des services, des ressources matérielles et logicielles) ;

- ne permettre l'accès aux données et aux ressources informatiques qu'aux personnes et aux processus informatiques habilités (confidentialité, intégrité des données et des services) ;
- prouver que des actions, événements, transactions ont bien eu lieu (traçabilité, preuve, non-répudiation) ;
- exécuter les actions et rendre les services attendus dans des conditions de performance et d'utilisation adaptées (continuité de service, sûreté de fonctionnement, fiabilité, convivialité).

9.5.3 Risques particuliers

Les problèmes de sécurité se posent au niveau du client, du réseau et du site informatique de l'entreprise commercialisant des produits ou des services sur Internet.

Les **risques encourus par le client** sont relatifs à la divulgation d'informations confidentielles ou d'ordre privé et à leur usage illicite (fichage, détournement, usurpation d'identité, etc.), au leurre et à l'infection virale. D'autre part, il faut ajouter ceux liés aux escroqueries et à la non-livraison de produits commandés et payés (produit contrefait, ne correspondant pas à la commande, etc.).

D'un point de vue purement informatique, un **risque majeur pour l'entreprise** est celui de la pénétration de son environnement informatique à partir de son site marchand Internet, autorisant toute une série de malveillances (vol, destruction, détournement, etc.). Cela peut engendrer des pertes financières, d'exploitation, de production, d'image et de savoir-faire qui peuvent être importantes, pouvant aller jusqu'à mettre en péril la compétitivité et la survie d'une entreprise. Le risque de détérioration de réputation et d'image par défiguration de site web est considéré comme grave, il doit donc également être pris en considération. Toutefois, les risques de fraudes et d'escroqueries sont pour le commerçant et la banque vraiment préoccupants. Ils nécessitent des mesures de contrôle et de validation parfois lourdes à mettre en place.

9.5.4 Sécuriser la connexion entre l'acheteur et le vendeur

En fait, assurer la sécurité des transactions commerciales revient souvent à sécuriser la **connexion Internet entre le client et le vendeur**, en négligeant parfois de sécuriser le poste client lui-même et de renforcer la sécurité de l'environnement informatique du vendeur.

Comme nous l'avons vu précédemment, une connexion Internet peut être établie de manière sécurisée entre un navigateur et un serveur web via l'usage de SSL/TLS. Cela assure de façon transparente pour l'utilisateur, le chiffrement des données et l'authentification du serveur. Ainsi, un niveau de sécurité suffisant est atteint pour transmettre, par exemple, un numéro de carte de crédit sur le réseau. En fait, le risque pris alors par le client n'est pas plus grand que celui qu'il prendrait dans le monde réel en payant avec sa carte de crédit, mais cela ne répond pas aux problèmes d'usages frauduleux de cartes de crédits ou de fausses cartes.



Rendre uniquement confidentiel la transmission d'un numéro de carte de crédit n'est pas suffisant pour protéger la transaction commerciale. Il faut que les informations sensibles le soient tout au long de la chaîne de traitement et de leur durée de vie.

Le vendeur doit assurer la confidentialité des données lors de leur stockage et durant les **demandes d'autorisation de paiement**. Celles-ci peuvent être réalisées manuellement par fax (qui n'est pas sécurisé) ou en ligne *via* Internet par le biais de connexions sécurisées également par SSL/TLS.

Les principaux opérateurs de cartes de crédit (Visa, MasterCard, American Express) et de nombreux acteurs du monde Internet ont tenté de promouvoir le déploiement de **SET** (*Secure Electronic Transaction*), qui ne s'est jamais réellement imposé et qui, depuis 2008, a été remplacé par des alternatives permettant de mieux contribuer à limiter les fraudes liées à de fausses cartes de crédits ou à des cartes volées, par le groupe Visa par la solution **3-D Secure** (service « *Verified by Visa* ») et par le groupe MasterCard par « *MasterCard SecureCode* »¹².

Lors de l'achat en ligne par carte de crédit, le site marchand demande à la banque de l'internaute-acheteur d'authentifier celui-ci afin de s'assurer que l'achat est réellement émis par le détenteur de la carte et que la carte est bien réelle. Cela reporte la responsabilité de l'authentification sur la banque du consommateur, qui doit être en mesure de recourir à des solutions d'authentification robustes. Ainsi, la sécurité des achats est renforcée si le détenteur de la carte est inscrit à un service « *Verified by Visa* » ou « *MasterCard SecureCode* », qui utilise Internet et un canal de communication séparé, comme le téléphone portable, pour obtenir un code à usage unique que l'usager doit fournir pendant la procédure de paiement en ligne.

9.5.5 Sécurité des paiements en ligne

Caractéristiques

Bien qu'il ne faille pas restreindre la notion de commerce électronique au paiement en ligne, celui-ci constitue souvent le facteur de risque prépondérant.

Dans le domaine du **commerce électronique interentreprises**, rappelons que l'essentiel des transactions est réglé par des moyens de paiement traditionnels, par virement bancaire par exemple. Certaines entreprises travaillent aussi en **EDI** (*Electronic Data Interchange*). On observe également le déploiement dans le marché de solutions de présentation électronique des factures (**EBPP**, *Electronic Bill Present-ment and Payment*). Dans ces architectures, la facture est dématérialisée et peut être transmise à la banque du client. Celui-ci peut alors la consulter en ligne et en valider le règlement *via* une interface de **e-banking**. Le paiement se fait par virement direct de banque à banque.

Dans le domaine du **commerce électronique avec le consommateur**, le mode de paiement préférentiel est celui par **carte de crédit**, qui est très répandu en termes à

12. Au Japon, la compagnie JCB (*Japan Credit Bureau*) supporte la solution **J/Secure**.

la fois de nombre de cartes en circulation mais aussi en termes de nombre d'entreprises déjà autorisées à recevoir des paiements par carte, que ce soit en présence du client ou par téléphone. Sur Internet, comme dans la vente à distance, la transaction commerciale est réglée sur présentation des informations indiquées sur la carte. Il s'agit du numéro de la carte, du nom du titulaire, de la date d'expiration (mois/année), du nombre figurant au verso de la carte et du type de carte. Ces informations doivent être traitées de façon confidentielle, c'est pourquoi les sites de commerce sécurisent la communication avec leurs clients, le plus souvent par une connexion SSL/TLS. Dans la plupart des cas, le compte du client est débité immédiatement, néanmoins le vendeur peut aussi réserver un certain montant sur la carte, pour le débiter ensuite, par exemple lors de l'expédition des produits.

Mode opératoire

Le **principe de fonctionnement** du paiement est très simple. Le vendeur qui a préalablement passé un contrat de type vente à distance avec les sociétés émettrices des cartes de crédit établit un autre contrat avec un opérateur de passerelle de paiement. Une fois ces éléments contractuels établis, le vendeur dispose d'un accès sécurisé à des **interfaces applicatives** (API ou service web) permettant de réaliser différentes opérations comme le paiement, la réservation d'un montant ou la vérification de la carte. Le vendeur construit une application web capable de demander les informations sur la carte en mode sécurisé à l'acheteur. Il récupère ces informations et appelle ensuite, en mode sécurisé, l'interface applicative proposée par la passerelle de paiement. Il lui transmet les paramètres de la transaction (information sur la carte, montant et devise). La passerelle exécute la transaction et renvoie un code permettant de prouver que la transaction a bien eu lieu. En cas de problèmes (insolvabilité, carte bloquée, informations incorrectes, etc.), la passerelle renvoie un code d'erreur que l'application devra gérer.

Certaines passerelles proposent aussi un mode de fonctionnement dans lequel l'utilisateur est en fait **redirigé sur leur site web** dès lors qu'il s'agit d'exécuter le paiement. L'avantage de cette solution en termes de sécurité est que le vendeur n'aura pas connaissance des informations liées à la carte de crédit. Il s'affranchit ainsi des risques associés au stockage de ce type d'information (et au piratage éventuel de cette base). La limite de ce système est qu'en général la conception de l'application de paiement diffère de celui du site du commerçant. En termes de communication et d'image, ce changement de design n'est pas idéal car il peut inquiéter le client utilisateur.

Les opérateurs de carte ont ajouté un code, le **CVV (Card Verification Value Code)**, de trois ou quatre chiffres imprimés sur la carte. À la différence des autres informations présentes sur la carte, il n'est pas en relief et n'est donc pas reproduit sur les facturettes. Les opérateurs dénomment ce code de différentes façons : CVV2 chez Visa, CVC2 chez MasterCard, et CID chez American Express. Il s'agit d'un cryptogramme visuel de sécurité qui se trouve au resto ou au verso de la carte afin de s'assurer que seul le détenteur de la carte physique est en mesure de lire cette information. Ainsi, si un

fraudeur possède uniquement le numéro de la carte et sa date de validité, il ne sera pas autorisé à finaliser la transaction.

Les opérateurs ont également rédigé des recommandations vis-à-vis des vendeurs en ligne. Ces meilleures pratiques, comme par exemple celles exprimées par le « *Payment Card Industry - Data Security Standard* »¹³, permettent, si elles sont respectées, d'améliorer la sécurité des paiements par carte de crédit.

Certains opérateurs ont également développé des **processus d'audit** permettant de contrôler la sécurité des infrastructures mises en place par les vendeurs.

Ainsi par exemple, le programme *Verified by Visa* prévoit l'enregistrement des données relatives à la carte de crédit chez Visa. Ces données sont associées à un nom d'utilisateur et à un mot de passe. Les vendeurs ayant adhéré à ce programme acceptent des paiements par carte de crédit sans toutefois manipuler les données de la carte. Celles-ci restent chez l'opérateur émetteur de carte. Elles y sont protégées par le mot de passe de l'utilisateur. Ce nouvel élément que le porteur « connaît » est essentiel, car il ne figure pas sur la carte. S'il devait se généraliser, il permettrait d'éviter qu'un tiers trouvant ou dérobant une carte ne puisse s'en servir pour réaliser des achats en ligne. Afin de motiver les vendeurs, Visa couvre les problèmes de défaut de paiement sur les transactions réalisées dans le cadre de ce programme. Cet incitatif commercial devrait pousser l'adoption de ce système.

En marge des systèmes de paiement par carte de crédit, le système de paiement électronique ayant réussi à percer sur le marché est celui mis en place par la société PayPal, du groupe eBay¹⁴. Cette solution est une des rares permettant le **micropaiement** et les **transactions entre consommateurs**. Quand bien même la diffusion de Paypal n'est pas comparable à celle des cartes de crédit, PayPal s'appuie sur des moyens de paiement existants, notamment les cartes de crédit, les cartes de débit et les comptes bancaires. La solution offre l'avantage de ne pas divulguer les informations de paiement au vendeur. Remarquons que dans la mesure où les informations sensibles des clients se situent sur les serveurs Paypal, ces derniers font l'objet d'attaques...

Google offre un service de paiement en ligne, « **Google Wallet** », proche de PayPal. Ces développements devraient contribuer à démocratiser encore plus les paiements en ligne.

Par ailleurs, des solutions de paiement sur Internet, à partir du téléphone portable (**m-paiement**) se développent, comme également celles qui reportent les montants dépensés sur Internet sur la facture de l'opérateur Internet de l'acheteur.

9.5.6 Sécuriser le serveur

Sécuriser le serveur revient à contrôler les requêtes qui lui sont adressées et à renforcer la sécurité de la plate-forme matérielle et logicielle mais aussi celle du système d'information avec lequel il collabore pour rendre le service sollicité par les

13. https://www.pcisecuritystandards.org/pdfs/pci_dss_v1-1.pdf

14. www.paypal.com ; www.ebay.com.

clients. Au-delà de la stricte configuration de la machine appelée à héberger le serveur, il est généralement recommandé de protéger les environnements de support au commerce électronique par des mesures de cloisonnement et de détection d'intrusion telles que présentées au chapitre 8.

Protéger les données consiste aussi à en limiter les accès et à les rendre disponibles. Ce dernier point est important et relève plus du génie logiciel, de la gestion des configurations et des sauvegardes (*back-up*), du dimensionnement et de la redondance des serveurs, des capacités du réseau, de la gestion de réseau que des outils de sécurité à proprement parler.

On peut également considérer que tous les aspects liés au support des utilisateurs en interne chez le commerçant, mais aussi à l'aide aux clients (support téléphonique, *hot line*) font partie de la sécurité du serveur, comme d'ailleurs sa conception, son ergonomie, sa convivialité et sa facilité d'utilisation.

9.5.7 Notions de confiance et de contrat dans le monde virtuel

Confiance

La confiance est à la base de tout échange. Dans le cyberespace, elle peut être accréditée par des organismes tiers, offrant des services d'enregistrement et de certification à l'image des notaires. Ces tiers de confiance ou autorités de certification (cf. chapitre 5) sont habilités à délivrer des certificats qui permettent, entre autres, de garantir à un destinataire que la signature électronique d'un document reçu a bien été réalisée par le supposé émetteur. Ainsi, le rôle, le statut et la responsabilité de ces organismes de certification, qui interviennent comme garants dans une transaction commerciale, sont des facteurs déterminants du succès du commerce électronique sur Internet. En effet, c'est sur eux que repose toute l'authentification d'une transaction commerciale.

Contrat

Au-delà des aspects organisationnel et technique liés à la mise en place de toutes activités commerciales, il est important de pouvoir **matérialiser la notion de contrat** lors d'échanges commerciaux électroniques. Dans le monde immatériel, l'information transmise, qu'elle soit relative à la déclaration de volonté amenant à la conclusion d'un contrat, ou qu'elle soit le bien lui-même, constitue un bien juridique dont la diffusion et l'appropriation doivent être juridiquement réglées.

Droit de révocation

La facilité avec laquelle il est possible d'effectuer des achats sur Internet peut favoriser des comportements de consommation relevant d'une décision irréfléchie. Dans ce contexte, le droit de révocation prend une grande importance. Au niveau européen, c'est la directive 1997/7 du 20 mai 1997 qui régit le droit de révocation. Il est stipulé que pour tout contrat à distance, le consommateur dispose d'un délai d'au

moins sept jours ouvrables pour se rétracter sans pénalités et sans indication du motif. Au cas où le fournisseur n'a pas rempli les obligations visées à l'article 5, notamment les modalités du droit de rétraction, le délai est de trois mois.

En cas de litige

Dès lors qu'un contrat est valablement conclu, la question de la preuve se pose lors de litige, qu'il s'agisse d'Internet ou non : il est nécessaire d'apporter des preuves. Ainsi, il est toujours judicieux de garder des traces de la transaction (copie d'un message électronique, copie d'écran, etc.). Les lois nationales relatives au commerce spécifient quels sont les types de documents admissibles auprès d'un tribunal comme moyen de preuve.

Si les contrats comportent des conditions générales, elles doivent être facilement accessibles, consultables en ligne, et le client doit être clairement informé qu'elles font partie du contrat.

Le concept d'ODR (*On-line Dispute Resolution*) est issu de cette volonté de pouvoir trouver des solutions immédiates à des conflits liés au non-respect de contrats passés *via Internet*. Cela constitue une alternative au dépôt de plainte devant des tribunaux, démarche qui peut être longue et complexe du fait de la nature souvent internationale du commerce électronique. Ce type de résolution des litiges se base sur la capacité de conciliation des entités en litige et s'appuie sur les notions de négociation, de médiation et d'arbitrage. En principe, cela est plus rapide, plus accessible financièrement et convivial pour les internautes. En revanche, du fait que cela se base sur des **codes de conduite** ou des recommandations qualifiées de « *soft law* », leur force contraignante est limitée. La majorité des services de paiement en ligne comme ceux précédemment cités proposent des mécanismes de résolution de conflits en ligne.

9.6 SÉCURITÉ DES DOCUMENTS XML

9.6.1 Risques et besoins de sécurité liés à l'usage de documents XML

La navigation web est possible du fait de l'implémentation du protocole HTTP (*HyperText Transfert Protocol*), mais aussi parce que les documents appréhendés sont construits de manière à autoriser de multiples contenus de nature multimédia, marqués et reliés entre eux par des liens logiques (liens hypertextes). Ces documents hypertextes sont conçus, architecturés et structurés, en utilisant le langage de marquage XML (*eXtended Markup Language*). Il s'agit d'un métalangage de marquage, qui permet de décrire la structure logique et le contenu d'un document, défini par le W3C (*World Wide Web Consortium*)¹⁵. Il constitue une amélioration du langage HTML (*HyperText Mark-up Language*), issu du langage SGML (*Standard*

15. <http://www.w3.org/XML/>

Generalized Markup Language). Il a été normalisé à l'ISO au milieu des années 1980 et est largement utilisé dans le monde de la gestion électronique de documents.

Ce qui rend XML si puissant (données structurées et sémantiquement enrichies, format textuel, balisage) pose des problèmes de sécurisation de documents XML. En effet, comment appliquer des procédés de chiffrement ou de signature électronique, pour rendre confidentiel des contenus ou authentifier des auteurs, sur des documents multiparties, potentiellement réalisés par divers auteurs¹⁶ ?

En fait, deux possibilités existent, à savoir :

- **XML Signature** [xmlsig]¹⁷ qui a été conjointement conçu par le W3C (*World Wide Web Consortium*) et l'IETF (*Internet Engineering Task Force*) ;
- **XML Encryption** [xml-encryption]¹⁸ qui est une recommandation du W3C.

9.6.2 Signatures XML

Caractéristiques

Comme toute signature numérique, la **signature XML** permet d'offrir des services d'**authentification du signataire et/ou du message** et d'**intégrité**. La signature XML peut s'appliquer sur un document dans son intégralité ou sur une partie de celui-ci, sur tous les types de données décrites et aussi sur le code XML utilisé.

Lorsqu'un document XML est composé de différentes parties élaborées par divers auteurs, chacun peut signer uniquement la partie qui le concerne. Cette flexibilité peut toutefois être problématique, comme par exemple lorsqu'un formulaire XML est signé par son concepteur puis donné à un utilisateur pour être complété et signé par ce dernier. Si la première signature se rapporte à la totalité du formulaire XML, tout changement introduit par l'utilisateur l'invalidise. En fonction de l'application du procédé de signature, **XML Signature**, et la manière dont la signature est incluse ou attachée au document, il est distingué plusieurs types de signature.

La **signature** est dite **enveloppée** ou **enveloppante** lorsqu'elle porte sur des données du même document XML que la signature. En revanche, la signature est dite **détachée** lorsqu'elle opère sur des ressources réseaux externes ou des objets locaux de données qui résident dans le même document XML en tant qu'éléments voisins. Dans ce cas, la signature n'est ni enveloppante (la signature est parente) ni enveloppée (la signature est enfant), elle est détachée. La validation de la signature nécessite que les données signées soient accessibles. La signature elle-même indique généralement la localisation de l'objet signé : par un URI (*Unified Ressource Identifier*) dans la

16. Les paragraphes concernant la sécurité des documents XML ont été écrits en collaboration avec Sarra Ben Lagha.

17. [xmlsig] *XML-Signature Syntax and Processing*, IETF/W3C Recommandation. Eds. Donald Eastlake, Joseph Regale and David Solo. 12 February 2002. <http://www.w3.org/TR/2002/REC-xmlsig-core-20020212> et <http://www.ietf.org/rfc/rfc3275.txt>

18. [xml-encryptionVf] *La syntaxe et le traitement du cryptage XML*. Recommandation W3C. D. eastlake et J. Reagle. 2002. <http://www.w3.org/TR/2002/REC-xmlenc-core-20021210>

signature, ou par un identificateur de fragment de document dans le même document, ou encore en étant parent ou enfant de l'élément signé.

La spécification XML Signature définit un **type d'élément** de signature XML et une **application** de signature XML, ainsi que les critères de conformité pour chacun d'eux. Elle définit aussi des méthodes pour référencer des ensembles de ressources, d'algorithmes et d'instructions pour la gestion des clés.

Composants d'une signature XML

Le contenu à signer (*Data Objects*) est prétraité (condensé par une fonction de hachage) et la valeur obtenue est placée dans un élément (avec d'autres informations). Cet élément est par la suite prétraité et signé cryptographiquement.

Les signatures numériques XML sont représentées par l'**élément Signature**, qui possède la structure suivante :

```
<Signature ID_?> - élément optionnel
<SignedInfo>
  <CanonicalizationMethod/>
  <SignatureMethod/>
  (<Reference URI_?> - élément optionnel
   (<Transforms>) ?- élément optionnel
   <DigestMethod> - identification de l'algorithme de
   chiffrement générant le digest
   <DigestValue> - valeur du digest
   </Reference>)+- élément répétable
  </SignedInfo>
  <SignatureValue> - valeur de la signature
  (<KeyInfo>) ? - clé publique du signataire, élément optionnel
  (<Object ID_?>)* - élément optionnel et répétable
</Signature>
```

Mode opératoire, création et validation de signatures XML

La **production d'une signature XML** se base sur l'usage d'empreintes numériques (*digests*) tel que présenté au chapitre 5 et se présente schématiquement de la manière suivante :

1. Collecte des données à signer.
2. Calcul de l'empreinte (*digest*) de chaque ressource, à laquelle on associe un élément *Reference*.
3. Assemblage des éléments *Reference* dans un élément *SignedInfo* (avec l'algorithme à utiliser).
4. Calcul de la signature à partir d'un algorithme asymétrique et de la clé privée du signataire.
5. Rajout éventuel de la clé publique du signataire.
6. Encapsulation de tous ces éléments dans un élément *Signature*.

La vérification de l'intégrité et de l'authenticité d'un document XML se fait en recalculant la valeur du *digest* global de l'élément *SignedInfo* et celles de chaque *digest* de chaque référence et en les comparant avec les valeurs initiales.

Deux phases de validation, celle de la signature et celle de la référence, sont nécessaires à la validation globale de la signature. En effet, la validation de la signature de l'élément *SignedInfo* s'effectue à partir du recalcul du *digest* de l'élément *SignedInfo*, en utilisant les algorithmes spécifiés dans *canonicalizationMethod* et *SignatureMethod*, et en utilisant la clé publique du signataire afin de vérifier que la valeur de l'élément *SignatureValue* correspond au *digest* de l'élément *SignedInfo*. Le recalcul de l'empreinte numérique (valeur du *digest*) de chaque *Reference* incluse dans l'élément *SignedInfo* et la comparaison avec la valeur de l'élément *DigestValue* (contenu dans l'élément *Reference*) permet de valider la référence.

9.6.3 Chiffrement/déchiffrement XML

La recommandation [**xml-encryption**] du W3C a pour objectif de permettre le chiffrement de données XML. Elle définit des processus pour chiffrer et déchiffrer les contenus, et une syntaxe XML pour représenter les contenus chiffrés et les informations permettant le déchiffrement par le destinataire concerné.

Des opérations de signature XML et de chiffrement XML peuvent toutes deux être réalisées sur un document XML à n'importe quel moment et dans n'importe quel ordre. Ainsi, les opérations de chiffrement, qui sont effectuées après une opération de signature sur une partie du contenu déjà signée, rendent la signature invérifiable. Il est alors nécessaire de déchiffrer les parties chiffrées après signature, avant que la signature ne soit vérifiée. Pour cela, le W3C a proposé une recommandation de transformation de décryptage [**xmldec**]¹⁹ qui fournit un mécanisme de déchiffrement des seules parties signées puis chiffrées (tout en ignorant celles chiffrées puis signées). C'est une transformation destinée à apporter une solution au problème de l'ordre de déchiffrement/vérification à l'intérieur des ressources signées.

9.7 MARQUAGE DE DOCUMENTS ET DROITS NUMÉRIQUES

9.7.1 Tatouage numérique

Bien qu'il existe des mécanismes de sécurité pour assurer la confidentialité et l'intégrité des données, peu existent pour les protéger de la copie, de la distribution abusive ou illicite, pour éviter la contrefaçon, le plagiat, les atteintes au droit d'auteur ou le vol de propriété intellectuelle par exemple. Les techniques de **marquage** (*watermarking*) ou encore de **tatouage**) répondent à ces besoins. Elles sont apparues au début des années 1990, principalement pour le marquage des images numériques. Leur usage s'est étendu depuis à l'estampillage de données audio et vidéo, puis, dans une plus faible mesure, aux programmes informatiques.

19. [**xmldec**] Transformation de décryptage pour XML Signature. Recommandation du W3C. Eds. Merlin Hughes, Takeshi Imamura et Hiroshi Maruyama. 10 décembre 2002. <http://www.w3.org/TR/2002/REC-xmlenc-decrypt-20021210>

Le concept de base du **tatouage** repose sur la possibilité de pouvoir insérer de manière inaltérable, indélébile et souvent imperceptible, dans les données du propriétaire, une séquence d'information spécifique (notion d'empreinte, de signature) afin de les marquer (*fingerprinting*). Issu du domaine d'application de la **stéganographie**, qui consiste à cacher à une information en clair dans une autre information en clair, le tatouage insert une marque fortement liée aux données dans lesquelles elle est intégrée. La marque peut alors être visible ou non.

Outre le fait qu'un tatouage permet de lier un propriétaire à un document numérique afin de pouvoir réaliser une gestion des droits d'auteurs, contrôler la distribution des contenus, le tatouage peut également intervenir pour assurer l'intégrité des documents ainsi que leur indexation. Le chiffrement des données mis en œuvre pour tatouer un document permet de prévenir d'une modification non autorisée ou d'indiquer que les données ont été modifiées sans autorisation. De plus, le tatouage permet d'intégrer une restriction à l'utilisation du document (le brouillage du document est effectué après un certain nombre de lectures ou à l'expiration de la date de validité par exemple). Parfois, le tatouage peut également avoir un effet dissuasif, il n'a pas besoin d'être dans ce cas indétectable. Sous certaines conditions, le tatouage peut servir à reconstituer le document auquel il est associé ou être utilisé pour marquer des contenus « mobiles ».

Le frein majeur au déploiement du tatouage réside dans le manque de standards et dans le fait de la nécessité de disposer d'une plate-forme matérielle et logicielle en mesure d'écrire et de lire une marque. Le concept de marquage, tatouage, étiquetage de documents a permis le développement des savoir-faire en matière de gestion des droits numériques (DRM, *Digital Rights Management*).

9.7.2 Gestion des droits numériques

La gestion des droits numériques, DRM (Digital Rights Management)²⁰, est une question d'ordre économique, légal et technologique. Elle concerne tous les acteurs de la chaîne « producteurs-consommateurs » de contenus notamment les utilisateurs, les auteurs, les fournisseurs et distributeurs de contenus au sens large (industrie du divertissement, organisations, etc.).

Elle s'inscrit dans un cadre réglementaire et légal déterminé et relatif, entre autres, à la protection du droit d'auteur, de la propriété intellectuelle et au téléchargement qui répond au besoin de protection des valeurs de certains acteurs qui dépendent de modèles économiques particuliers.

Pour une organisation, la gestion des droits numériques s'appuie sur une politique donnée et la mise en œuvre de techniques cryptographiques et de contrôle des usages. Cela peut être conditionné en fonction des périphériques d'accès, de lecture et de stockage de contenus, des techniques de compression des données ou encore, par exemple, de l'usage des réseaux *peer-to-peer*. Toutefois, le principe de gestion

20. Le paragraphe sur la gestion des droits numériques est réalisé avec la collaboration de Jean-Henri Morin.

des droits numériques repose toujours sur la capacité à définir pour chaque contenu, qui peut être chiffré, des **règles d'usage** qui doivent être respectées au point de consommation du contenu et sur des moyens de **contrôle d'accès** autorisés conditionnellement. Les technologies de support à la gestion des droits numériques contribuent à sécuriser les contenus de manière persistante, c'est-à-dire en dehors même des frontières où l'objet numérique a été créé et mis à disposition et indépendamment de sa localisation.

Pour lutter contre la copie illégale de contenus, des règles DRM peuvent s'appliquer à tous types de contenus (fichiers texte, tableurs, messages électroniques, musiques, films, etc.) et de circonstances d'utilisation (copie possible mais seulement un certain nombre de fois, selon une date d'expiration donnée, sur un type de périphérique déterminé, etc.).

La notion de **protection persistante** sous-tend le concept de **superdistribution**, qui permet de copier et de distribuer légitimement tout contenu sans aucune limitation. Les contraintes, les exigences de sécurité sont exprimées par des règles formulées dans un langage ayant un fort pouvoir expressif afin de pouvoir formuler des règles complexes.

Le client doit disposer d'un module DRM (*enforcement point*) qui doit être résistant aux attaques, capable d'interpréter les règles associées au contenu. Une interface de restitution « de confiance » afin de restituer le contenu est également nécessaire, comme le sont des entités tierces, pas forcément de confiance, mais auprès desquelles le module de DRM peut s'adresser pour obtenir des licences, renouvellements, ou simplement des règles de bases qui auraient été volontairement dissociées du contenu afin d'en garder une parfaite maîtrise.

Le scénario général du **mode opératoire des DRM** se décompose en quatre étapes principales :

1. La préparation du contenu consiste pour le détenteur à « encapsuler » de façon sécurisée et persistante le contenu avec les règles qui vont gouverner son utilisation. Les règles peuvent être acheminées séparément du contenu selon les besoins.
2. La distribution du contenu, incluant la superdistribution, concerne la distribution du contenu préparé à l'étape précédente par n'importe quel moyen (www, CD, e-mail, ftp, streaming, etc.).
3. L'utilisation du contenu est l'étape où un client souhaite accéder au contenu en respectant les règles qui y sont attachées. L'accès au contenu n'est accordé que si ces règles ont été interprétées avec succès, permettant ainsi le déchiffrement et la restitution du contenu. Cette étape met souvent en œuvre un intermédiaire externe (serveur de licences) chargé d'émettre des licences d'utilisation et de récolter les informations financières pour les ayants droit. Notons au passage le rôle particulier de cet acteur pouvant par le simple fait de son activité récolter des informations précieuses à destination des départements marketing des détenteurs de contenu.

4. Finalement, le traitement des transactions permet une répartition auprès des ayants droit des compensations financières selon les informations et mesures effectives d'usage collectées.

La protection de l'information repose encore aujourd'hui essentiellement sur la définition de périmètres statiques de sécurité *via* des pare-feu et sur des procédures de contrôle d'accès et de chiffrement. Or, du fait des supports de **mémorisation amovibles** (clés USB, CD, DVD, etc.) et des **systèmes portables** (PDA, portables, etc.), les données quittent les frontières traditionnelles de l'entreprise et, souvent, ne sont plus protégées correctement par les mesures de sécurité en vigueur au sein de son système d'information.

Dorénavant, les données appartenant à l'organisation existent en dehors de ses frontières et persistent également dans le temps (du fait de copies multiples existant sur des supports amovibles). Elles sont rarement restituées à leur propriétaire, même après le départ des employés de l'entreprise. Dès lors, le rapport qui s'établit entre l'organisation et ses employés est un rapport de confiance qui ne peut être contrôlé et maîtrisé par l'institution. Ce simple **rappo~~rt~~t de confiance** n'est plus suffisant en regard de la nature stratégique de l'information et du **risque informationnel** encouru par l'organisation.

Les politiques relatives à l'usage des données de l'organisation, visant au contrôle de l'usage des données selon une attitude responsable vis-à-vis de la gestion du capital informationnel et des valeurs liées à la propriété intellectuelle de l'organisation, peuvent être instrumentalisées par des **technologies DRM**. Si ces dernières sont bien conçues, gérées, mises en œuvre et appliquées systématiquement, elles contribuent à réduire les risques d'erreurs de manipulation non autorisée des données.

La gestion des politiques électroniques devient alors un projet stratégique qui s'intègre dans celui de la gestion de la sécurité, clairement identifié dans la politique de sécurité d'une organisation.

9.8 LE BYOD, LES RÉSEAUX SOCIAUX ET LA SÉCURITÉ

Le phénomène **BYOD** (*Bring Your Own Device*)²¹, qui autorise l'usage de moyens d'accès personnels à l'information de l'organisation (téléphones intelligents, tablettes, etc.), sur le lieu de travail, ou ailleurs, peut paraître attractif au premier abord. En effet, l'employeur n'a pas à financer l'outil de travail ; l'employé utilise les outils qu'il a lui-même choisis, souvent performants, personnalisés et de dernière génération. Cette approche complète les applications et les services que le service informatique ne propose pas et qui permettent aux utilisateurs d'être plus mobiles et efficaces dans leur mission.

Toutefois, cela pose des problèmes de sécurité difficilement maîtrisables par l'organisation, les données étant hors du périmètre traditionnel de celle-ci et de son contrôle. Les risques sont essentiellement relatifs à la fuite d'information

21. Ce paragraphe est réalisé avec la collaboration de Arnaud Dufour.

consécutive à la perte ou au vol de l'équipement (*information leakage*) et à l'intrusion et à l'infection des systèmes de l'organisation²². Cela constitue de nouvelles menaces pour lesquelles il n'existe pas vraiment de contre-mesures spécifiques hormis celles liées à la définition, dans la politique de sécurité, de règles interdisant, ou éventuellement définissant et limitant le type d'usage, de données, d'applications et d'interconnexions possibles au système d'information de l'entreprise, à partir d'équipements privés. Cela doit être accompagné par des mesures de sensibilisation et d'éducation et de chiffrement des données sensibles sur l'équipement personnel ainsi que sur des mesures de surveillance et de contrôle. Une alternative à la vague « BYOD » serait que l'infrastructure informatique de l'organisation soit en mesure d'offrir des services et des moyens d'y accéder peut-être plus appropriés aux besoins des employés en y intégrant des mesures de sécurité adaptés. En fait, le phénomène BOYD ne fait que souligner la difficulté de protéger un système d'information sans frontières physiques, comme cela est déjà le cas avec l'usage de la messagerie électronique et des services de cloud computing (cf. chapitre 6).

Pour répondre aux préoccupations des organisations, des solutions de **gestion de flottes de mobiles** (*Mobile Device Management*, MDM) ont été développées par les fournisseurs. Pour autant, il faut encore que l'employé soit d'accord de voir l'entreprise imposer ces éléments sur son appareil qui contient également des données personnelles²³. Par ailleurs, certains employés n'hésitent pas à recourir à des services de Cloud personnels, y compris pour des applications dans le cadre professionnel²⁴. Cette nouvelle manière de travailler et d'utiliser des ressources autres que celles de l'organisation « UYOCs » (*Use Your Own Cloud Service*) représente de nouvelles menaces et constitue un véritable enjeu de la maîtrise de la sécurité des données.

L'usage de mobiles génère des risques spécifiques. Plusieurs scénarios ne manqueront pas de se concrétiser, soulevant des défis juridiques et techniques additionnels, comme le fera certainement à l'avenir l'usage des lunettes *Google Glass* et autres objets communicants.

De manière analogue, parmi les nouveaux usages et comportements pouvant mettre en danger la sécurité d'une organisation retenons ceux liés à l'emploi des **r  seaux sociaux**. En effet, ils constituent une source d'information exploit  e (phase d'ing  nierie sociale d'une cyberattaque [cf. chapitre 2]) pour leurrer des employ  s (phishing cibl   et personnalis  ) et les amener    r  aliser des actions qui conduiront    l'intrusion du syst  me d'information de leur organisation ou    l'infection des ressources. De plus, ils permettent g  n  ralement de « d  duire » des mots de passe des employ  s    part par exemple des lieux de naissance, des dates, des pr  noms des enfants et de l'animal familier, etc. Compte tenu des pratiques peu s  curis  es des

22. BYOD peut s'interpr  ter comme *Bring Your Own Disaster* ou se transformant g  n  ralement en BYOV (*Bring Your Own Virus*).

23. Souvent les politiques de BYOD sont devenues des politiques de type *Choose Your Preferred Device in a list proposed by the company*.

24. Services de stockage d'information dans le nuage (comme par exemple DropBox, Box.net, etc.), ces services r  pliquent les fichiers qu'on y stocke sur tout une s  rie d'appareils (par exemple : le PC de bureau, le PC portable, la tablette, le t  l  phone mobile).

utilisateurs en matière de mot de passe, les réseaux sociaux, comme Facebook, sont des mines d'or pour les criminels...

Il n'y a aucune contre-mesure d'ordre technique pour parer à cela. Des cyberattaques d'envergure, y compris sur des sociétés spécialisées dans le domaine de la sécurité informatique et de la défense, ont été possibles du fait de l'**intelligence sociale** des attaquants qui ont su tirer parti des données trouvées sur les réseaux sociaux pour contourner les mesures et technologies de sécurité en place.

Outre le gaspillage de ressources (consommation de bande passante etc.) et le fait que les employés peuvent passer du temps sur ces réseaux au lieu de travailler (leur côté addictif renforce ce problème), le risque de fuite d'informations exploitables n'est pas négligeable. En effet, par exemple sur *LinkedIn* se trouvent de nombreuses informations détaillées sur les projets que gèrent les personnes (et dans certains cas des choses que l'entreprise ne souhaite pas voir communiquées...), en même temps, dans le domaine de l'**intelligence économique**, le fait d'interroger des employés est un classique (par exemple en organisant de faux recrutements, avec de faux entretiens lors desquels les candidats sont amenés à divulguer des informations). Par ailleurs, peut se poser le problème de la prise de contrôle de la page d'une entreprise sur un réseau social par une entité tierce qui en modifie le contenu et diffuse des messages erronés aux « amis » et « *followers* » de l'organisation, affectant ainsi la réputation de celle-ci et la confiance de ses clients et partenaires. Cela peut également concerter les sites de micro-*blogging* comme *Twitter* par exemple.

Résumé

La plupart des applications possèdent une version sécurisée qui permet le plus souvent de réaliser l'authentification des correspondants et le chiffrement des données transmises. Une alternative à l'implantation de nouvelles versions sécurisées des protocoles d'application consiste à implanter un mécanisme commun de sécurité, offrant des services génériques de sécurité à toutes les applications. Le logiciel SSL/TLS, couramment utilisé à l'heure actuelle, notamment pour réaliser des transactions commerciales sur Internet, joue ce rôle.

L'usage extensif de documents hypertextes, comme le téléchargement de contenus actifs ou non, pose de nombreux problèmes de sécurité concernant entre autres : leur origine, leur auteur, leur authenticité, leur caractère nuisible ou non, etc. Des éléments de réponses à cette nouvelle dimension de la sécurité des systèmes d'information passent par des techniques de signature de documents XML, de tatouage, de gestion des droits électroniques, afin de conférer à la sécurité une certaine persistance. Un niveau donné de sécurité doit pouvoir être conservé, même si l'objet concerné par la sécurité sort des frontières physiques de l'environnement dans lequel sa sécurité est habituellement gérée.

Les données de l'entreprise sont de plus en plus en dehors de son périmètre de sécurité. C'est également le cas avec l'usage de l'informatique personnelle et des réseaux sociaux. Ces nouvelles pratiques augmentent le niveau de vulnérabilité des données et les opportunités d'exploitation criminelle. L'ingénierie sociale fait partie des outils de la cybercriminalité pour laquelle l'organisation a de la peine à déployer des contre-mesures.

La protection des données personnelles dans le cyberespace soulève de nouveaux défis techniques, juridiques et humains qui touchent la société dans son intégralité. En effet, la protection des données personnelles est une condition préalable d'une part à l'autodétermination et à la protection de la liberté d'expression et de la dignité humaine et d'autre part à la démocratie. Que cela soit à l'échelle d'un individu, d'une organisation ou d'un État, les technologies du numérique, comme la sécurité informatique au sens large, devraient pouvoir garantir le respect des droits fondamentaux et des libertés civiles, comme nous le rappelle l'article 8 de la Convention européenne des droits de l'homme (ECHR) de 1998 « *Chacun a droit au respect de sa vie privée et de sa famille, de son domicile et de sa correspondance* ».

Exercices

9.1 Pourquoi a-t-on besoin de sécuriser la messagerie électronique ? Identifiez les risques et les mesures sécuritaires disponibles.

9.2 Comment PGP s'intègre-t-il dans la messagerie électronique ? Peut-on l'utiliser pour d'autres types d'applications ?

9.3 Pourquoi le spam peut-il poser des problèmes de sécurité ?

9.4 De manière générale, comment sécurise-t-on une transaction commerciale sur Internet ?

9.5 Identifiez les avantages, inconvénients et limites des solutions courantes de sécurisation des transactions commerciales sur Internet.

9.6 Quels sont les problèmes de sécurité posés par l'usage de documents XML ?

9.7 Qu'est-ce qu'un tatouage électronique, sur quelles techniques de sécurité repose-t-il ?

9.8 Quels critères de sécurité un tatouage de document peut-il contribuer à saisir ?

9.9 Est-ce que le tatouage numérique d'un document peut offrir un niveau de sécurité inconditionnel ?

9.10 Donnez un exemple de vulnérabilité des applications web et proposez un élément de solution pour y remédier.

9.11 Dans quelles mesures les organisations sont-elles concernées par la gestion des droits numériques ?

9.12 Quels sont les principes de sécurité associés à la gestion des droits numériques (DRM) ?

9.13 Identifiez les principaux problèmes de sécurité générés par l'usage de la téléphonie Internet.

9.14 Pourquoi est-il difficile de sécuriser efficacement la téléphonie sous IP ?

9.15 Est-ce que les solutions de sécurité des transactions commerciales basées sur l'usage de SSL/TLS permettent de protéger la vie privée des consommateurs ?

Solutions

9.1 La **messagerie électronique** est un outil de communication incontournable, mais est considérée comme une application critique, conçue sans prise en compte des besoins de sécurité. Il en résulte que les critères de sécurité tels que la confidentialité (les messages peuvent être écoutés), l'intégrité (les messages peuvent être altérés), la disponibilité (les messages peuvent être détruits ou perdus), l'authentification (des utilisateurs) ou la non-répudiation (des échanges) ne sont pas garantis. Des risques liés à un défaut de sécurité peuvent avoir des impacts importants pour les utilisateurs et les organisations. Parmi eux retenons :

- l'usurpation d'identité des utilisateurs ;
- la perte, la modification, l'interception voire la destruction du message ;
- le démenti d'avoir reçu ou envoyé un courriel (la répudiation) ;
- le rejeu, la suppression ou le retardement d'envoi des messages ;
- les différentes facettes du harcèlement *via* la messagerie électronique (spam, lettres nigériennes, inondation de messages, etc.) ;
- l'infection, la prise de contrôle à distance des systèmes par le biais de programmes malveillants (virus, vers ou chevaux de Troie, logiciels espions, etc.) ;
- la diffusion d'informations censées être confidentielles ;
- le phishing à des fins d'escroquerie.

Il est recommandé d'utiliser des versions de logiciels de messagerie électronique qui intègrent des fonctions sécuritaires visant à assurer l'intégrité, l'authentification, la confidentialité et la non-répudiation des messages ainsi que la disponibilité de l'application de la messagerie électronique. Des antivirus et des antispams actifs, comme une bonne sensibilisation des utilisateurs aux risques sécuritaires renforcent la sécurité du système de messagerie.

9.2 PGP permet de sécuriser l'échange de messages électroniques. En s'intégrant dans le logiciel de messagerie électronique des utilisateurs (les serveurs de messagerie ne sont pas affectés par l'utilisation de PGP), PGP assure la confidentialité, l'authentification et l'intégrité des courriels. En utilisant PGP, l'émetteur, après avoir créé le message, applique une fonction de *hashage* (généralement SHA-1) pour générer un résumé (*digest*) de 160 bits. Ensuite, l'émetteur chiffre ce résumé en appliquant un algorithme de chiffrement asymétrique (RSA par exemple) avec sa clé privée. Le message et le résumé chiffré sont alors envoyés au destinataire. Cette pratique assure l'intégrité du message ainsi que l'authentification de l'émetteur. La

confidentialité est réalisée par l'utilisation d'un algorithme de chiffrement symétrique (principalement IDEA), la clé de session est alors envoyée, chiffrée par l'algorithme de chiffrement asymétrique et la clé publique du destinataire. L'émetteur chiffre alors le message en utilisant l'algorithme de chiffrement symétrique et l'envoie au destinataire.

PGP pourrait être utilisé pour la sécurité d'**autres types d'applications** comme les discussions *chat* confidentielles entre utilisateurs. Le fonctionnement est le même que pour la messagerie électronique.

9.3 Le **spam**, courrier publicitaire non sollicité, courrier illégitime ou encore pourriel (poubelle-courriel), est à la base de la réalisation d'escroqueries, d'actions d'hameçonnage (phishing). Le spam peut engendrer des problèmes de sécurité dans la mesure où il peut encombrer la boîte aux lettres d'un utilisateur, ce qui à grande échelle et de manière excessive pourrait conduire à sa saturation et à un déni de service (bombardement, à un grand nombre de destinataires, d'un grand nombre de messages de plus ou moins grandes tailles). Toutefois, le risque le plus important est sans doute celui lié à la propagation et à l'introduction de programmes malveillants (*malware*, virus, chevaux, de Troie, etc.) entraînant l'infection des systèmes ou leur prise de contrôle à distance et ainsi l'atteinte aux critères de sécurité.

Il n'a pas de moyens techniques 100 % efficaces pour lutter contre cette nuisance. Des filtres antispams peuvent exister, comme une liste noire des serveurs ou des utilisateurs générateurs de spam (sur la base de leur adresse IP ou adresse email).

9.4 Les solutions de sécurité en matière de **commerce électronique** s'appuient sur des mécanismes classiques de sécurité afin d'assurer l'identification et l'authentification des partenaires commerciaux, l'intégrité et la confidentialité des données transmises ainsi que sur la non-répudiation. De manière courante, les transactions commerciales sur Internet utilisent des certificats numériques pour authentifier le serveur et chiffrer les données en transit. Outre la nécessité de sécuriser la connexion entre l'acheteur et le vendeur en ligne par une connexion SSL/TLS ou le protocole SET (*Secure Electronic Transaction*), il est également nécessaire de sécuriser les serveurs dans l'environnement du vendeur, notamment pour la protection des données personnelles.

9.5 Les avantages sont à trouver dans la banalisation et la disponibilité des mécanismes tels que SSL/TLS mis en œuvre pour sécuriser une transaction commerciale (cf. réponse de l'exercice précédent 9.4), ce qui en constitue également un point faible et donc des inconvénients et limites, car ils peuvent être contournés et des faiblesses liées à leurs implantations et mode de fonctionnement existent et peuvent être exploitées.

9.6 La **manipulation et l'échange de documents XML** sont devenus quasi indispensables lors de la réalisation de services web. Avec XML, localiser l'information devient plus simple, ainsi, si les mots de passe sont dans un fichier balisé en XML, un malveillant peut y avoir directement accès.

Pour communiquer d'une manière sûre, plusieurs technologies de sécurisation des données ou de la session de travail, basées sur l'usage du chiffrement, existent. Par ailleurs, pour ne sécuriser qu'une partie d'un document (ce qui peut s'avérer très utile dans certaines applications nécessitant l'intervention de plusieurs responsables sur un même document), seuls les mécanismes de **signature XML** (*XML Signature*) et de **chiffrement XML** (*XML Encryption*) peuvent répondre à ce besoin. Lorsqu'il s'agit de chiffrer des parties de documents XML ayant déjà été signées, la validation de la signature devient impossible puisque le document aura été modifié. La recommandation relative au déchiffrement XML (*Decryption Transform for XML signature*) permet de répondre à ce besoin.

9.7 Un **tatouage électronique** peut être vu comme une marque, fortement liée aux données dans lesquelles elle est intégrée et associée, construite *via* des mécanismes cryptographiques. Tatouer un document consiste à solidariser le tatouage avec le contenu du document. En fonction des besoins, un tatouage doit être invisible et indéetectable (contrainte d'imperceptibilité). Il ne doit pas altérer la signification ni la représentation des informations tatouées. Un tatouage doit être robuste (éventuellement indélébile) et résister à diverses attaques et aux traitements subis par les documents tatoués (compression, changement d'échelle, etc.).

9.8 Tatouer un document permet de contribuer à réaliser une **protection des droits d'auteur**, de la **propriété intellectuelle** associés à des documents numériques. La technique de tatouage peut également être utilisée pour intégrer dans un document des informations supplémentaires constituant une étiquette (étiquetage) servant à son indexation et à son archivage ou à effectuer des contrôles sur les règles d'utilisation.

9.9 Le tatouage **n'offre pas** un niveau de sécurité inconditionnel car certains tatouages ne sont pas résistants et peuvent être effacés. De plus, il peut arriver qu'un document déjà tatoué puisse être « surtatoué » par un malveillant. Par ailleurs, la stéganographie, qui permet de dissimuler une information dans une autre, peut être considérée comme étant une forme particulière de tatouage électronique, or elle est souvent employée par des criminels pour communiquer...

9.10 Comme toutes les applications, les **applications web** peuvent être sujettes à un grand nombre de menaces qui exploitent leurs vulnérabilités conceptuelles ou opérationnelles. Ainsi, par exemple, une des vulnérabilités des applications web est liée à la possibilité de pouvoir injecter des données. Il s'agit d'une technique d'attaque sur les applications web ou sur les scripts CGI (*Common Gateway Interface*) qui consiste à insérer des données en entrée d'un programme, d'un script CGI afin de réaliser une fonction malveillante (débordement de mémoire, vol de données, exécution d'un code, etc.). On peut injecter du code SQL (*Structured Query Language* – langage de manipulation de bases de données relationnelles) dans les champs d'un formulaire HTML qui, ensuite, permettra par exemple d'accéder à des données d'un serveur web normalement protégé.

9.11 En fonction de leur nature, les organisations peuvent être concernées avec des degrés d'importance variable par la gestion des droits numériques associés aux contenus qu'elles produisent ou qu'elles possèdent. Cela dépend de la valeur des contenus et des besoins de sécurité qui en découlent, notamment du besoin de protection persistante (y compris en dehors des frontières traditionnelles de l'organisation).

9.12 Les principaux principes de sécurité associés à la gestion des droits numériques sont liés à la nécessité de pouvoir limiter les accès à des contenus spécifiques aux seules entités habilitées quelle que soit la localisation des contenus (notion de protection persistante).

9.13 Un des problèmes de sécurité posés par la téléphonie sur IP est lié au fait que le fonctionnement du réseau Internet est basé sur la commutation de paquets IP (sans garantie de qualité de service ou de réalisation de service). Or l'application de téléphonie devrait, dans l'absolu, être disponible 24h/24, 7 jours/7 pour tout ce qui concerne les appels aux numéros d'urgence.

La disponibilité du service de téléphonie sur IP ne peut pas être garantie, ni d'ailleurs la confidentialité ou l'intégrité des conversations téléphoniques.

9.14 La téléphonie sous IP est une application qui doit s'exécuter en quasi-temps réel avec une certaine interactivité des interlocuteurs, et sans perte de données, ce qui rend difficile la mise en œuvre de mécanismes de sécurité efficaces.

9.15 Non, car la mise en œuvre de SSL/TLS permet juste de rendre confidentielles certaines informations de la transaction commerciale mais ne peut garantir qu'il n'y aura pas de profilage des consommateurs (enregistrement et exploitation des habitudes d'achats, des dépenses, des fréquences, etc.), que les données personnelles des consommateurs ne seront pas exploitées par les acteurs légitimes de la transaction commerciale ou par des entités malveillantes qui pourraient pirater les systèmes de l'acheteur ou du commerçant, etc.

LA SÉCURITÉ PAR LA GESTION DE RÉSEAU

10

PLAN

- 10.1 Intégration des technologies de sécurité
- 10.2 Gestion de systèmes et réseaux
- 10.3 Gestion du parc informatique
- 10.4 Gestion de la qualité de service réseau
- 10.5 Gestion comptable et facturation
- 10.6 Gestion opérationnelle d'un réseau
- 10.7 Gestion de systèmes par le protocole SNMP

OBJECTIFS

- Présenter la complémentarité des approches de gestion de réseau et de gestion de la sécurité.
- Mettre en évidence l'apport majeur d'une gestion de réseau efficace pour une sécurité optimale.
- Valider les acquis par des exercices d'intégration des connaissances.

10.1 INTÉGRATION DES TECHNOLOGIES DE SÉCURITÉ

10.1.1 Interopérabilité et cohérence globale

Le nombre des systèmes interconnectés réalisant le système d'information de l'entreprise, l'ouverture de ce dernier sur Internet ainsi que la mobilité des équipements et des usagers rendent le système d'information plus vulnérable et plus difficile à sécuriser de façon uniforme avec une sécurité « **sans coutures** ». La sécurité est trop souvent réalisée au coup par coup, alors qu'elle devrait suivre une **démarche de gestion des risques et de la sécurité** (*cf. chapitres 3 et 4*). Les administrateurs réseaux comme le personnel du support technique interviennent souvent comme des pompiers, en réaction à des incidents, pour parer au plus pressé. Alors qu'une démarche de sécurité doit aussi être proactive et tenir compte des risques effectifs, dans une enveloppe budgétaire déterminée. En effet, mieux vaut prévenir que guérir, et de plus ça coûte beaucoup moins cher. Veiller à la **cohérence globale** et à la **non-redondance** excessive des mesures, quel que soit le niveau de sécurité souhaité, est primordial.



Entre efficacité, performance et facilité d'utilisation, la sécurité doit être équilibrée en fonction des valeurs, des risques et de leurs conséquences, et des coûts.

10.1.2 Externalisation et investissement

Seul le respect des aspects légaux notifiés contractuellement ainsi que des recours pénaux constitue un garde-fou à des situations défaillantes générées par des intermédiaires techniques ou des situations d'**externalisation** (*outsourcing*). Des **risques financiers** (surfacturation, coûts engendrés par des pannes, perte d'exploitation, changement de prestataire, etc.), des **risques techniques** (obsolescence, incapacité à délivrer le service requis, etc.) et des **risques d'exploitation** (interruption de service, déni de service, etc.) peuvent survenir lors de l'externalisation des services informatiques. Il en est de même lorsque l'on sous-traite tout ou partie de la sécurité d'un système d'information.

Une **bonne gestion budgétaire** est fondamentale à la maîtrise des risques dans la mesure où **l'investissement rentable et durable** en informatique et en sécurité permettra à l'organisation d'être performante et à son personnel de travailler en toute confiance.

S'il est relativement aisé de convaincre une direction générale de faire réaliser des tests de pénétration de systèmes informatiques¹ afin d'en montrer des vulnérabilités, il est parfois beaucoup plus difficile de la convaincre d'investir dans une véritable démarche d'analyse des risques ou encore dans la formation ou la sensibilisation des employés. Pourtant, le résultat de tests de pénétration est souvent prédictible. Une entité déterminée à pénétrer un système y arrive ! Il n'est donc pas nécessaire de payer pour ce que l'on connaît déjà ! La plus-value apportée par des tests de vulnérabilité sans interprétation des résultats ou recommandations particulières est souvent relativement faible pour l'entreprise qui l'a commanditée. La dimension spectaculaire de la démonstration de l'intrusion est souvent génératrice de peur et peut déclencher un réflexe d'achat en matière de sécurité, sans que cela soit forcément intégré correctement dans une démarche de gestion des risques. Même si cela contribue à sensibiliser aux problématiques de sécurité, vendre de la sécurité basée sur la peur n'est pas le meilleur moyen de réaliser une protection efficace et efficiente des actifs de l'organisation. Cela répond plus à une logique commerciale qu'à une logique de maîtrise des risques ou de **gouvernance de la sécurité**. Combien d'entreprises ont-elles fait les frais de tests de pénétration sans pour autant avoir par

1. Certains utilisent les termes de « **ethical hacking** » pour désigner des tests d'intrusion. Il ne s'agit pas de hacking mais d'une action commanditée faisant l'objet d'un contrat entre les parties prenantes. La motivation et la finalité des tests d'intrusion s'inscrivent dans une optique « business » et commerciale de la sécurité. Les tests d'intrusion ne relèvent pas de l'éthique, même si on peut espérer que les personnes qui les réalisent possèdent un sens de l'éthique développé et un comportement irréprochable (ils ne doivent pas utiliser leurs compétences et les connaissances acquises lors des tests de pénétration des systèmes appartenant à des tiers à des fins malveillantes).

la suite acquis la compétence interne leur permettant de maîtriser, sur le long terme, leurs risques ? Il serait sans doute plus judicieux, pour une organisation, d'investir dans la compréhension des risques, afin qu'elle puisse acquérir les moyens de diriger elle-même sa sécurité, plutôt que dans des actions ponctuelles de tests d'intrusion. Cela contribuerait à ne pas ignorer la **dimension transversale de la sécurité** et son rôle fondamental et critique pour la **compétitivité** et la **pérennité** de l'organisation. Mieux vaut présenter la sécurité comme un gain, obtenu par exemple par la confiance des clients ou des administrés.

Par ailleurs, dans un contexte de guerre économique, il est nécessaire de s'interroger sur la pertinence de l'externalisation de tout ou partie de la sécurité informatique d'une entreprise. La **dépendance** à des entités non contrôlables et non transparentes (outils, mesures, tierces personnes) est préjudiciable à la finalité de la sécurité, autrement dit à la diminution des pertes. En effet, la perte potentielle du contrôle de la sécurité, consécutive à une externalisation mal maîtrisée, génère des risques additionnels. Le transfert du traitement du risque informationnel et de la sécurité ne relève pas toujours d'une stratégie mais correspond le plus souvent à un transfert voire à un défaut de responsabilité des dirigeants et des intermédiaires techniques (fournisseurs de produits et services).



Sous-traiter la sécurité de ses données n'entraîne pas la sous-traitance de ses responsabilités.

Une alternative possible à l'externalisation serait de proposer aux dirigeants, des indicateurs des risques informationnels, pour qu'ils puissent diriger, en toute connaissance de cause, leur sécurité en fonction de leurs exigences stratégiques.

Des indicateurs pour améliorer la sécurité doivent fournir des informations mesurant la pertinence, l'efficacité, l'efficience des processus de gestion de la sécurité afin de contrôler et de maîtriser les processus en place qui contribuent à la maîtrise des risques. Or, le résultat des tests de pénétration de systèmes fournit uniquement des indicateurs sur des possibilités d'exploitation de failles techniques, organisationnelles ou humaines. Ils ne permettent pas de répondre à **l'exigence d'amélioration de la sécurité**, du fait que l'indication donnée est statique (une photographie du système informatique à l'instant t) alors que le contexte des risques est évolutif et que la gestion de la sécurité nécessite de l'appréhender sous forme de **processus dynamique**. Ainsi, les entreprises devraient être attentives à investir au mieux en matière de sécurité et peut-être différemment, afin qu'elles soient réellement maîtresses de leur sécurité informatique.

10.2 GESTION DE SYSTÈMES ET RÉSEAUX

Les activités de **gestion de systèmes et de réseaux**, lorsqu'elles sont menées correctement, permettent d'offrir les niveaux de disponibilité et de performance nécessaires à la réalisation de la sécurité. De plus, elles intègrent les tâches de surveillance du réseau, de détection des anomalies d'intrusions ou d'incidents, qui sont nécessaires

à la mise en œuvre de la sécurité et qui contribuent grandement à la sécurité globale du réseau et du système d'information qu'il dessert. La gestion de réseau intègre celle de sa sécurité et peut être vue comme un outil de la réalisation de la sécurité (figure 10.1).

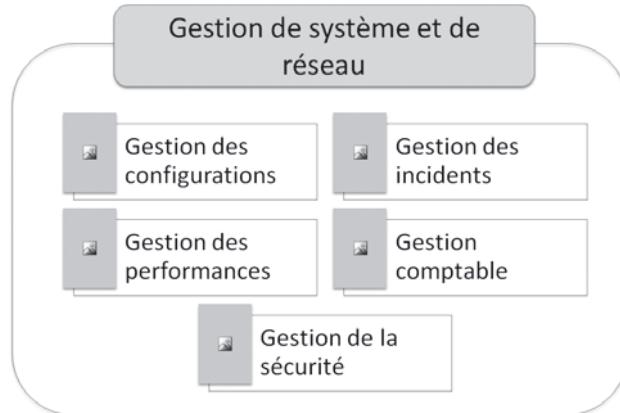


Figure 10.1 - Interdépendance de la gestion de réseau et de la sécurité.

De manière courante, la gestion de réseau contribue à réaliser les fonctions de sécurité relatives à la disponibilité par un dimensionnement et des procédures appropriées de gestion des performances, des configurations et des incidents. De plus, elle supporte la fonction de **contrôle d'accès logique**, qui contribue à la réalisation des critères de confidentialité et d'intégrité (cf. chapitre 6).

10.3 GESTION DU PARC INFORMATIQUE

10.3.1 Objectifs et fonctions

Comme on ne gère et on ne sécurise bien que ce que l'on connaît bien, il est primordial d'effectuer un **recensement** le plus exhaustif possible des actifs informatiques.

Les **fonctions d'un système de gestion du parc informatique** contribuent à la sécurité *via* les fonctions suivantes :

- gestion technique du parc ;
- gestion du catalogue, codification des équipements, terminologie commune, repérage physique des matériels à des fins d'inventaire ;
- inventaire initial et périodique de tous les composants du système d'information ;
- standardisation maximale des configurations (économie d'échelle, cohérence des fonctions à assurer) ;
- schéma de circulation des flux de données ;
- volumétrie des flux ;
- harmonisation des différents fournisseurs ;

- gestion commerciale (administration des contrats, tarifs, commandes, acquittement des factures, gestion des délais de paiement, délais de livraison et de garantie, suivi des comptes fournisseurs, suivi budgétaire, gestion des licences, etc.) ;
- gestion des immobilisations (traduction des états comptables réglementaires) ;
- gestion physique du parc (définition des responsabilités pour l'entrée, le suivi de l'état, la localisation des équipements, identification de vols ou de destruction des équipements, détermination de la valeur d'assurance du matériel, etc.) ;
- gestion des incidents (réception automatique des incidents, description, suivi des pannes par fournisseur, etc.) ;
- contrôle de gestion (mesure des coûts actuels et prévisionnels, refacturation aux utilisateurs, préparation de budgets, contrôle budgétaire des achats par centre d'activité, suivi des coûts de maintenance, d'exploitation, suivi d'un indicateur donnant le nombre d'interventions par unité d'équipement selon les marques/modèles/types, corrélation entre le niveau d'obsolescence et l'immobilisation comptable, etc.) ;
- processus d'identification, de valorisation et d'affectation des coûts réels pour contrôler les dépenses ;
- gestion des comptes à priviléges (les attaquants repèrent ces comptes en priorité).

L'inventaire des ressources, y compris des profils des utilisateurs, est fondamental pour identifier les valeurs à protéger et les critères de sécurité associés afin d'identifier les mesures de sécurité pour les satisfaire.



10.3.2 Quelques recommandations

La mise en œuvre d'un service de gestion de parc s'inscrit dans une logique de qualité et doit s'interfacer et dialoguer harmonieusement avec les autres services de gestion de réseau (modules de gestion des configurations, des performances, des incidents, de la comptabilité).

Une bonne gestion de parc informatique n'a de sens que si l'on sait également gérer correctement l'utilisation des **ressources informatiques** et les **fournisseurs** (éditeurs de logiciels, opérateurs, etc.) dont l'entreprise dépend.

La mise en place d'une politique cohérente de remplacement des machines pour faire évoluer le parc informatique, ainsi qu'une bonne connaissance du réseau donne lieu à une meilleure anticipation des besoins et justification des demandes budgétaires qui en découlent.

La **dénomination des ressources** est très importante. L'administrateur doit choisir les noms des serveurs, des stations, des ressources périphériques, des répertoires pour les logiciels, des utilisateurs et des groupes d'utilisateurs. Une politique de dénomination claire, cohérente et connue des administrateurs réseau est primordiale si l'on souhaite maintenir une cohérence des noms dans le parc informatique d'une entreprise. Cela permet également de partitionner, cloisonner ou de réaliser des groupes logiques de ressources possédant des besoins identiques de protection pour y appliquer globalement des règles de sécurité.

Le côté rébarbatif des inventaires informatiques et l'évolution rapide des configurations entraînent parfois un certain flou dans la gestion de la connaissance du réseau. Il est du ressort de la direction informatique de l'entreprise d'imposer une bonne **gestion des inventaires**, afin de faciliter les évolutions du réseau et d'assurer sa sécurité. L'**inventaire** est un des fondements indispensables à tout dimensionnement correct (disponibilité, fiabilité, sûreté de fonctionnement) ainsi qu'à la qualité des services et donc à leur sécurité.

La direction informatique doit s'assurer de la cohérence, de la complétude et de l'exactitude des inventaires et en vérifier l'état par un **audit** ou un **contrôle informatique interne** par exemple. Il est souvent nécessaire de contraindre les utilisateurs à suivre les directives de l'administrateur réseau, notamment en ce qui concerne l'utilisation des logiciels et des données de l'entreprise, pour satisfaire les critères de sécurité de cette dernière.

Une solution consiste à utiliser un outil logiciel de gestion des inventaires prévu à cet effet. Certains comportent des modules situés sur les stations qui s'exécutent périodiquement lors des connexions, alors que d'autres scannent dynamiquement le réseau. Ils permettent de connaître presque en temps réel la configuration complète du réseau et contribuent souvent à la surveillance des activités.

10.4 GESTION DE LA QUALITÉ DE SERVICE RÉSEAU

Les fonctions de **gestion de la qualité du service réseau**, la gestion comptable, l'ingénierie du réseau autorisent la réalisation des principaux critères de sécurité. Ils sont satisfaits au quotidien par une bonne gestion opérationnelle des ressources et des services, ils seront des facteurs de la garantie d'un niveau correct de la sécurité opérationnelle.

10.4.1 Indicateurs de qualité

Disponibilité, capacité, accessibilité, temps de réponse, fiabilité d'un réseau sont des **critères mesurables de la qualité de service** du réseau considéré :

- La **disponibilité** est la période de temps pendant laquelle le service offert est opérationnel.
- Le volume potentiel de travail susceptible d'être pris en charge, durant la période de disponibilité du service réseau, détermine la **capacité** d'un réseau.
- L'**accessibilité** du réseau définit la façon dont la capacité est distribuée aux utilisateurs. Elle est perçue comme étant le **temps de réponse** du réseau.
- La **fiabilité** d'un réseau est la probabilité, pour un utilisateur, de pouvoir mener correctement à terme une session de travail. Elle exprime le niveau de confiance possible envers l'infrastructure de service.

La qualité d'un service réseau est contrôlable tout au long de la vie du réseau par une **mesure de performances**. Vérifier le niveau de satisfaction des utilisateurs, veiller à ce que les performances réelles du réseau soient compatibles avec celles

auxquelles l'utilisateur a souscrit dans son contrat de service fait partie de la gestion du réseau.

Afin de garantir la **satisfaction des utilisateurs** et de prévenir tout conflit, un processus continu d'amélioration de la qualité doit être réalisé par le biais de la mise en place :

- de tableaux d'indicateurs qualité ;
- d'un bureau d'aide aux utilisateurs (support technique ou *help desk*) ;
- de contrats de service.

La prise en compte du facteur « performance du réseau » s'effectue dès la rédaction du **cahier des charges** dans lequel les performances attendues doivent être clairement énoncées. Préalablement à un engagement contractuel sur une convention de service, on définit des **indicateurs** de performance et la façon de les mesurer en des points de surveillance précis.

Une **analyse** des performances permet de les améliorer, de trouver la configuration optimale et de prévoir l'évolution potentielle du réseau. Pour cela, il faut identifier la croissance des activités générant des flux informationnels, l'augmentation du volume des applications, etc.

Concernant la sécurité, on ajoute l'intégrité, la confidentialité et la traçabilité des informations sensibles :

- l'intégrité est l'assurance qu'une information n'a pas été modifiée par une personne qui n'en avait pas l'autorisation ;
- la confidentialité est l'assurance qu'une information ne peut être lue que par les personnes qui en ont l'autorisation ;
- la traçabilité est l'assurance qu'il sera possible de remonter le cycle de vie d'une information.

10.4.2 Évaluation et efficacité

Un contrôle de la réalisation effective des améliorations par une étroite surveillance de l'évolution des indicateurs de performance est fondamental pour un bon suivi du réseau.

Les **évaluations du niveau de service** et de son amélioration potentielle sont réalisées à la fois par les utilisateurs et par le service informatique, souvent par le biais d'enquêtes. Une divergence de perception du niveau de service peut survenir, reflétant des besoins et des contraintes différentes. Une telle enquête permet de recueillir des informations précises sur les conditions d'utilisation des postes de travail et sur la perception du service réseau fourni. Elle s'effectue par un processus classique d'enquêtes et de questionnaires appliqués à un échantillon représentatif d'utilisateurs, après une campagne d'information et un suivi sur le terrain. L'impact, en terme de valeur financière, du temps de réponse et de la disponibilité du réseau est lui aussi parfaitement chiffrable.

Une **politique de qualité de service** nécessite la mise en place d'une structure organisationnelle adéquate, la réalisation d'investissements en divers outils matériels et logiciels (systèmes de gestion de bases de données, de visualisation, de tests,

de duplication de ressources, surplus de capacité informatique, de téléchargement, de contrôle d'accès, etc.). Une estimation correcte du rapport entre charges de pointe moyenne et optimum des coûts contribue largement à une bonne sûreté de fonctionnement du réseau.

Une **observation suivie** de la qualité de service permet de mesurer l'efficacité du réseau. Cela contribue également à connaître le trafic, à repérer très tôt les incidents potentiels, à surveiller la croissance et les tendances des utilisateurs. Ainsi, la prévision de l'évolution des besoins et du réseau est facilitée.

La **gestion du trafic** (facteur de performance du réseau) peut entraîner un redimensionnement du réseau en fonction des tendances lourdes détectées par les observations du trafic avec comme corollaire, la mise en œuvre de nouveaux services et équipements.

Un **SOC** (*Security Operating Center*) peut être utilisé pour visualiser l'état du trafic, les incidents et les tentatives d'attaques sur le réseau.

10.5 GESTION COMPTABLE ET FACTURATION

Un système de comptabilité participe au contrôle, à la réduction et à l'analyse des coûts de communication, dans l'optique d'optimiser les investissements et de maîtriser les **coûts** et les **risques financiers**. Il peut supporter par exemple des fonctions :

- d'enregistrement des appels sortants par poste de travail ou par compte (possibilité de refacturer en interne) ;
- de génération d'états d'utilisation (états d'activité [par poste, compte, date...], états récapitulatifs [par poste, service, centre de coûts, appel...], états des exceptions [numéros le plus souvent appelés, sites consultés, durée supérieure à x minutes...], etc.) ;
- de suivi des décisions d'exploitation ;
- d'identification des abus, détection d'utilisations frauduleuses ou abusives du réseau, etc.

Toutes les facilités dont a besoin la gestion de réseau pour réaliser une comptabilité appropriée de l'usage des ressources contribuent également à la gestion des identités, des profils des utilisateurs, de leurs droits d'accès, de la surveillance de leurs activités. Ainsi, la sécurité a tout à gagner d'une gestion efficace des **données comptables** liées à l'usage des technologies l'information. Les fonctions de comptabilité et de facturation sont basées sur l'enregistrement de données et sur la surveillance. Ceci facilite donc l'implantation de mesures d'audit, de non-réputation, de traçabilité, d'imputation et de contrôles nécessaires à la réalisation de la sécurité.

10.6 GESTION OPÉRATIONNELLE D'UN RÉSEAU

La **gestion opérationnelle d'un réseau** recouvre l'ensemble des activités d'exploitation journalière et de maintenance qui conservent le réseau en état de marche avec des niveaux de qualité de service et de sécurité satisfaisants. La gestion opération-

nelle ne peut se faire que si on analyse le fonctionnement du réseau et si on détermine dans quelle mesure les objectifs de qualité de service et de sécurité sont atteints. Pour cela, il est nécessaire de disposer d'informations relatives à l'état du réseau. Ces informations observées constituent en quelque sorte des « prises de température » systématiques, qui peuvent être appréhendées comme des indicateurs de performance qui permettent d'identifier au plus vite des anomalies, des intrusions ou une dégradation des performances préjudiciable à la sécurité. Cela autorise, autant que faire se peut, un diagnostic afin d'établir des mesures adaptées, pour optimiser l'infrastructure et les services.

Les technologies du **SIEM** (*Security Information and Events Management*) permettent de recueillir des informations sur les non-conformités à la politique de sécurité de l'organisation, sur les vulnérabilités des applications et sur les incidents de sécurité). Ces informations peuvent être visualisées dans un pupitre de contrôle (un SOC).

10.6.1 Gestion des configurations

Rendre un réseau opérationnel, c'est tout d'abord le **configurer**. C'est à ce niveau de paramétrage du réseau que l'on fixe les critères d'accès aux ressources (permissions), les seuils d'alarmes, les éléments à auditer et à sauvegarder dans des logs (traces), qui contribuent à la réalisation de la sécurité.

En effet, c'est lors de la configuration que l'on positionne les sondes permettant d'effectuer un **audit actif** des événements du réseau. Ainsi, de façon dynamique, le système est capable d'identifier la survenue d'atteintes sécuritaires et de déclencher des actions *ad hoc* (génération d'alarmes, déconnexions automatiques par exemple). Du point de vue sécuritaire, cette phase est primordiale dans la mesure où elle permet d'appliquer la politique de sécurité sur l'ensemble des éléments du réseau et d'établir les procédures de contrôle d'accès.

La configuration d'un réseau reflète son architecture et la manière dont il est dimensionné, structuré, cloisonné, compartimenté. C'est également une phase importante de la détermination de la localisation des systèmes, de leurs redondances, plan d'adressage, liens logiques et physiques et de leurs protections par des systèmes pare-feu.

La configuration du réseau permet sa génération : c'est un chargement effectif de la configuration dans les éléments du réseau. Le réseau possède alors la connaissance de son architecture, de son mode de fonctionnement, de l'implantation de chaque entité, de leur localisation et des protocoles de communication.

Les phases de **configuration** et de **génération** constituent l'initialisation du réseau, après laquelle il devient opérationnel et capable de répondre à une demande de service. Un réseau peut voir son architecture évoluer au cours de son utilisation (ajout, suppression, modifications logicielle ou matérielle), nécessitant une reconfiguration-génération. Cette phase doit pouvoir se faire dynamiquement, sans entraîner un arrêt du réseau afin d'assurer la continuité des services.

La gestion des configurations s'accompagne d'un **contrôle des modifications**, matérialisé par un processus d'autorisation, de mise au point, de test et de documentation des modifications apportées (gestion sécurisée des configurations).

Le **risque** associé à cette fonction peut être lié à des modifications non testées, prohibées ou non documentées qui peuvent mettre à mal le réseau et sa sécurité (mauvais paramétrage du routage, des contrôles d'accès, conduisant par exemple à des effondrements du réseau, à l'indisponibilité de certaines ressources, à des dénis de service, à une facturation erronée, etc.).

10.6.2 Surveillance et optimisation

La fonction de surveillance, véritable outil de gestion des performances et des incidents mais aussi de la maîtrise de la sécurité, permet de réaliser, entre autres, la **traçabilité** des actions et des événements.

La **surveillance** consiste à observer en permanence le fonctionnement et le comportement du réseau, *via* notamment des « sondes réseau » qui permettent des observations du trafic, des remontées d'alarmes, des comptes rendus d'anomalies, par la signalisation d'incidents par les usagers, etc.

Il s'agit de :

- s'assurer que la qualité de service est satisfaisante, que les exigences de sécurité sont respectées ;
- déceler des variations qui pourraient affecter la qualité de service et la sécurité ;
- déterminer s'il n'existe pas de problèmes sur le réseau qui ralentissent les services (goulot d'étranglement, dysfonctionnement, panne partielle, mauvaise configuration, etc.) ;
- détecter les tentatives d'accès frauduleux, de détournement de l'usage de ressources, etc. (notion de *monitoring* actif, de système de détection des intrusions) ;
- vérifier, à l'aide de mesures, que le réseau ou les serveurs ne sont pas saturés, ou en tout cas qu'ils travaillent avec un **degré de charge** supportable. Cela traduit un souci de recherche de configuration optimale et de dimensionnement correct.

L'administrateur système/réseau doit non seulement s'assurer que le réseau est **opérationnel**, mais aussi vérifier périodiquement qu'il fonctionne de façon **optimale**.



10.6.3 Gestion des performances

L'évaluation des **performances** a pour objet principal de mesurer les performances des systèmes et des réseaux en vue de leur optimisation. De plus, elle permet d'évaluer et de paramétrier les outils nécessaires pour satisfaire les exigences de qualité de service et de sécurité.

Les évaluations de performances s'effectuent lors des différentes phases de la vie du réseau :

- à sa conception (dimensionnement du réseau) ;

- lors de modifications d'équipements (prise en compte des expériences passées) ;
- durant le suivi du réseau (surveillance des paramètres de temps de réponse, analyse du trafic, évaluation du débit efficace et maximal, réalisation de tests — tests d'intrusion, test du niveau de robustesse des mots de passe —, identification du seuil d'effondrement des systèmes conduisant à des dénis de service, etc.).

Les performances d'un réseau peuvent être appréhendées de trois façons complémentaires :

- par des **mesures** sur le réseau (*monitoring*, surveillance, sondes, remontées d'alarmes, etc.), elles constituent le seul moyen d'obtenir les indicateurs de performance qui tiennent compte de toutes les caractéristiques réelles du réseau ;
- par des **simulations informatiques** qui passent par la réalisation et l'exécution de programmes modélisant les mécanismes de comportement du système observé en fonction des valeurs des variables étudiées ;
- par des **méthodes analytiques** (étude théorique, le plus souvent basée sur des mathématiques) qui reposent sur la théorie des files d'attente et sur la résolution d'équations modélisant les aspects du fonctionnement du réseau que l'on désire analyser.

10.6.4 Maintenance et exploitation

La **maintenance** est l'ensemble des actions entreprises pour conserver ou remettre un équipement dans un état tel qu'il puisse remplir correctement ses fonctions. La maintenance des systèmes distribués est donc une composante de la réalisation de la sécurité de ces derniers.

Les ressources matérielles et logicielles qui composent le réseau font l'objet de **tests** tout au long de leur vie. Appliqués lors de leur conception, les tests permettent de déterminer le degré de fiabilité et de confiance que l'on peut avoir envers elles. Lors de leur usage, ils contribuent avec des mesures de performances à réaliser la maintenance préventive du réseau. Si les tests sont mis en œuvre sans interruption partielle ou totale du service réseau, les tests sont qualifiés de **tests on line** et, dans le cas contraire, de **tests off line**.

La **maintenance préventive** vérifie le bon fonctionnement d'un équipement par des tests et le remplacement périodique de certains organes fragiles, sans même faire d'essai ou de mesure.

La **maintenance corrective** s'effectue après la localisation de l'origine d'une anomalie afin d'y remédier, par réparation ou par remplacement de l'entité défectiveuse.

Toutes les actions et procédures de maintenance sont déterminées par la politique de maintenance et de gestion des anomalies définie par les politiques de gestion de réseau, de la sécurité et de la continuité des services d'une organisation.

Rendre imperceptible les pannes aux utilisateurs ou, en tout cas, minimiser la durée de l'interruption de service est l'objectif à atteindre de la fonction de gestion des incidents, contribuant ainsi à la continuité des services, à la disponibilité et à l'intégrité des ressources.

La **détection des pannes et des incidents** (localisation et signalisation) est indispensable pour que les mécanismes de réparation et de reconfiguration puissent se réaliser et laisser un système dans un état opérationnel fiable et sûr. L'origine d'une défaillance se détecte par logiciel, soit par des mécanismes de senseurs ou de « chiens de garde » internes, soit par la surveillance d'une unité par une autre. Cela est réalisé par les fonctions suivantes :

- surveillance et déclenchement des alertes et du processus de gestion de crise, si nécessaire ;
- prise en compte des événements non sollicités ;
- localisation, détermination et identification des pannes ;
- correction (actions curatives et réactives, qui peut éventuellement aboutir à une action judiciaire).

Des tests périodiques et systématiques autorisent la signalisation de défaillances des équipements. La plupart des équipements informatiques intègrent des mécanismes de contrôle et de surveillance divers (détection d'erreur, de parité en mémoire ou sur bus, de contrôle d'état des coupleurs, etc.). Toutes ces détections donnent lieu à des transferts d'informations, à des fins de gestion (notion d'informations de gestion), au(x) point(s) de contrôle du réseau dont dépendent les équipements. Les points de contrôle, pouvant agir à distance sur des systèmes en déclenchant des procédures de tests par exemple, autorisent des actions de **télémain-tenance** et de **télésurveillance** en temps réel ou en différé.

La surveillance permet de prévenir certaines pannes ou attaques par détection anticipée des défaillances (identification de mode de fonctionnement dégradé pouvant conduire à des défaillances totales des équipements). C'est le cas pour des systèmes dits de « pots de miel » (*honey pot*), installés spécifiquement pour être des cibles privilégiées de cyberattaques et qui font l'objet d'une surveillance attentive afin d'empêcher ou de limiter la propagation des attaques à l'intérieur du système d'information, mais aussi afin d'essayer de comprendre les tactiques et les stratégies utilisées par les attaquants.



En ce qui concerne la sécurité et la sûreté des systèmes d'information des **systèmes industriels**, comme ceux impliqués dans les centrales nucléaires ou des usines de production par exemple, la détection des incidents est primordiale pour éviter les défaillances des systèmes industriels et de production, les catastrophes industrielles, ou pour limiter les impacts.

La **gestion des incidents** est une fonction qui permet de consigner, d'étudier, de comprendre et de corriger les incidents de fonctionnement du réseau. Elle s'appuie sur une organisation et sur des procédures de traitement des incidents pour savoir que faire lors d'un incident, qui prévenir, comment ? Elle intègre, notamment, une procédure qui oriente les utilisateurs en panne vers un centre d'assistance adéquat. La notification d'un incident entraîne généralement les actions suivantes :

- consignation de l'incident (historique des incidents) ;
- identification de la personne responsable de sa correction ;
- analyse visant à déterminer son origine ;

- mise en œuvre des mesures correctives et préventives nécessaires.

À cela, il faut ajouter pour les incidents critiques, la mise en place d'une procédure de définition des responsabilités et de gestion de crise.

La direction peut imposer, par exemple, au responsable d'un réseau local d'indemniser en interne les départements de l'entreprise pour chaque heure d'interruption. Il s'agit en quelque sorte d'offrir une **garantie de service**, en partant du principe que si le service n'est pas fourni, les départements de l'entreprise ne peuvent travailler correctement, ce qui justifie une indemnisation comptable interne.

On dénomme **exploitation**, toutes les actions qui contribuent à maintenir opérationnel un réseau de télécommunication. Cela consiste également à prélever des informations et à les transmettre à une entité compétente, en vue de réaliser la facturation de l'utilisation des ressources.

La fonction d'exploitation est l'administration quotidienne du réseau. Elle effectue les contrôles de vérification de bon fonctionnement du réseau. Comme toute fonction vitale à la vie du réseau, cette dernière est à sécuriser (sécurité de l'exploitation) en fonction des risques effectifs qu'elle pourrait encourir. **Préventive** ou **corrective**, la fonction d'exploitation intègre les tâches suivantes :

- mise en route ;
- suivi ;
- intervention en cas d'alerte ou de problème ;
- prévention des risques liés aux virus ou autres formes d'attaques ;
- application des mesures correctives ;
- activation du plan ou des équipements de secours, etc.

Le fonctionnement de l'exploitation sera qualifié de bon, dans la mesure où il est en position de service vis-à-vis des utilisateurs, et de partenaire vis-à-vis des développeurs. Pour ce qui concerne ces derniers, cela sera vraiment nécessaire lors de la phase d'industrialisation des applications. Celle-ci a pour objectif de s'assurer que leur intégration et leur mode opératoire sont corrects, administrables, exploitables avant leur diffusion et mise en production. De nouveaux applicatifs ne doivent pas perturber l'environnement d'exécution dans lequel ils s'insèrent, ni la sécurité mise en place.

De plus, l'essai et la réception d'applications doivent être prévus en collaboration avec l'équipe de développement d'applications et les utilisateurs, afin de garantir l'emploi de tests adéquats (plan de tests, tests de charge critique) dans des conditions de fonctionnement normal.

L'automatisation de l'exploitation contribue généralement à la réduction des coûts d'exploitation, du nombre d'interventions humaines et à l'amélioration de la qualité et de la rapidité de service. Pour ce faire, il faut préalablement « normaliser » le processus opératoire des exploitants et mettre en place les systèmes permettant de le réaliser.

10.6.5 Supervision et contrôle

Les activités reliées à la collecte, à la mémorisation, et au traitement des données relatives aux usagers et aux équipements, autorisent celles de la **supervision** et du **contrôle** de l'utilisation des ressources du réseau.

Les principales composantes de la supervision sont la surveillance du réseau et du trafic, la mise en œuvre des procédures de sauvegarde et la coordination des services. Cela consiste en :

- réception en temps réel des informations relatives à la qualité de service ;
- transfert de ces informations vers l'application de gestion concernée, ou vers un système de gestion de bases de données ;
- traitement (détection des anomalies, génération d'alarmes, mise en œuvre du plan de secours, etc.) ;
- présentation des données selon certaines caractéristiques (ergonomie, valeurs significatives, forme, couleur, son), pour une meilleure aide à la décision (vue synoptique de l'état du réseau, etc.) ;
- aide à la télé-action (plan de secours prédéterminé) ;
- mémorisation des actions et événements (journal de bord) dont l'analyse *a posteriori* permet d'améliorer les procédures, les configurations, les plans de secours.

10.6.6 Documentation

La direction informatique ou la direction générale doit exiger une **documentation** complète, précise et à jour de tout ce qui concerne la vie du réseau et sa sécurité. La documentation des activités est une tâche fastidieuse souvent sous-estimée mais toutefois nécessaire à la gestion du réseau et de la sécurité. En effet, aux données strictes de l'inventaire, on intégrera des informations relatives aux configurations logicielles et matérielles, afin d'apprendre des événements passés, de mémoriser le savoir-faire mais aussi les événements à des fins de traçabilité, d'audit et d'optimisation.



Une erreur qui est survenue doit être connue, documentée et réparée. Si elle se répète, cela ne sera plus une erreur mais une faute !

La non-documentation crée ou maintient une dépendance très forte entre l'entreprise et son (ou ses) administrateur(s) réseau. Ce qui réduit considérablement sa capacité de contrôle, de gestion et de sécurité.

 La sécurité passe par la confiance, et la confiance n'exclut pas le contrôle !

L'entreprise court un risque non négligeable si un responsable réseau vient à faire défaut (accident, décès, vacances, départ, etc.). Le contrôle du réseau devient très difficile si l'on n'a pas eu la prudence d'enregistrer et de rendre accessible à des personnes de confiance, des informations que seul un administrateur est censé posséder (mots de passe, etc.).

Toutefois, il est bon d'effectuer un compromis adéquat entre « tout documenter » jusqu'au moindre détail, auquel cas l'administrateur réseau ne fait plus que de la documentation, et « ne rien documenter ». Si la direction générale a le sentiment de ne pas maîtriser les questions techniques et n'est pas en mesure d'assurer elle-même

le contrôle de la documentation, il est de son ressort de la faire valider par des auditeurs externes. Il sera alors demandé une **estimation du degré de détail** exigé dans la documentation, et les auditeurs vérifieront la conformité de la documentation par rapport à ce qui en est attendu.

10.7 GESTION DE SYSTÈMES PAR LE PROTOCOLE SNMP

L'échange d'informations administratives et opérationnelles, sur une base internationale, entre des réseaux ou des éléments de réseaux multiconstructeurs, passe par la **normalisation** de ces échanges. Pour répondre à cet objectif, le **protocole SNMP** (*Simple Network Management Protocol*) a été standardisé par l'IETF² pour supporter les échanges d'information de gestion pour gérer des systèmes distants *via* une infrastructure TCP/IP. Chaque système raccordé (poste de travail, serveur, routeur, etc.) qui doit être géré, intègre un module logiciel « agent de gestion » qui interagit à distance avec un système gérant (le manager). SNMP est le protocole d'échange d'information entre des processus agents et gérant. Pour que ce protocole de gestion appréhende de façon universelle toutes les ressources à gérer, leur représentation a également été standardisée.

Toute ressource à gérer est modélisée selon une approche orientée objet et possède des attributs sur lesquels des opérations particulières de gestion peuvent s'effectuer. Si une ressource réelle n'est pas représentée par un objet de gestion, elle n'est pas visible du système de gestion et ne peut donc pas être gérée. L'ensemble des objets de gestion est sauvegardé dans une base d'information de gestion qui doit être associée à tout équipement.

Ainsi, les ressources réelles gérables à distance sont modélisées par des objets regroupés dans des **MIB** (*Management Information Base*). Les modèles informationnels qui en découlent sont, comme pour tous les protocoles de la famille Internet, mis à la disposition du public. Chaque équipementier peut intégrer, lors de la conception de son matériel, l'interface logicielle (la MIB) qui offrira une visibilité administrative unique de sa ressource, normalisée dans le monde d'Internet. Ainsi n'importe quel système gérant (proposé par un fournisseur quelconque) pourra y accéder *via* le protocole SNMP, pour y appliquer des opérations de gestion.

Comme la notation de syntaxe abstraite **ASN-1**³ permet de décrire n'importe quel élément d'information (*cf.* chapitre 6), elle a été retenue par la communauté Internet pour représenter de façon universelle la vue administrative des ressources à gérer et décrire les objets de gestion. Leur description universelle est, après une procédure d'enregistrement, mise à disposition de la communauté industrielle.

Il existe des procédures d'enregistrement auprès d'autorités internationales qui attribuent un identificateur non ambigu et unique à la spécification standardisée d'un objet de gestion que l'on désire normaliser et mettre à la disposition de la communauté.

2. Protocole SNMP, RFC 1157 accessible à partir du site de l'IETF : *Internet Engineering Task Force* (www.ietf.org).

3. Norme multipartie ISO/IEC 8824:2002.

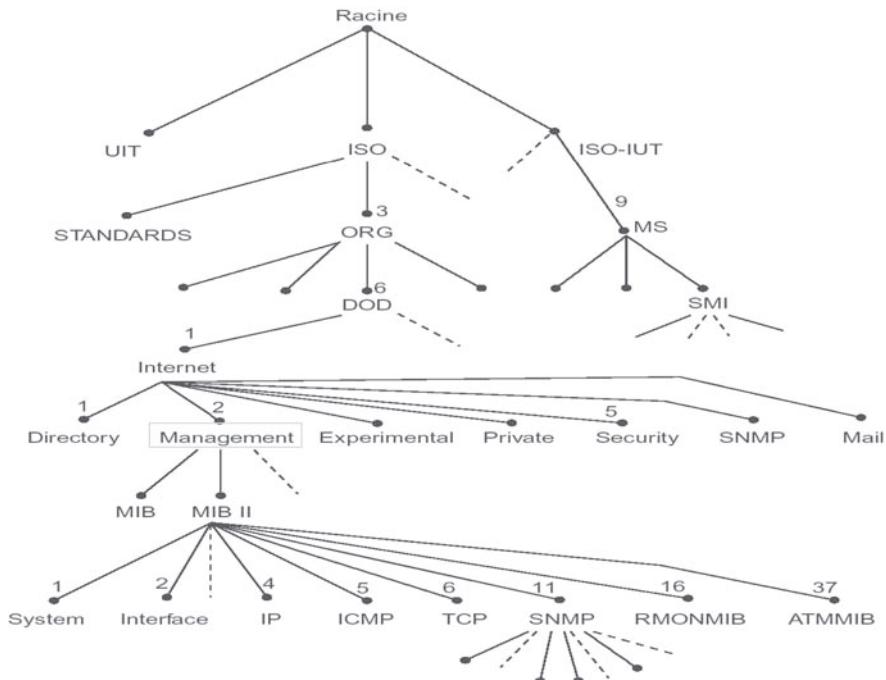


Figure 10.2 – Extrait de l'arbre d'enregistrement des objets de gestion.

Les **autorités d'enregistrement** compétentes pour l'enregistrement des objets de gestion sont organisées selon une structure hiérarchique arborescente (figure 10.2).

De la racine de l'arbre partent trois branches aboutissant à des nœuds distincts de premier niveau, qui représentent les domaines de dénomination des autorités internationales d'enregistrement : l'UIT (CCITT), l'ISO, et un comité joint ISO-UIT. Le niveau immédiatement inférieur à l'ISO autorise, entre autres, l'enregistrement :

- des diverses normes ISO (*standard 0*) ;
- des membres nationaux de l'ISO (*member body 2*), sous lesquels se trouvent l'AFNOR (208), l'ANSI (310), etc.
- des organisations (*organization 3*) sous lesquelles se situent, par exemple, le département américain de la Défense (DOD 6), duquel dépend le domaine de nommage d'Internet (branche 1) dont est issu (branche 2) le domaine contenant tous les noms des entités contribuant à la gestion du réseau (différentes MIB contenant la définition des objets de gestion, du protocole SNMP, etc.).

Les fonctions spécifiques de la gestion système portent sur les objets de gestion (création, modification, etc.) et sur la réalisation de fonctions de gestion (rapport d'alarme, alarme de sécurité, événements, contrôle, test, gestion du temps, enregistrement d'audit de sécurité, mesure de coûts, contrôle d'accès, surveillance de la charge système, etc.).

Le protocole d'application **SNMP** (*Simple Network Management Protocol*) de manipulation et de transfert d'informations de gestion sert de véhicule pour acheminer des requêtes (de consultation et de modification des objets de gestion à distance), les réponses associées et les événements non sollicités (notifications de pannes) entre les processus managers et les processus agents (figure 10.3).

Ce protocole, comme son nom l'indique, pour des raisons de simplicité de mise en œuvre et de performance, est élémentaire. Il ne supportait pas à l'origine des mécanismes d'authentification (manager, agent) et de chiffrement des requêtes nécessaires au support d'opérations sécurisées de gestion de réseau (ce qui a été corrigé). De plus, il était souvent mis en œuvre *via* le protocole UDP. Ainsi, il était aisément dans les deux premières versions du protocole d'accéder sans contrainte aux MIB des équipements, de les modifier et de générer des problèmes de sécurité dus à la non-intégrité des MIB.

La version 3 du protocole (SNMPv3⁴) pallie ces limitations en réalisant en natif des mécanismes d'authentification de la source, de contrôle d'accès et de chiffrement des données véhiculées.

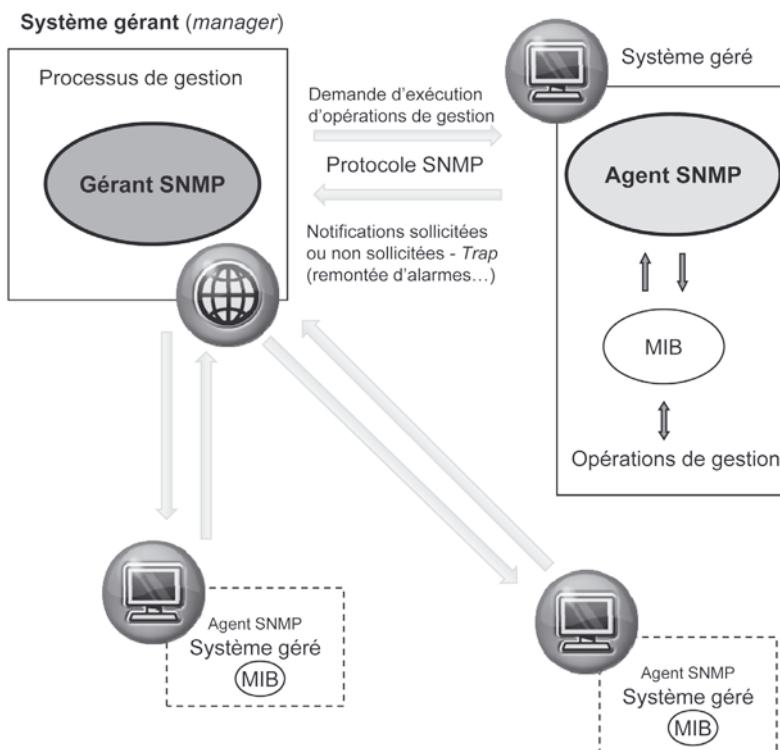


Figure 10.3 – Systèmes gérant et agent et protocole SNMP.

4. SNMP v3, RFC 3410 à 3417.

Résumé

Une bonne gestion de réseau, notamment par les fonctions de gestion des configurations, des performances et des incidents, contribue à assurer la disponibilité et l'intégrité des infrastructures, services et données. De plus, la dimension de gestion de réseau qui fait référence à la gestion comptable permet de disposer de toutes les données nécessaires non seulement à la facturation des usagers mais aussi à la réalisation des fonctions de surveillance et d'audit qui sont de première importance en matière de sécurité. Cela peut permettre une certaine vérification des actions à des fins de preuve ou de non-répudiation ou d'enquête. La gestion de réseau contribue également à réaliser l'objectif de confidentialité dans la mesure où elle assure qu'il n'y a pas d'écoutes clandestines ou des accès non autorisés aux données. La fonction de contrôle d'accès aux ressources, qui fait partie de la gestion de réseau, est fondamentale à la mise en œuvre opérationnelle de la sécurité. La gestion opérationnelle des systèmes et des réseaux contribue à la réalisation des politiques de sécurité, quels que soient les secteurs d'activité des systèmes d'information, c'est d'autant plus critique s'il s'agit de systèmes industriels ou d'infrastructures vitales.

Exercices

10.1 Dans quelle mesure les caractéristiques d'un réseau de télécommunication rendent-elles difficile sa sécurisation ?

10.2 Quelle est l'importance de la gestion de réseau pour la maîtrise de la sécurité ?

10.3 Quelles sont les compétences attendues d'un administrateur réseau ?

10.4 Pourquoi l'inventaire des ressources informatiques et télécoms d'une organisation est-il utile à la sécurité ?

10.5 Pourquoi la fonction de surveillance d'un réseau est-elle essentielle pour assurer sa sécurité ?

10.6 De quelle manière la documentation des actions de gestion du réseau contribue-t-elle à sa sécurité ?

10.7 Est-ce que la notion d'accessibilité d'un réseau intervient dans celle de sa sécurité ?

10.8 Quel est le rôle du protocole SNMP ?

10.9 Comment la mise en œuvre du protocole SNMP peut-il mettre à mal la sécurité d'un réseau ?

10.10 Quelles relations existe-t-il entre les notions de gestion de systèmes et de réseau, de gestion de la qualité et de gestion de la sécurité ?

Exercices d'intégration des connaissances portant sur l'ensemble des chapitres

10.11 Identifier les principaux types d'impacts « business » d'un défaut de sécurité informatique pour une organisation.

10.12 Proposer pour les applications critiques d'une organisation les types de mesures de sécurité à mettre en place.

10.13 Identifier les principaux types d'incidents pouvant nuire à la sécurité d'un système d'information.

36 questions, une réponse possible

Q.1 Quelle atteinte aux données est encourue par l'écoute passive des transmissions ?

- A : Confidentialité
- B : Disponibilité
- C : Intégrité
- D : Authenticité

Q.2 Quel ensemble de facteurs génériques concerne les activités cybercriminelles ?

- A : Méthodes, opportunités, moyens, motivations
- B : Menace, outils, manipulations, juridictions multiples
- C : Permissivité, cibles, défaillances humaines
- D : Gestion inadaptée, éthique, incertitude

Q.3 Quel est le type de programme malveillant qui s'active lors de la survenue d'un événement particulier ?

- A : Virus
- B : Ver
- C : Bombe logique
- D : Cheval de Troie

Q.4 Quelle serait typiquement la première étape d'une attaque informatique ?

- A : Identification de matériel en place
- B : Identification de failles techniques
- C : Scanning de trafic
- D : *Social engineering*

Q.5 Quel élément ne fait pas partie d'un système de la gestion de la sécurité de l'information (ISMS) ?

- A : *Plan*
- B : *Do*
- C : *Check*
- D : *React*

Q.6 Dans une organisation, qui détient la plus grande responsabilité pour la gestion de risques ?

- A : *Senior management*
- B : *Chief Information Officer*
- C : *Chief Information Security Officer*
- D : Responsable de l'audit interne

Q.7 Lequel des éléments suivants ne fait pas partie des motivations d'un cyberattaquant ?

- A : Politique
- B : Erreur
- C : Gain
- D : Curiosité

Q.8 Quelle est la menace qui ne peut pas avoir une origine accidentelle, délibérée et environnementale ?

- A : Feu dans le centre informatique
- B : Perte de documents liés à l'exploitation
- C : Perte de courant électrique dans le centre informatique
- D : Poussière dans la salle de machines

Q.9 Quel type de contrôle interne doit être mis en place pour empêcher la surveillance d'un incident ?

- A : Préventif
- B : DéTECTif
- C : Compensatoire
- D : Correctif

Q.10 Pourquoi n'est-il pas correct de voir l'enregistrement de tentatives d'intrusion comme une mesure de contrôle interne ?

- A : Parce que l'enregistrement ne concerne que des activités extérieures à l'organisation
- B : Parce qu'il est impossible de tout logger, donc les enregistrements sont par nature incomplets

- C : Parce qu'il s'agit plutôt d'une mesure de gestion de risque
- D : Parce les logs sont inutiles sans processus de révision et de remédiation

Q.11 Quel élément est le moins important pour l'analyse des impacts d'un système d'information (SI) ?

- A : L'objet du SI dans l'organisation
- B : Le nombre d'utilisateurs du SI
- C : La criticité du SI
- D : La sensibilité du SI

Q.12 Lequel n'est pas une option pour le traitement final des risques ?

- A : Acceptation des risques
- B : Évitement des risques
- C : Transfert des risques
- D : Évaluation des risques

Q.13 Quelle norme internationale traite des Critères Communs ?

- A : ISO 13335
- B : ISO 15408
- C : ISO 18028
- D : ISO 27001

Q.14 Quelle norme internationale traite les bonnes pratiques pour la gestion de la sécurité ?

- A : ISO 27002
- B : ISO 27001
- C : ISO 15408
- D : ISO 27004

Q.15 Les éléments à entreprendre pour bien gérer la sécurité incluent :

- (1) quels sont les risques ?
- (2) comment protéger l'entreprise ?
- (3) que protéger et pourquoi ?
- (4) de quoi protéger les biens ?

Dans quel ordre doit-on traiter ces questions ?

- A : 1, 2, 3, 4
- B : 2, 3, 4, 1
- C : 4, 2, 3, 1
- D : 3, 4, 1, 2

Q.16 À qui, dans une grande organisation, appartient la responsabilité de la stratégie de la sécurité de l'information ?

- A : Aux responsables de systèmes
- B : Au CISO
- C : À l'*Executive management*
- D : Au conseil d'administration

Q.17 Par quelle section de la loi Sarbanes-Oxley la gestion de l'informatique est-elle principalement concernée ?

- A : 102
- B : 302
- C : 403
- D : 404

Q.18 Dans l'application de la gestion intégrée des risques selon Bâle II, quel aspect des risques n'est pas explicitement cité ?

- A : Inhérent
- B : Crédit
- C : Marché
- D : Opérationnel

Q.19 Quel critère n'est pas nécessaire pour que les métriques liés à l'informatique soient significatifs ?

- A : Alignement avec les objectifs organisationnels
- B : Pertinence aux problèmes actuels
- C : Mesurables et liés aux coûts
- D : Facile à représenter de manière graphique

Q.20 Quel durée maximale d'interruption justifiera-t-elle la création d'un site de secours dit « *warm* » ?

- A : 1 heure
- B : 4-8 heures
- C : 24-48 heures
- D : > 48 heures

Q.21 Une infrastructure de sécurité PKI est constituée des éléments suivants :

- A : Un cryptosystème à clé publique, un cryptosystème à clé privée, et un certificat numérique
- B : Un cryptosystème à clé publique, chiffrement symétrique et autorités de certification

- C : Chiffrement symétrique, certificat numérique et authentification Kerberos
- D : Un cryptosystème à clé publique, certificat numérique et autorité de certification

Q.22 Pour un malveillant, il est plus difficile de détourner les types de contrôle d'accès basés sur :

- A : *Smart Card*
- B : Biométrie
- C : *Challenge-response token*
- D : ID de l'utilisateur et mot de passe

Q.23 Le « *digest* » d'un message obtenu par une « *one-way function* » permet :

- A : De montrer si le message a été modifié après transmission
- B : De définir l'algorithme de chiffrement
- C : De confirmer l'identité de l'émetteur
- D : La transmission du message en format numérique

Q.24 Quel est le moyen le plus important pour sécuriser logiciels et données dans un centre informatique ?

- A : Sensibilisation à la sécurité
- B : Lecture de la politique de sécurité
- C : Comité de sécurité
- D : Restrictions sur l'accès logique

Q.25 Pour rendre confidentiel un message, le chiffrement asymétrique nécessite que :

- A : L'émetteur possède une clé publique et le destinataire possède une clé privée
- B : L'émetteur possède une clé privée et le destinataire possède une clé publique
- C : L'émetteur et le destinataire possèdent tous les deux une clé publique
- D : L'émetteur et le destinataire possèdent tous les deux une clé privée

Q.26 Lors de la connexion sécurisée à un système en ligne, quel processus le système réalise-t-il le premier ?

- A : Initiation, Initialisation ou identification
- B : Vérification
- C : Autorisation
- D : Authentification

Q.27 Pour empêcher que les systèmes informatiques d'une organisation deviennent un élément d'une attaque DDoS, les paquets IP qui contiennent des adresses listées comme « non-routables » peuvent être isolés par :

- A : La mise en place de filtrage de trafic vers l'extérieur

- B : L'activation du blocage des *broadcast*
- C : La limitation des services permisibles
- D : La surveillance de la performance du réseau

Q.28 Les mots de passe devraient être :

- A : Assignés par l'administrateur de la sécurité
- B : Changés de façon régulière
- C : Réutilisés afin d'assurer que les utilisateurs ne les oublient pas
- D : Montrés sur l'écran pour que l'utilisateur puisse s'assurer que la saisie a été correcte

Q.29 Lequel des procédés suivants peut être utilisé pour capturer des mots de passe sur un réseau ?

- A : Chiffrement
- B : *Sniffing*
- C : *Spoofing*
- D : Destruction de données

Q.30 Lequel des procédés suivants est le plus efficace à détecter des intrusions ?

- A : Les identifiants et priviléges des utilisateurs sont octroyés suivant des procédures autorisées
- B : Les stations de travail inactives depuis un certain temps sont déloggées automatiquement
- C : Un certain nombre de tentatives infructueuses d'accès provoque le blocage automatique d'un compte utilisateur
- D : Les tentatives infructueuses d'accès sont surveillées par l'administrateur de sécurité

Q.31 Laquelle des propositions suivantes caractérise un système de détection d'intrusions (IDS) ?

- A : La récolte de preuves de tentatives d'attaque
- B : L'identification de faiblesses dans la définition de la politique de sécurité
- C : Le blocage d'accès à certains sites Internet
- D : Le fait d'empêcher l'accès de certains utilisateurs à certains serveurs

Q.32 Dans un certificat numérique, quel est l'élément le moins important pour les besoins d'identification par un tiers de confiance (*trusted third party* – TTP) ou par une autorité de certification (*certification authority* – CA) ?

- A : Le nom du TTP/CA
- B : La clé publique de l'émetteur
- C : Le nom du détenteur de la clé publique
- D : Le délai pendant lequel la clé est valable

Q.33 Dans un système de « *single sign-on* » (SSO), les accès non autorisés :

- A : Sont moins probables
- B : Sont plus probables
- C : Auront un plus grand impact
- D : Auront un moins grand impact

Q.34 Les procédures d'accès incluent la création d'un identifiant unique et d'un mot de passe pour chaque utilisateur. Un audit découvre que dans plusieurs cas l'identifiant et le mot de passe sont les mêmes. Le meilleur contrôle pour diminuer ce risque consiste à :

- A : Changer la politique de sécurité de l'entreprise
- B : Former les utilisateurs sur les risques liés aux mots de passe faibles
- C : Mettre en place des validations pendant les processus de création d'utilisateur et de changement de mot de passe
- D : Instaurer une révision périodique d'identifiants et mots de passe pour détecter et corriger les cas fautifs.

Q.35 La technique utilisée pour assurer la sécurité dans les réseaux privés virtuels (VPNs) est :

- A : L'encapsulation
- B : La stéganographie
- C : La transformation
- D : Le chiffrement sélectif

Q.36 Avec l'aide du responsable de la sécurité, l'octroi des droits d'accès aux données est de la responsabilité des :

- A : Propriétaires des données et systèmes
- B : Programmateurs
- C : Analystes de système
- D : Responsables de l'informatique

Solutions

10.1 La principale **difficulté** pour sécuriser un réseau de télécommunication provient de la nature même de celui-ci, et de ses caractéristiques de fonctionnement, du fait notamment :

- de la mise en commun, du partage et de la grande accessibilité des ressources ;
- du mode de fonctionnement « instantané », « dynamique », « transparent » d'un réseau ;
- de la distribution des systèmes et des processus ;
- de la couverture géographique du réseau (du local à l'international) ;
- de la nécessaire flexibilité dont il doit faire preuve (adaptation, évolution) ;
- du nombre, de la pluralité, de la diversité, de l'hétérogénéité des équipements, des ressources, des modes de fonctionnement et des acteurs ;
- des vulnérabilités intrinsèques à l'informatique ;
- du mode de contrôle réparti entre divers intervenants lors de l'interconnexion de réseaux appartenant à des domaines de gestion différents (difficulté d'obtenir un contrôle homogène de « bout en bout »).

S'il s'agit d'un réseau public, il est donc ouvert au public, c'est-à-dire à des entités dont ne sait pas *a priori* si elles sont bienveillantes ou malveillantes. On ne peut sécuriser que ce qu'on connaît. Cela se traduit par une grande complexité de l'environnement à maîtriser et à sécuriser.

10.2 Les architectures de communication doivent être évolutives, réactives, performantes et sécurisées. Elles s'inscrivent dans une politique stratégique de conception, de mise en œuvre et de gestion des technologies de l'information de l'organisation. La **gestion de réseau** intègre la gestion de la sécurité des télécommunications, qui elle-même fait partie de la sécurité des systèmes d'information. La sécurité informatique doit être appréhendée dans son intégralité et suppose que l'on sache, entre autres, gérer efficacement et de manière sécurisée les réseaux de télécommunication. L'exigence de sécurité qu'est la disponibilité des ressources et services passe par des actions de gestion des systèmes et des réseaux (dimensionnement, gestion des performances, des incidents, etc.). Les exigences de confidentialité et d'intégrité peuvent être partiellement satisfaites par la mise en œuvre du contrôle d'accès, par une bonne configuration des serveurs, des pare-feu, qui sont des tâches relevant de la gestion de réseau. La **journalisation des événements, la surveillance du trafic, la détection des incidents par exemple sont aussi des fonctions relatives à la gestion opérationnelle du réseau. Elles contribuent à la réalisation des services de sécurité.** La fonction d'assistance aux utilisateurs (*help desk*) est intégrée à la gestion de systèmes et de réseau et est également un élément au service de la sécurité.

10.3 Sécuriser un environnement informatique impose une démarche pragmatique et cohérente combinant harmonieusement deux savoir-faire complémentaires et indissociables :

- un savoir-faire conceptuel et organisationnel par le biais de la définition et de la mise en place d'une politique de gestion de réseau et d'une politique de sécurité ;

- un savoir-faire plus technique et opérationnel par la mise en place de solutions efficaces (produits, mécanismes, services de gestion et de sécurité).

L'**administrateur réseau**, comme le responsable sécurité, doit posséder des compétences organisationnelles (maîtrise des politiques, des processus, des mesures, de tous les aspects liés au management), des compétences techniques (maîtrise des outils) et des qualités humaines et des compétences juridiques. En effet, administrateur réseau et responsable sécurité doivent être notamment capables de dialoguer, de négocier, de déléguer car un système sécuritaire, aussi pertinent soit-il, ne pourra être validé que s'il est accepté par l'ensemble des acteurs de l'organisation. Cela impose donc une bonne diffusion et une bonne compréhension de la politique de sécurité au sein de l'entreprise ainsi qu'une sensibilisation adaptée aux problèmes sécuritaires (notion de plan de sensibilisation). La sécurité est également une question de « communication » et de « responsabilisation » du personnel. Si l'on considère qu'environ 80 % des sinistres ont une origine interne à l'entreprise, sécuriser les télécommunications ne suffit pas à bien protéger les ressources sensibles de l'entreprise.

10.4 L'inventaire des ressources informatiques et télécoms d'une organisation est nécessaire à la sécurité informatique parce qu'il contribue à la réalisation des services de gestion de systèmes et de réseau, gestion du parc informatique et de la sécurité. Outre le fait que l'on ne gère bien que ce que l'on connaît bien, l'inventaire contribue à la gestion des configurations, des performances, au dimensionnement et à l'exploitation-maintenance des ressources. Ces fonctions contribuent à satisfaire des besoins de disponibilité, de fiabilité et d'intégrité. De plus, l'inventaire à un rôle majeur dans l'identification des ressources et de leur degré de criticité. La classification des ressources selon leur degré d'importance permet de définir des mesures de sécurité appropriées pour les protéger. L'inventaire des ressources intervient également pour la mise en œuvre du contrôle d'accès lors notamment du processus d'identification des ressources, d'assignation des permissions (droit d'accès) en fonction du profil des utilisateurs. Ainsi, l'inventaire contribue indirectement à la réalisation de service de confidentialité et d'intégrité.

10.5 La surveillance d'un réseau informatique consiste à observer le fonctionnement de ce dernier et ceci d'une manière continue. La surveillance du réseau vise non seulement à s'assurer que la qualité de service du réseau est acceptable mais aussi à déceler les problèmes, incidents, erreurs et les anomalies qui dégradent les performances du réseau et qui pourraient porter atteinte à la sécurité des ressources afin de répondre au plus vite et de manière adaptée aux dysfonctionnements. La fonction de surveillance du réseau permet la traçabilité des actions et des événements afin de les journaliser pour les analyser dans une optique d'optimisation/amélioration mais aussi de recherche de preuves ou d'imputation. La surveillance du réseau contribue également à s'assurer de la disponibilité des ressources en vérifiant que le réseau fonctionne d'une manière correcte. Ainsi, il s'agit d'une fonction cruciale de la gestion de réseau puisqu'elle contribue à réaliser la gestion des performances, des incidents, des configurations, des utilisateurs et de la sécurité.

10.6 De manière générale la documentation des activités ou des opérations de gestion possède de la valeur dans tous les domaines d’activité d’une organisation, ce qui explique les exigences documentaires de nombreux standards, lois et réglementations. En ce qui concerne spécifiquement la gestion du réseau, un niveau approprié de documentation est primordial afin de garder la mémoire des actions qui impactent la vie du réseau et sa sécurité, mais aussi pour apprendre des événements ou incidents passés, capitaliser le savoir-faire, pour pallier l’éventuelle absence d’un employé clé, pour s’assurer que toutes les activités nécessaires sont effectuées de manière régulière et appropriée.

10.7 Oui, dans la mesure où la disponibilité (qui est un des critères de sécurité) n’a de sens que s’il est possible d’accéder à la ressource (rendue disponible par des mesures de sécurité appropriées). Rendre accessible une ressource, c’est l’ouvrir, la faire connaître, donner les moyens à des entités bienveillantes et/ou malveillantes d’y accéder, de s’y introduire... ce qui est à l’opposé du bon sens sécuritaire qui consiste à ne pas les exposer... La sécurité est en partie une question de bon équilibre entre l’accessibilité d’un réseau (y compris services et données) et la restriction des accès à ces services et données aux seules entités habilitées.

10.8 Le protocole SNMP (*Simple Network Management Protocol*) a été défini pour supporter les échanges d’information de gestion dans le contexte de la gestion de systèmes distants d’un environnement Internet. Chaque système raccordé intègre un module logiciel « agent de gestion » qui interagit à distance avec un système gérant. SNMP est le protocole d’échange d’information entre des processus agents et gérant.

10.9 Le détournement du mode de fonctionnement du protocole SNMP peut conduire à des prises de contrôle des systèmes et à la réalisation de tous types de dysfonctionnements, manipulations et leurres. Cela est d’autant plus facile que le protocole SNMP, relativement simple et élémentaire, ne supportait pas à son origine, des mécanismes d’authentification des agents et des gérants et le chiffrement des requêtes. De plus, il était souvent mis en œuvre *via* le protocole UDP (mode non sécurisé connecté). Il était donc facile d’accéder aux MIB (*Management Information Bases*) des équipements, de faire des modifications et ainsi de générer des problèmes de sécurité. Ces faiblesses ont été palliées depuis la version 3 du protocole.

10.10 Ces notions sont liées et englobées dans la sécurité au sens large. Il ne peut y avoir de sécurité sans gestion de la qualité et sans gestion de systèmes et de réseaux.

Inversement, il ne peut y avoir de qualité sans gestion de la sécurité et pour cela les systèmes et les réseaux doivent être bien gérés.

La gestion de systèmes et de réseaux concerne des installations et des procédures assez techniques et sont relatives à la sécurité opérationnelle des éléments du réseau. Elle contribue à fournir de la qualité et de la sécurité à toute l’organisation.

10.1.1 Les principaux types d'impacts « business » d'un défaut de sécurité informatique pour une organisation sont :

Impacts financiers :

- perte de ventes, commandes ou contrats ;
- perte de biens (actifs) ;
- pénalités ou devoirs légaux ;
- coûts imprévus ;
- perte de valeur de l'entreprise (chute du prix de l'action) ;
- perte d'image.

Impacts opérationnels :

- perte de contrôle par le management ;
- perte de compétitivité ;
- retards dans des nouveaux développements ;
- perte de productivité.

Impacts affectant la clientèle :

- retards de livraisons aux clients ;
- perte de clientèle ;
- perte de confiance de la part de tiers ;
- atteintes à la réputation.

Impacts affectant les employés :

- perte de moral, de productivité, de confiance ;
- atteinte à l'intégrité physique des personnes.

10.12

Tableau 10.1 – Tableau proposant pour les applications critiques d'une organisation les principaux types de mesures de sécurité à mettre en place.

Besoins du « business » pour la sécurité	Identification des valeurs
	Identification des applications critiques
	Classification des informations
	Évaluation et gestion des risques liés à l'informatique
Sécurité des ressources humaines	Accords avec les employés
	Programme de sensibilisation
	Messages de sensibilisation
	Formation en sécurité
	Définition des rôles et des responsabilités
	Coordination, contrôle et optimisation
Management des applications	Protection des applications
	Protection des applications dans les navigateurs
	Validation de l'information
	Gestion de changements
	Gestion de documents
	...
Gestion des identités et des accès	Dispositions particulières pour l'accès par la clientèle
	Identification
	Authentification
	Contrôle d'accès
	...
Gestion des systèmes	Contrats de niveau de service (Service Level Agreements – SLA)
	Résilience
	Connexions aux réseaux externes
	Sauvegarde
Cryptographie	Solutions cryptographiques
	Gestion de clés cryptographiques
Gestion d'incidents	Gestion d'incidents liés à la sécurité informatique
	Solutions d'urgence
Continuité du business	Planning pour la continuité
	Dispositions pour la continuité
	Tests du planning pour la continuité
Audit de la sécurité	Gestion de l'audit de la sécurité
	Processus de l'audit de la sécurité – planification – réalisation – restitution - suivi

10.13**Tableau 10. 2 – Tableau récapitulatif des principaux types d'incidents pouvant nuire à la sécurité d'un système d'information.**

Incidents liés à l'infection des ressources par des programmes malveillants	
Virus/ver	Programme capable d'autoduplication qui effectue des opérations non autorisées
Cheval de Troie/Rootkit	Logiciel qui cache sa présence ou dissimule sa vraie nature et qui effectue des opérations non autorisées
Clients botnet	Logiciel qui fait de l'ordinateur un membre d'un réseau virtuel utilisé pour des tâches illicites (attaques DDoS et spams)
Incidents liés au hacking	
Attaques en déni de service	Surcharge délibérée des systèmes et réseaux afin de nuire aux performances du système cible
Utilisation non autorisée de paramètres de connexion	Connexions illicites pouvant résulter de l'usurpation d'identité
Scans non autorisés de réseaux	Reconnaissance de l'infrastructure et configuration d'un réseau afin de trouver des vulnérabilités et préparer des attaques en APT
Interception de trafic non autorisée	Interception ou modification d'information qui transit sur un réseau ou entre deux réseaux
Hijacking de session	Contrôle ou manipulation d'une connexion existante à un réseau
Modification non autorisée d'un site web	Modification ou remplacement (défiguration) du contenu d'un site
Modification non autorisée de logiciel	Modification, ajout ou suppression de logiciels (programmes, code source, plugins)
Accès non autorisé ou modification des données	Accès, modification, ajout ou suppression de données sans permission
Déchiffrement non autorisé d'informations sensibles	Déchiffrement typiquement utilisant des techniques telles que mots de passe crackés ou attaques en force brute
Vol d'information d'authentification	Vol d'informations telles qu'identifiants, mots de passe, clés de chiffrement
Incidents « sociaux »	
Usurpation de marque	En prétendant être une organisation légitime, souvent par l'acquisition de domaines et de sites web frauduleux
Phishing	Acquisition de données personnelles et confidentielles par tromperie
Spam	Grands volumes de messages non sollicités, souvent à des fins commerciales
Révélation non autorisée d'information	Publication accidentelle ou délibérée d'informations telles que données de connexion ou de paiement

Chapitre 10 • La sécurité par la gestion de réseau

Tableau 10. 2 – Suite.

Incidents liés aux abus de ressources	
Modification non autorisée de priviléges d'accès	Modification avec des priviléges étendus, des droits d'accès des utilisateurs. Souvent le prélude à une attaque en APT
Activité système non autorisée	Toute utilisation, modification, destruction partielle ou totale non autorisée
Vol de logiciel	Vol de programmes, de codes sources, etc.
Vol d'information, vol de propriété intellectuelle, de savoir-faire, etc.	Vol de listes de clients, détails de produits, secrets industriels, données financières sensibles, etc.
Incidents physiques	
Accès physique non autorisé	Accès aux installations obtenu par force, effraction ou leurre
Vol ou perte d'équipements informatiques	Vol ou perte de stations de travail, serveurs, portables, téléphones, tablettes, etc.
Vol ou perte de périphériques de stockage	Vol ou perte de supports de mémorisation, clés USB, disques, appareils photos, etc.
Vol ou perte d'entités impliquées dans l'authentification	Vol ou perte de tokens, de Smart Cards, de smartphones, etc.
Incidents liés aux erreurs	
Erreurs des utilisateurs	Erreurs lors de l'utilisation d'applications ou de la transmission d'informations
Erreurs des employés techniques	Erreurs de conception, d'administration, d'implémentation, de maintenance ou opération de la part des équipes techniques
Fonctionnement défectueux de logiciel (interne)	Exécution erronée ou faille d'un logiciel développé à l'interne
Fonctionnement défectueux de logiciel (externe)	Exécution erronée ou faille d'un logiciel acheté ou développé par un tiers sur commande
Surcharge de système	Demande excessive de ressources qui provoque la dégradation des performances ou l'arrêt du système
Fonctionnement défectueux de matériel	Mauvais fonctionnement d'un ordinateur, d'un disque dur, d'un routeur, etc.
Impact non désiré d'un changement	Impact sur les systèmes et/ou sur l'information de changements apportés aux processus, à l'organisation, aux logiciels ou au matériel

Tableau 10. 2 – Suite.

Incidents environnementaux	
Risque naturel	Désastres naturels incluent orages, tremblements de terre, incendies, et les impacts de météo extrême
Dégâts physiques accidentels	Dégâts aux systèmes et aux installations provoqués par incendie ou fuite d'eau ou délabrement d'un bâtiment
Dommages physiques malveillants aux équipements	Dégâts aux systèmes et aux installations provoqués délibérément par incendie, interférence électrique ou explosion
Perte d'alimentation énergétique	Perte ou coupure de l'alimentation électrique normale ou de secours. Perte des capacités de climatisation (ventilation, refroidissement)
Dommage ou perte des communications externes	Dommage ou perte des connexions Internet, WAN, LAN, Wi-Fi ou satellite
Blocage malveillant ou interférence des communications sans fil	Interférence avec des communications Wi-Fi afin d'empêcher ou de ralentir le passage de messages et de données

36 questions, une réponse possible

Q.1 A

Q.2 A

Q.3 C

Q.4 D

Q.5 D

Q.6 A

Q.7 B

Q.8 B

Q.9 A

Q.10 D

Q.11 B

Q.12 D

Q.13 B

Q.14 A

Q.15 D

Q.16 C

Q.17 D

Q.18 A

Q.19 D

Q.20 B

Q.21 D

Q.22 B

Q.23 A

Q.24 D

Q.25 B

Q.26 D

Q.27 A

Q.28 B

Q.29 B

Q.30 D

Q.31 A

Q.32 C

Q.33 C

Q.34 C

Q.35 A

Q.36 A

GLOSSAIRE

802.11i – Norme définissant une nouvelle architecture ainsi que de nouveaux algorithmes d’authentification et de chiffrement afin de renforcer la sécurité des réseaux locaux sans fil de type 802.11.

A3 – Algorithme utilisé dans le processus d’authentification d’abonné d’un réseau GSM.

A5 – Algorithme de chiffrement utilisé dans un réseau GSM.

A8 – Algorithme utilisé dans un réseau GSM pour dériver la clé de chiffrement à partir de la clé d’authentification.

Accaparement de noms de domaine (*cybersquatting, domain name grabbing*) – Enregistrement d’un nom de domaine dans l’intention de le rendre indisponible à des titulaires légitimes et d’opérer une opération commerciale en le leur revendant.

Accident (*accident*) – Élément fortuit, imprévisible, portant atteinte à une entité.

Accord sur les clés (*key agreement*) – Méthode permettant de négocier la valeur d’une clé de chiffrement sans la transférer même sous une forme chiffrée.

Administrateur de la sécurité (*security administrator*) – Personne responsable de la définition ou de la réalisation de tout ou partie d’une politique de sécurité.

Algorithme cryptographique (*cryptographic algorithm*) – Algorithme utilisé pour le chiffrement des données afin de les rendre confidentielles, il est basé sur une fonction mathématique et sur une clé de chiffrement.

Algorithme de cryptographie asymétrique (*asymmetric cryptographic algorithm*) – Algorithme basé sur l’usage d’une bi-clé, l’une servant au chiffrement des données, l’autre au déchiffrement.

Analyse de risque (*risk analysis*), **évaluation des risques** (*risk assessment*) – Processus d’identification et d’évaluation des risques (estimation de leur probabilité d’occurrence et de leurs impacts).

Analyse des menaces (*threat analysis*) – Processus d’identification des menaces potentielles contre des ressources, qui, si elles se réalisent, leur portent atteinte.

Analyse du trafic (*traffic analysis*) – Observation et étude des flux d’information entre entités source et destination (présence, absence, volume, direction, fréquence, etc.).

Anonymat (*anonymity*) – Caractéristique d’une entité dont on ignore le nom, ou qui ne fait pas connaître son nom, propriété permettant à une entité d’utiliser des ressources sans être identifiée (*incognito*). Il devrait être possible de respecter la volonté de certains utilisateurs qui peuvent avoir une raison valable de ne pas révéler leur identité lorsqu’ils font des déclarations sur Internet afin de ne pas restreindre de manière excessive leur liberté d’expression, de favoriser l’expression libre d’informations et d’idées et d’assurer une protection contre les surveillances en ligne non autorisées par des entités publiques ou privées. En revanche, les instances de justice et de police devraient avoir la possibilité d’obtenir des informations sur les personnes responsables d’activités illicites, dans les limites fixées par le droit national, la Convention européenne des droits de l’homme, et les autres traités internationaux tels que la Convention sur la cybercriminalité.

Cybersécurité, sécurité informatique et réseaux

Antivirus – Programme de détection de codes malveillants (de virus).

Application stratégique (*major application*) – Application d'une importance déterminante, qui nécessite un haut degré de protection et qui doit être impérativement sécurisée de manière à ce qu'elle soit continuellement opérationnelle.

Architecture de sécurité (*security architecture*) – Ensemble des éléments matériels, logiciels, organisationnels et humains permettant de réaliser une politique de sécurité.

Association de sécurité (*security association*) – Dans le contexte du protocole IPSec, une association de sécurité est une connexion logique entre deux entités, dont les extrémités peuvent être authentifiées et les données qui y transitent chiffrées.

Association de sécurité RSNA (*Roburst Security Network Association*) – Association de sécurité robuste utilisée dans un réseau local de type 802.11.

Assurance (*assurance*) – Sentiment de sécurité, de confiance envers une entité, notion de garantie.

Attaque (*attack*) – Offensive, agression, action contre des personnes ou des biens leur portant atteinte. Il existe différents types d'attaques informatiques.

Attaque active (*active attack*) – Attaque qui modifie les ressources ciblées par l'attaque (atteinte aux critères d'intégrité, disponibilité, confidentialité).

Attaque bête et méchante (*smurf attack*) – Attaque par saturation, inondation, qui entraîne le plus souvent des dénis de service.

Attaque en rafale, attaque combinée (*multi-pronged attack*) – Mise en œuvre d'attaques informatiques multiples et simultanées, chacune reposant sur une méthode d'attaque différente, afin de maximiser la destruction et de dérouter les défenseurs.

Attaque logique (*logical attack*) – Attaque mettant en œuvre des ressources immatérielles et portant atteinte aux programmes et aux données.

Attaque par dictionnaire (*dictionary attack*) – Recherche de mots de passe par essais successifs de mots contenus dans des dictionnaires.

Attaque par interception, via un intermédiaire (*man in the middle attack*) – Modification, destruction, création de messages, leurre des entités.

Attaque passive (*passive attack*) – Attaque qui n'altère pas sa cible (écoute passive, atteinte à la confidentialité).

Atteinte (*breach*) – Effet ou dégradation résultant d'une agression, d'une attaque qui peut avoir des *impacts tangibles* (altération physique et matérielle, dysfonctionnement logique, désorganisation des procédures, etc.), des *impacts logiques* (non-disponibilité, perte d'intégrité, perte de confidentialité de l'information), des *impacts stratégiques* (notamment sur le plan financier, frais supplémentaires d'hébergement, de transport, de télécommunications, d'intervention d'experts, d'achat/location de matériel et progiciels, de personnels, et de sous-traitance, pertes d'exploitation [pertes de marge, de trésorerie, de clientèle], de fonds ou de biens, etc.).

Audit (*audit*) – Examen d'un environnement (systèmes, procédures, situation, organisation, etc.) en vue d'en vérifier la conformité à des dispositions préétablies et de valider s'il répond de manière optimale aux besoins qu'il doit satisfaire – Expression d'un jugement sur une situation par rapport à une situation de référence – Différents types d'audit existent en fonction de leur portée : audit financier, audit opérationnel, audit des systèmes d'information, audit de sécurité, etc. – Un **audit externe** est effectué par des auditeurs

extérieurs à l'organisation concernée par l'audit, sur demande de la direction ou d'un tiers (actionnaires, État, etc.) – Un **audit interne** est réalisé par une équipe d'auditeurs reliés fonctionnellement à la direction générale afin de vérifier le plus souvent le respect des règles et des politiques, et tester l'efficacité des procédures opérationnelles mises en œuvre dans l'organisation.

Audit de sécurité (*security audit*) – Examen méthodique de toutes les composantes et de tous les acteurs de la sécurité (politique, mesures, solutions, procédures et moyens mis en œuvre par une organisation, pour sécuriser son environnement) effectué à des fins de contrôle de conformité, d'évaluation de l'adéquation des moyens (organisationnels, techniques, humains, financiers) investis au regard des risques encourus, d'optimisation, de rationalité et de performance.

Auditabilité (*auditability*) – Propriété, pour un environnement, de permettre l'enregistrement des actions, d'événements qui occurrent afin de laisser une trace exploitable à des fins d'analyse et d'audit.

Auditeur (*auditor*) – Personne réalisant un audit.

Authenticité (*authenticity*) – Caractère de ce qui est authentique. Capacité permettant d'attester, de certifier conforme à... Souvent associé au fait qu'une information (ou un événement) n'a pas été altérée, modifiée, contrefaite et qu'elle ait été produite par l'entité qui revendique l'avoir réalisée.

Authentification (*authentication*) – Action d'authentifier. L'authentification sert à confirmer (ou non) qu'une action, déclaration, information est authentique (originale, vraie). Processus mis en œuvre notamment pour vérifier l'identité d'une entité et s'assurer que l'identité fournie correspond à l'identité de cette entité préalablement enregistrée. Fonction de sécurité contribuant à garantir la véracité d'une identité.

Authentification à clé partagée (*shared key*) – Mode d'authentification basé sur la connaissance d'une clé partagée entre deux entités, utilisé par exemple dans un réseau de type 802.11 où une station mobile doit démontrer la connaissance d'une clé secrète afin de pouvoir être authentifiée par un point d'accès du réseau.

Authentification de l'origine des données (*data origin authentication*) – Confirmation ou non du fait que la source des données reçues est identique à celle revendiquée.

Authentification de l'identité de l'abonné (*user identity authentication*) – Vérification du fait que l'identité envoyée au réseau dans le processus d'identification est bien celle de l'abonné qui est en train d'utiliser le système.

Authentification d'entité paire (*peer-entity authentication*) – Confirmation qu'une entité paire dans une association est bien celle revendiquée.

Authentification mutuelle (*mutual authentication*) – Processus qui permet une authentification réciproque et simultanée de deux entités. Ainsi par exemple, le réseau peut authentifier un abonné et ce dernier, en même temps, peut authentifier le réseau.

Autorisation (*authorization*) – Action d'autoriser, de permettre, d'habiliter. Fait de recevoir la permission de réaliser certaines actions, d'accorder des droits, d'obtenir le droit d'accès à un service, à des informations, à un système, etc.

Autorité (*authority*) – Organe du pouvoir. Fait référence le plus souvent à une entité responsable de l'émission des certificats numériques.

Autorité de certification (CA, *Certification Authority*) – Tiers partie de confiance pour la génération, la signature et la publication des certificats de clés publiques.

Autorité de sécurité (*security authority*) – Entité responsable de la définition, de l'implémentation et de la mise en œuvre d'une politique de sécurité.

Autorité du domaine de sécurité (SDA, *Security Domain Authority*) – Autorité responsable de l'implémentation d'une politique de sécurité pour un domaine de sécurité donné.

Balayage de ports (*port scanning*) – Action consistant à tester les ports d'un système afin de découvrir ceux qui permettront une intrusion.

Bastion (*bastion host*) – Système qui renforce la sécurité d'un environnement informatique (notion de fortification). Terme souvent associé aux notions de système pare-feu (*firewall*) et de zone démilitarisée (DMZ).

Besoin de sécurité (*security need*) – Pour des valeurs à protéger, identification des exigences de disponibilité, d'intégrité et de confidentialité à satisfaire par des mesures de sécurité appropriées.

Bien, valeur (*asset*) – Entité qui a un prix et qui représente pour celui qui la possède un capital, un patrimoine (notion de *bien sensible*). En matière de sécurité, il est important de déterminer les valeurs et de les classifier en fonction de leur importance, afin de mettre en place les mesures de protection nécessaires et suffisantes afin d'éviter de les perdre ou du moins de minimiser les impacts négatifs consécutifs à leur perte éventuelle.

Blockchain (chaîne de blocs) – Application particulière des techniques de chiffrement pour développer des services de confiance distribuée.

Bogue (*bug*) – Terme d'origine anglaise qui illustre une erreur de programmation. Par extension, défaut de conception ou de réalisation se manifestant par des anomalies de fonctionnement (JO 19 février 1984).

Bombardement de messages (*mail bombing, mailbombing, e-mail bombing*) – Envoi, à des fins malveillantes, d'une grande quantité de courriels pour nuire à un destinataire (dénie de service possible).

Bombe logique (*logical bomb*) – Programme malveillant qui s'active lors de la réalisation d'événements particuliers (date anniversaire par exemple) pour porter atteinte au système dans lequel il se trouve.

Botnet (réseau de machines zombies) – mot construit à partir des mots *robot* et *network* faisant référence à un ensemble de systèmes infectés, pilotés et contrôlés à distance par un malveillant, pour réaliser des attaques (notamment en déni de service).

Buffer overflow (dépassement de zone tampon) – Attaque contre un système informatique consistant à saturer une zone mémoire.

Canal caché (*covert channel*) – Canal logique de communication servant à transmettre des informations de manière cachée généralement à des fins malveillantes.

Canular (*hoax*) – Information diffusée ayant pour finalité la manipulation des personnes pour les influencer et éventuellement les conduire à effectuer des actions particulières pour le bénéfice de tierces personnes.

Capteur clavier, enregistreur de frappes (*keylogger, keystroke logger*) – Entité permettant d'enregistrer à l'insu d'une personne sa frappe au clavier et d'envoyer les informations espionnées à une tierce personne.

Carder – Action de pirater des numéros de cartes de crédit.

Cardeur (*carder*) – Pirate spécialisé dans l'utilisation de numéros de cartes de crédit obtenus de façon illicite (*via* des générateurs de numéros de cartes de crédit disponibles

sur le Web, ou par la récupération des numéros sur les justificatifs de paiement, le piratage de bases de données, etc.).

Carding (carding) – Piratage de cartes de crédit, génération ou utilisation de numéros de cartes de crédit obtenus illégalement ou du moins à l'insu du propriétaire de la carte.

Carte SIM universelle (USIM, Universal SIM) – Carte SIM utilisée dans les réseaux mobiles de troisième génération UMTS.

CBC (Cipher Block Chaining) – Méthode de chiffrement qui consiste à chiffrer un message par bloc et dont le chiffrement dépend non seulement de la clé et du texte en clair mais aussi du bloc précédent ou, lorsqu'il s'agit du premier bloc, d'un vecteur d'initialisation.

CCMP (CTR with CBC MAC Protocol) – Algorithme de chiffrement standard utilisé dans le réseau 802.11i.

Centre d'authentification (AuC, Authentication Center) – Centre d'authentification d'un réseau GSM. Cette entité est la seule entité qui peut accéder aux clés d'authentification des abonnées stockées dans la base de données HLR pour les authentifier. En pratique, le centre d'authentification et la base de données HLR sont physiquement associés. Ils sont souvent notés ensemble HLR/AuC.

Certificat (certificate), certificat de clé publique (public-key certificate) – Ensemble des données émises par une autorité de certification (tiers de confiance) qui permet de réaliser des services de sécurité (confidentialité, authentification, intégrité). Un certificat dit numérique fait référence à la mise en œuvre du chiffrement à clé publique. En effet, dans un certificat se trouve entre autres la valeur de la clé publique de son propriétaire, qui est attestée par le fait que le certificat est signé par l'autorité de certification émettrice.

CHAP (Challenge-Handshake Authentication Protocol) – Protocole d'authentification par défî-reponse dans lequel le message de réponse est généré en ajoutant un secret partagé ainsi qu'une fonction de hachage (*hash function*).

Charte d'utilisation (user charte) – Document établi par une organisation précisant les droits, les devoirs et la responsabilité de ses employés au regard de l'utilisation des ressources informatiques et télécoms qu'elle met à leur disposition, signé par les parties concernées. Se trouvent ainsi spécifier, par exemple, les conditions d'accès et d'utilisation de l'informatique et des services Internet, les règles de sécurité, de bon usage, les conditions de confidentialité, les moyens d'analyse et de contrôle de l'utilisation des ressources, les dispositions légales, les sanctions encourues si elles ne sont pas respectées, etc.

Cheval de Troie (Trojan horse) – Programme malveillant introduit subrepticement dans des systèmes pour en prendre le contrôle (vol de temps processeur, altération, modification, destruction des données et programmes, dysfonctionnements, écoutes illicites, etc.).

Chiffrement de bout en bout (end-to-end encipherment) – Chiffrement des données à leur source et déchiffrement à leur destination finale, sans déchiffrement intermédiaire. Contrairement au **chiffrement lien par lien (link-by-link encipherment)** ou encore chiffrement de liaison) où les données chiffrées à la source sont déchiffrées dans les systèmes relais afin d'en assurer l'acheminement, puis rechiffrées avant d'être retransmises sur le lien de sortie. De ce fait, les données sont en clair dans les systèmes intermédiaires.

Chiffrement, cryptage, encodage (encipherment, encryption) – Le chiffrement est une transformation cryptographique des données (*cryptogramme*) afin d'en assurer la confidentialité. Cela consiste à rendre les données incompréhensibles à tous ceux qui ne détiendraient pas

la clé de déchiffrement. Un texte en clair est chiffré à l'aide d'un algorithme et d'une clé de chiffrement, afin d'obtenir un texte chiffré, qui pourra être déchiffré à l'aide d'une clé de déchiffrement correspondante (sauf dans le cas où le chiffrement est irréversible). Le **déchiffrement** (*decipherment, decryption*) est l'opération inverse au chiffrement.

Chiffrement homomorphe (*homomorphic encryption*) – Capacité à pouvoir réaliser des traitements sur des cryptogrammes sans avoir accès aux données en clair.

Cible d'évaluation (*evaluation target*) – Entité qui est soumise à une évaluation de la sécurité.

Cible de sécurité (*security target*) – Terme relatif à la certification par les « Critères Communs » d'une entité. Spécification de la sécurité qui est exigée d'une cible d'évaluation et qui sert de base pour l'évaluation de son niveau de sécurité. La cible de sécurité doit spécifier les fonctions dédiées à la sécurité de la cible d'évaluation. Elle spécifie les objectifs de sécurité, les menaces qui pèsent sur ces objectifs ainsi que les mécanismes de sécurité particuliers qui sont employés.

Clé (*key*) – Clé de chiffrement ou de déchiffrement, il s'agit généralement d'une valeur mathématique fournie à un algorithme de chiffrement. Sauf s'il s'agit d'une clé publique, une clé de chiffrement est à gérer comme un secret. Ainsi, il faut protéger un secret (la clé) qui permet de protéger un autre secret (l'information qui a été chiffrée pour être confidentielle).

Clé de session (*session key*) – Clé secrète générée via un système de chiffrement asymétrique par les correspondants lors de l'établissement d'une session de travail, dont la durée de vie est limitée à cette session, servant à chiffrer des gros volumes d'informations avec un algorithme de chiffrement symétrique.

Clé privée (*private key*) – Clé utilisée dans les mécanismes de chiffrement asymétrique (ou chiffrement à clé publique) qui appartient à une entité et qui doit être secrète.

Clé privée principale (*root private key*) – Clé privée de plus haut niveau d'une autorité de certification, normalement utilisée pour signer les certificats numériques d'autorités de certification de plus bas niveaux ou d'autres entités.

Clé publique (*public key*) – De manière générale, en cryptographie asymétrique, la clé publique d'une entité doit être rendue publique aux interlocuteurs qui souhaitent lui envoyer des données chiffrées afin qu'elle puisse les déchiffrer avec sa clé privée correspondante.

Clé secrète (*secret key*) – Clé utilisée avec un algorithme de chiffrement symétrique et qui doit impérativement être secrète (privée) pour son propriétaire. Elle permet de chiffrer et de déchiffrer.

Clé WEP (*Seed WEP*) – Clé utilisée avec l'algorithme WEP, constituée de 24 bits du vecteur d'initialisation et de 40 bits de clé secrète partagée entre le mobile et le réseau. Cette clé WEP sert d'entrée à l'algorithme RC4 pour générer une séquence de clés qui est ensuite utilisée pour chiffrer les données utilisateurs.

Clonage de serveur DNS (*DNS pharming*) – modification des informations d'adressage enregistrées dans un serveur DNS (serveur de noms de domaine), afin d'effectuer des redirections vers des systèmes autres que ceux qui sont légitimes (contrôlés par des malveillants) et de leurrer les internautes en leur faisant croire qu'ils ont atteint les serveurs souhaités.

Code (*cipher*) – Algorithme de chiffrement qui permet de transformer un texte clair en un texte chiffré.

Compteur TKIP (TSC-TKIP Sequence Counter) – Valeur de séquence dans l'algorithme TKIP qui est unique pour chaque trame envoyée.

Condensat, résumé, digest (*digest*) – Résultat sous forme de chaîne de caractères, de l'application d'une fonction de hachage sur une suite d'informations.

Confiance (*trust*) – Assurance de celui qui se fie à quelqu'un, à quelque chose (critère qualitatif, suggestif, très relatif). Terme relativement à la mode en matière de sécurité, faisant référence le plus souvent à la fiabilité. Ainsi par exemple, une entité Pif a confiance en une entité Hercule pour un ensemble d'activités, si Pif est sûr qu'Hercule se comportera d'une manière particulière en ce qui concerne ces activités. Bâtir la confiance dans un environnement numérique passe en autres par la mise en place de mesures de sécurité pertinentes. La **confiance dans l'efficacité des fonctions** (*functions efficiency trust*) se base sur l'estimation que les fonctions et les mécanismes dédiés à la sécurité satisfont les objectifs déclarés. La **confiance dans la conformité** (*compliance trust*) exprime le degré de crédit que l'on accorde dans la réalisation des fonctions et **des** mécanismes dédiés à la sécurité (développement et exploitation). **Fonctionnalité de confiance** (*trusted functionality*) : fonctionnalité perçue comme étant correcte par rapport à certains critères, par exemple comme établie par la politique de sécurité.

Confidentialité de l'identité de l'abonné – Propriété qui prévient la divulgation de l'identité de l'abonné aux individus, entités ou processus non autorisés.

Confidentialité (*confidentiality*) – Maintien du secret des informations et des transactions. Caractère de ce qui est secret. Objectif de sécurité à réaliser afin de prévenir la divulgation non autorisée d'informations à des tiers, qui doit permettre leur protection contre des lectures, écoutes, copies illicites d'origines intentionnelle ou accidentelle durant leur stockage, traitement et transfert (notion de **confidentialité de données** [*data confidentiality*]).

Confidentiel défense (*top secret*) – Se dit des informations qui ne présentent pas en elles-mêmes un caractère secret mais dont la connaissance, la réunion ou l'exploitation peuvent conduire à la divulgation d'un secret intéressant la Défense nationale et la sûreté de l'État.

Conformité (*compliance*) – Caractère de ce qui est conforme, qui est en concordance, qui ressemble à..., conformité à certaines normes.

Contenu actif (*active content*) – Programme ou script au format HTML.

Contexte de sécurité – Ensemble des éléments nécessaires pour assurer les services de sécurité.

Contournement de la politique de sécurité – événement ou action qui passent outre les mesures de sécurité définies par la politique de sécurité. Contexte qui ne permet pas l'application de la politique.

Contre-mesure (*counter measure*) – Fonction, mesure, procédure ou mécanisme dédié à la sécurité d'un système afin d'en réduire le niveau de vulnérabilité et de contrer une menace avant qu'elle ne se concrétise en action malveillante.

Contrôle d'accès (*access control*) – Mécanisme permettant de prévenir de l'utilisation non appropriée ou non autorisée d'une ressource (services, systèmes, données, programmes).

Contrôle du routage (*routing control*) – Application de règles pendant le processus de routage de façon à choisir ou à éviter des réseaux, liens ou relais spécifiques.

Cybersécurité, sécurité informatique et réseaux

Cookies – Fichiers envoyés sur le poste de travail des internautes à leur insu, lors de l'accès à certains sites web, qui récoltent des informations les concernant pour, en principe, la personnalisation des services web offerts.

Correctif de sécurité (patch) – Rustine de sécurité d'un logiciel pour en supprimer une vulnérabilité qui a été identifiée après son installation.

Crackeur (cracker) – Personne qui, pour s'introduire dans des systèmes, casse les mots de passe des utilisateurs habilités ou les protections mises en place (notion de « cracker », de « déplomber » la protection d'un logiciel). Par extension, le déplombage d'un logiciel est la suppression de ses protections.

Cryptanalyse (cryptanalysis) – La cryptanalyse comprend l'ensemble des moyens qui permettent d'analyser une information préalablement chiffrée, afin de la déchiffrer. Plus un système de chiffrement est robuste, plus sa cryptanalyse est difficile.

Cryptogramme (cryptogram, ciphertext) – Ensemble de données ayant subi une transformation cryptographique, données chiffrées, texte ou message chiffré. Données obtenues par chiffrement.

Cryptographie (cryptography) – Application des mathématiques permettant d'écrire de l'information de manière à la rendre inintelligible à ceux ne possédant pas les capacités de la déchiffrer. Voir *Chiffrement*.

Cryptographie à clé publique (public key cryptography) – Système de chiffrement asymétrique qui utilise un couple de clés, appelé *bi-clé*, composé d'une clé privée secrète et d'une clé publique, publiable. Ces deux clés sont complémentaires et indissociables. La relation mathématique qui les relie ne permet pas de retrouver la clé secrète à partir de la clé publique.

Cryptologie – Science du secret qui englobe la cryptographie et la cryptanalyse.

Cryptopériode (cryptographic period) – Période de temps pendant laquelle les clés d'un système restent inchangées.

Cyberattaque (cyberattack) – Attaque informatique réalisée à distance, *via* les technologies de l'Internet sur des systèmes connectés à Internet.

Cybercriminalité (cybercriminality) – Criminalité s'exprimant *via* les technologies de l'information et de l'Internet. L'ordinateur et le réseau sont des moyens et/ou des cibles de la criminalité.

Cyberdéfense (cyberdefence) – Concept de sécurité nationale et militaire d'un État qui tient compte du cyberspace, des technologies de l'information, des besoins de protection et de défense de ses infrastructures vitales et de l'évolution de la manière de faire la guerre, y compris par des moyens non militaires. La cyberdéfense englobe les concepts d'information offensive et défensive.

Cyberespace (cyberspace) – Espace créé par l'humain, résultant de la mise en réseau des ordinateurs et de la dématérialisation de l'information et des activités.

Cyberpouvoir (cyberpower) – Pouvoir conférer par la maîtrise du cyberspace et de la cybersécurité ou encore par la maîtrise des technologies de l'information et de la communication et l'exploitation de leurs vulnérabilités.

Cyberrésilience (cyberresilience) – Capacité à résister à des cyberattaques État d'un environnement informatique connecté à Internet suffisamment robuste pour résister à des événements portant atteinte à sa sécurité et continuer à opérer.

Cybersécurité (*cybersecurity*) – Sécurité informatique et réseaux appliquée au cyberspace, aux activités et services en ligne et aux systèmes d'information ouverts sur Internet.

DDoS (*Distributed Denial of Service*) – Attaque par saturation (ou déni de service) lancée simultanément à partir de plusieurs systèmes.

Deamon dialer – Programme qui appelle systématiquement un numéro de téléphone et qui peut être utilisé dans le cadre d'une attaque par déni de service.

Défiguration (*defacement*) – Modification mal intentionnée des données d'un site web portant préjudice à l'intégrité, à l'image et à la réputation du site.

Degré d'acceptabilité du risque (*acceptability level of risk*) – Élément à prendre en considération lors de l'établissement d'une politique de sécurité qui permet de décider des mesures de sécurité à mettre en place en fonction de la probabilité d'apparition du risque et du niveau de gravité de son impact. Il permet de quantifier le risque selon le fait qu'il est acceptable, moyennement acceptable, peu acceptable, difficilement acceptable ou inacceptable. Il constitue un élément de décision pour le choix et la mise en œuvre des mesures de sécurité.

Délégation (*delegation*) – Transfert de priviléges détenus par une entité, à une autre.

Démonstration de faisabilité (*Proof of Concept, PoC*) – Action réalisée pour démontrer la faisabilité d'une opération, éventuellement d'une attaque exploitant une vulnérabilité.

Déni de service (*Denial of Service, DoS*) – Attaque par saturation d'une entité afin qu'elle s'effondre et ne puisse plus réaliser les services attendus d'elle.

DES (*Data Encryption Standard*) – Algorithme de chiffrement symétrique d'origine américaine adopté par le NIST (*National Institute of Standards and Technology*) en 1977. Les données sont chiffrées par blocs de 64 bits avec une clé de 56 bits. Il est largement répandu et utilisé pour des applications financières. Il est souvent mis en œuvre en un mode dit de chaînage de blocs (CBC, *Cipher Block Chaining*), où le chiffrement d'un bloc dépend du précédent.

Détenteur (*holder*) – Entité qui détient certains priviléges.

Discretion (*discretion*) – Les solutions et mesures de sécurité implantées ne doivent pas être provocantes afin de ne pas tenter un attaquant potentiel.

Disponibilité (*availability*) – Critère de sécurité permettant que les ressources soient accessibles et utilisables selon les besoins (pas de refus d'accès autorisé aux systèmes, services, données, infrastructures, etc.).

Dissuasion (*dissuasion*) – Mesure destinée à persuader une personne à renoncer à effectuer une malveillance, par intimidation ou en la persuadant que la valeur de l'enjeu qu'elle convoite est inférieure à celle des dommages que le système menacé pourrait lui infliger.

Divulgation d'informations (*information disclosure*) – Utilisation non autorisée des ressources du système d'information, entraînant la divulgation à des tiers d'informations confidentielles.

DLP (*Data Loss [ou Leak] Prevention*) – Ensemble de techniques de protection contre la fuite d'informations.

Domaine de sécurité (*security domain*) – Domaine d'application, ensemble des ressources d'une politique et des mesures de sécurité gérées par une autorité particulière.

Cybersécurité, sécurité informatique et réseaux

DSA (*Digital Signature Algorithm*) – Algorithme défini conjointement par le NIST (*National Institute of Standards and Technology*) et la NSA (*National Security Agency*) aux États-Unis en 1994.

DSS (*Digital Signature Standard*) – Standard d'origine américaine spécifiant la manière de réaliser une signature numérique.

EAP (*Extensible Authentication Protocol*) – Protocole d'authentification du protocole PPP (*Point to Point Protocol*) avec possibilité d'extension qui permet aux utilisateurs de sélectionner un protocole d'authentification parmi une liste. Utilisé dans l'authentification 802.1x.

Échange d'authentification (*authentication exchange*) – Mécanisme permettant de s'assurer de l'identité d'une entité par le biais d'échange d'information.

Échange de clé (*key exchange*) – Échange de clés parfois nécessaire au chiffrement de données entre deux entités.

Efficacité (*efficiency*) – Caractère de ce qui produit l'effet attendu, des résultats utiles. Propriété des mesures de sécurité qui assure leur pertinence et leur capacité à réellement bien protéger une ressource.

Elévation de privilège (*privilege escalation*) – Octroi de privilège et de droits d'accès de manière incrémentale, souvent réalisé de manière sournoise par un malveillant en exploitant des vulnérabilités technique et humaine afin de prendre le contrôle des systèmes.

Empreinte numérique (*digest*) – Voir *Condensat*.

Enregistreur de localisation nominal (HLR, *Home Location Registrar*) – Base de données contenant les profils (notamment la clé d'authentification et l'identité internationale) et les localisations actuelles des abonnées d'un réseau GSM.

Enregistreur de localisation visité (VLR, *Visitor Location Registrar*) – Base de données, associée à un commutateur mobile d'un réseau GSM, contenant des informations (notamment les triplets et la correspondance IMSI-TMSI) des stations mobiles qui sont desservies par ce commutateur.

Espioniciel (*spyware*) – Programme « espion, mouchard » installé à l'insu du propriétaire d'une machine dont la finalité est de surveiller ses activités, de copier des données et de les transmettre à des tiers.

Éthique (*ethics*) – Qui concerne les principes de la morale. Ensemble de règles morales adoptées par une communauté.

Exploit (*exploit*) – Code informatique tirant partie des vulnérabilités d'un système à des fins malveillantes.

Extension (en-tête) d'authentification (AH, *Authentication Header*) – Option des protocoles IPSec et IPv6 qui permet d'assurer l'intégrité des données, l'authentification de la source et de la destination, ainsi que de se prémunir des attaques de type rejet.

Extension de confidentialité et d'authentification (ESP, *Encapsulating Security Payload*)
– Option des protocoles IPSec et IPv6 qui permet la réalisation de mécanismes de chiffrement pour rendre confidentiel le contenu du paquet ainsi que le flux. Optionnellement, l'ESP propose des services d'authentification similaires à ceux proposés par l'*Authentication Header* (AH).

Fiabilité (*reliability*) – Aptitude d'un système à fonctionner sans incident pendant un temps donné.

Finger – Programme qui permet de connaître les noms de tous les comptes présents sur un serveur.

Flaming – Technique qui consiste, pour affecter la crédibilité d'un groupe de discussions, à y envoyer un grand nombre de messages peu pertinents.

Flooding – Type de moyen d'intrusion dans des systèmes qui est basé sur le cassage de mots de passe des utilisateurs.

Floudeur (flooder) – Programme malveillant servant à ralentir les communications entre un fournisseur d'accès et un internaute ou à déconnecter ce dernier.

Fonction à sens unique (one-way function) – Fonction mathématique appliquée à des données (entrée de la fonction) qui donne un résultat. Normalement, il est impossible, à partir de ce résultat, de retrouver la valeur des données spécifiées en entrée pour l'obtenir.

Fonction de hachage (hash function) – Dans le contexte du chiffrement, cette fonction est qualifiée également de fonction *digest*. Elle permet de générer, à partir de données qui lui sont fournies en entrée, leur résumé (sorte d'empreinte numérique [*digest*]), plus court que le message original et incompréhensible. Ce résumé peut être ensuite chiffré avec la clé privée de l'émetteur et associé au message à transmettre. Sur réception du message et de son empreinte, le destinataire déchiffre cette dernière avec la clé publique de l'émetteur, puis recalcule à partir du message reçu, avec la même fonction *hash*, l'empreinte, et la compare ensuite avec celle reçue. Si le résultat est identique, le destinataire a ainsi vérifié l'identité de l'émetteur et est assuré de l'intégrité du message. En effet, si le message est altéré, même légèrement, son empreinte est alors considérablement modifiée.

Fonction de hachage à sens unique (one-way hash function) – Fonction permettant de calculer l'empreinte de données, mais pas d'engendrer des données qui ont une empreinte particulière. Cette fonction ne doit pas produire des collisions, c'est-à-dire qu'une même empreinte puisse être générée à partir de différents messages.

Fraude (fraud) – Utilisation non autorisée et détournement des ressources du système d'information, conduisant à un préjudice. Les vols des services sans fil, satellites, ou de lignes terrestres sont des exemples de **fraude aux télécommunications**. La fraude d'enchère, le non-paiement ou la non-livraison des marchandises sont des exemples de **fraude de confiance** qui peuvent se réaliser aux travers des services marchands d'Internet. La fraude aux cartes de crédit/débit est un exemple de **fraude aux institutions financières**. L'usurpation d'identité est également une fraude.

Fréquence d'apparition (apparition frequency) – Paramètre pris en compte dans l'appréciation de l'impact d'un risque permettant de quantifier le nombre de fois où l'événement survient durant une période donnée (exemple de fréquence : une fois par an, par mois, par semaine, plusieurs fois par jour).

Gravité de l'impact (impact gravity) – Appréciation du niveau de gravité d'un incident, pondéré par sa fréquence d'apparition. Il est important de pouvoir quantifier ce critère d'impact afin d'identifier au mieux les impératifs de sécurité et les degrés d'urgence de la prise en considération de ces impératifs (exemple de quantification : impact de gravité insignifiante : (1) sans gravité, (2) peu grave, (3) très grave, (4) extrêmement grave).

Hacker, hackeur (hacker) – Action consistant à s'introduire de manière illicite dans un système. Personne qui, quelle que soit sa motivation, pénètre sans autorisation et de manière illégale dans un système appartenant à un tiers.

Hacking – Ensemble des opérations permettant une intrusion dans un système informatique.

Cybersécurité, sécurité informatique et réseaux

Hameçonnage (phishing) – Procédé de leurre des internautes pour les amener à réaliser certaines actions (consultation de sites web contrôlés par des malveillants, etc.) ou à livrer des informations qu'ils n'auraient pas données s'ils n'avaient pas été abusés (informations confidentielles, personnelles, etc.).

Homologation (accreditation) – Autorisation d'utiliser, dans un but précis ou dans des conditions prévues, un produit ou un système. C'est l'autorité responsable de la mise en œuvre du produit ou du système qui délivre cette autorisation, conformément à la réglementation en vigueur.

IDEA (International Data Encryption Algorithm) – Algorithme de chiffrement symétrique développé en 1990, conjointement par des chercheurs de l'École polytechnique fédérale de Zurich et de la société Ascom, notamment utilisé par le protocole de messagerie sécurisée PGP (*Pretty Good Privacy*).

Identification (identification) – Processus qui permet de reconnaître une entité préalablement identifiée.

Identité (identity) – Information qui permet de désigner et de distinguer, si possible de manière unique et non ambiguë, une entité à l'intérieur d'un domaine de nommage.

Identité internationale d'abonné (IMSI, International Mobile Subscriber Identity) – Identité internationale, qui est unique pour chaque abonné du réseau GSM. La notion d'IMSI est utilisée aussi dans les réseaux GPRS et UMTS.

Identité temporaire d'un mobile (TMSI, Temporary Mobile Station Identity) – Identité temporaire attribuée à une station mobile du réseau GSM afin d'éviter l'envoi de l'identité internationale de l'abonné sur le lien radio.

Identité temporaire d'un mobile en mode paquet (P-TMSI, Packet TMSI) – Identité temporaire attribuée à une station mobile du réseau GPRS ou UMTS afin d'éviter l'envoi de l'identité internationale de l'abonné sur le lien radio.

IKE (Internet Key Exchange) – Protocole responsable non seulement de l'échange de clés authentifiées, mais aussi de la gestion des associations de sécurité en général.

Impact (impact) – Exprime le niveau des conséquences produites par une atteinte : **impact financier (financial impact)** : coût de l'atteinte ; **impact logique (logical impact)** : atteinte aux critères de disponibilité, d'intégrité, de confidentialité ; **impact stratégique (strategical impact)** : atteinte préjudiciable à la survie d'une organisation ; **impact tangible (tangible impact)** : atteinte que l'on peut directement et facilement constater.

Imputabilité (imputability) – Propriété qui permet d'imputer de façon certaine une opération à un utilisateur à un moment donné. Fait de pouvoir identifier un responsable en cas de violation du règlement.

Information classifiée (classified information) – Information sensible dont la divulgation ou l'accès non autorisé pourrait nuire à la sécurité d'un pays ou d'une organisation.

Infrastructure de gestion clés (IGC ou PKI, Public Key Infrastructure) – Infrastructure de support à la réalisation de la mise en œuvre du chiffrement asymétrique (à clé publique) offrant entre autres des services de gestion et de distribution de clés de chiffrement et de certificats numériques.

Infrastructure de management des privilèges (PMI, Privilege Management Infrastructure) – Infrastructure capable de supporter la gestion des privilèges, permissions ou habilitations.

Ingénierie sociale (*social engineering*) – Ensemble des techniques utilisées par des malveillants pour obtenir des informations auprès des personnes afin de leurrer des systèmes informatiques ou de contourner les mesures de sécurité. Capacité à exploiter les failles humaines, pour ensuite réaliser des cyberattaques, pouvant faire appel à la manipulation, à l'intimidation, à l'écoute, à la surveillance de données, à l'escroquerie, à l'exploitation des données publiées sur des réseaux sociaux (*open source intelligence*), à celle de la crédulité ou de la naïveté des internautes par exemple.

Innocuité (*safety*) – Qualité de ce qui n'est pas nuisible.

Intégrité (*integrity*) – État d'une chose qui est demeurée intacte. Critère de sécurité qui, s'il est réalisé, permet de s'assurer qu'une ressource n'a pas été altérée (modifiée ou détruite) d'une façon non autorisée.

Intelligence économique – Capacité à maîtriser l'information stratégique (recherche, collecte, traitement) à des fins de performance et de compétitivité économiques.

Intranet (*Intranet*) – Réseau interne, réseau privé à une organisation, utilisant les technologies d'Internet et généralement isolé d'Internet par des systèmes pare-feu.

Intrusion (*intrusion*) – Accès non autorisé dans un environnement privé.

IPSec (*Internet Protocol Security*) – Version du protocole IP qui offre des services de sécurité. IPSec permet de créer un canal logique de communication (tunnel IP), au travers de l'Internet public, entre deux correspondants. Les extrémités du tunnel sont authentifiées et les données qui y transitent peuvent être chiffrées (notion de canal chiffré ou de réseau virtuel).

IPv6 (*Internet Protocole version 6*) – Évolution de la version 4 du protocole IP, qui, entre autres, intègre en mode natif des mécanismes permettant de réaliser des services de sécurité (authentification des entités source et destination, confidentialité des données transmises).

Jeton d'authentification (*authentication token*) – Information transmise durant un échange d'authentification contribuant à authentifier un correspondant.

Jeton de sécurité (*security token*) – Information utilisée dans la mise en œuvre de certains services de sécurité.

Kerberos – Serveur dédié permettant d'offrir un service d'authentification aux applications. Concept développé au MIT (*Massachusetts Institute of Technology*) repris par la communauté Internet (RFC 1510 Kerberos, version 5).

Label de sécurité (*security label*) – Marquage lié à une ressource qui nomme ou désigne les attributs de sécurité de cette ressource.

Liste de contrôle d'accès (*access control list*) – Liste d'entités, avec leurs droits d'accès, qui sont autorisées à avoir accès à une ressource.

Liste de révocation de certificat (CRL, *Certificate Revocation List*) – Liste signée par une autorité de certification identifiant des certificats numériques qui ne sont plus valides par l'émetteur du certificat. Liste qui répertorie tous les numéros de série des certificats numériques révoqués par une autorité de certification donnée.

Liste de révocation de certificat indirecte (*indirect CRL*) – Liste de révocation qui contient des informations de révocation concernant des certificats qui ont été émis par d'autres autorités que celle qui a émis cette liste.

Liste de révocation de l'autorité de certification (*certification authority revocation list*) –

Liste contenant une liste de certificats à clé publique émis par des autorités de certification, qui ne sont désormais plus considérés comme valide par l'émetteur du certificat.

Logiciel espion (*spyware*) – Programme qui envoie à un malveillant des informations sensibles depuis l'ordinateur compromis.

Logiciel malveillant (*malware*) – Terme générique désignant un programme de type virus, ver, cheval de Troie, etc. ou toute autre forme de code informatique dont l'exécution porte atteinte à la sécurité d'un système.

Mail harvesting (récolte d'adresses de messagerie) – Opération consistant à obtenir des adresses de messagerie électronique afin le plus souvent de les revendre et de les utiliser à des fins malveillantes (diffusion de spams, virus, canular, etc.).

Malveillance (*malevolence*) – Actions à caractère hostile et nuisible portant atteinte aux biens et aux valeurs, éventuellement acte criminel.

Man-in-the-Middle – (homme du milieu) – Caractérise une attaque informatique qui consiste à ce qu'une entité malveillante intercepte une communication légitime et se substitue à un des interlocuteurs pour leurrer ces derniers.

Management des clés (*key management*) – Gestion des clés de chiffrement, génération, distribution, archivage, destructions des clés en fonction de la politique de sécurité.

Management du risque, gestion des risques (*risk management*) – Processus continu d'évaluation des risques encourus par une organisation afin de les maîtriser, de les réduire à un niveau acceptable. Permet de déterminer la politique de sécurité la plus adaptée à la protection des valeurs de l'organisation.

Marion – Une des premières méthodes d'analyse des risques et d'optimisation par niveaux, élaborée par le Clusif (Club de la Sécurité de l'Information Français), qui contribue à la définition d'une politique de sécurité.

Mascarade (*masquerade*) – Type d'attaque basée sur le leurre des systèmes.

MCO (maintien en conditions opérationnelles) – Partie du plan de continuité des activités (PCA) qui décrit les mesures décidées pour garantir, en cas de crise, le basculement d'applications vers un environnement dégradé n'induisant pas une altération non acceptable des conditions de travail.

Menace (*threat*) – Signe, indice, qui laisse prévoir un danger. Action ou événement susceptible de se produire, de se transformer en agression contre un environnement et de porter préjudice à sa sécurité. Menaces délibérées (attaques), menaces involontaires (erreurs, défaillances, événements naturels, etc.), menaces connues, inconnues, etc., **menace active** (*active threat*), menace d'un changement délibéré et non autorisé de l'état du système (modification d'un message, génération de faux messages, déni de service, etc.) ; **menace passive** (*passive threat*), menace d'une divulgation d'information confidentielle, sans modification de l'état du système.

Mesures de sécurité (*security measures*) – Ensemble de moyens technologiques, organisationnels, juridiques, financiers, humains, procéduraux et d'actions permettant d'atteindre les objectifs de sécurité fixés par la politique de sécurité. Les mesures sont généralement classifiées selon leur rôle fonctionnel (ex. : mesure de prévention, de protection, de dissuasion, etc.).

Mirroring – Technique de sécurité contribuant à la disponibilité des données et à la continuité des services dans la mesure où les données sont sauvegardées en parallèle sur

plusieurs disques rattachés à un même contrôleur de disque. Si l'un des disques tombe en panne, les données ne sont pas perdues.

Mot de passe (*password*) – Information confidentielle que doit produire un ayant droit afin de prouver son identité lors d'une procédure d'authentification dans le cadre d'une demande d'accès à une ressource.

Non-répudiation (*non-repudiation*) – Capacité de prévenir le fait qu'un expéditeur démente plus tard avoir envoyé un message ou effectué une action. Assure la disponibilité de preuves qui peuvent être présentées à un tiers et utilisées pour prouver que tel type d'événement ou d'action a eu lieu. Preuve qu'un message a été envoyé par une personne précise à un moment précis, sans avoir été modifié depuis son envoi. Cette preuve devrait pouvoir être vérifiée à tout moment par un tiers. Sans la non-répudiation, des émetteurs et des récepteurs d'informations pourraient nier les avoir reçues ou envoyées.

No-opt – Service dans lequel les clients n'ont pas le choix sur la façon dont les informations les concernant sont utilisées (possibilité d'atteinte à la protection des données privées).

Notarisation (*notarization*) – Enregistrement de données à des fins de preuve.

Numéro de série de certificat (*certificate serial number*) – Paramètre d'identification non ambigu d'un certificat numérique, attribué par l'autorité de certification émettrice du certificat.

Oakley – Protocole d'authentification mutuelle avec échange de clé, qui peut être utilisé dans le cadre de la version sécurisée du protocole IP.

Panne (*failure*) – Dysfonctionnement, arrêt de fonctionnement entraînant l'indisponibilité d'une ressource.

Pare-feu (*firewall*) – Matériel ou logiciel permettant de réaliser le cloisonnement d'environnements informatiques, le masquage des ressources, le filtrage des données (en entrée et en sortie) afin de contribuer à leur protection.

PCA (plan de continuité d'activité, *continuity plan*) – Ce plan doit permettre un fonctionnement du système d'information et un accès à l'information, même en mode dégradé ou en situation de crise.

Perte de service essentiel (*lost of essential services*) – Indisponibilité ou dysfonctionnement total ou partiel de ressources nécessaires au bon fonctionnement d'un système, d'une organisation.

Pertes directes (*direct losses*) – Pertes identifiables directement consécutives à un défaut de sécurité.

Pertes indirectes (*indirect losses*) – Pertes générées indirectement par un défaut de sécurité.

PGP (*Pretty Good Privacy*) – Logiciel de messagerie offrant des services de sécurité comme l'authentification par la signature digitale ou la confidentialité.

Photuris – Protocole d'authentification mutuelle avec échange de clé, développé pour IP.

Phraker – Personne qui réalise des actes de *phreaking* (détournement des télécommunications) et de *hacking* (intrusion dans les systèmes).

Phreak – Utilisation illégale ou détournement, aux dépens d'un individu ou d'un opérateur, des services de télécommunication, par un *phreaker* (notion de *phreaking*).

Pirate, malveillant, attaquant (*hacker*) – Personne qui s'introduit illégalement dans des systèmes afin de réaliser des attaques passives ou actives.

Cybersécurité, sécurité informatique et réseaux

Plan de gestion de crise (*emergency plan*) – Ensemble des moyens techniques et organisationnels prévus pour répondre de manière optimale à un incident grave affectant la bonne marche des opérations et préjudiciable à l'organisation.

Plan de reprise d'activité (PRA) – Ce plan permet d'assurer, après une crise, une remise en route des applications, et la reconstruction de l'infrastructure qui permet l'accès à l'information.

Plan de secours (*back-up plan*) – Ensemble des moyens techniques et organisationnels prévus pour assurer la pérennité des informations et la continuité des activités quels que soient les problèmes rencontrés.

Politique de sécurité (*security policy*) – Référentiel de sécurité établi par une organisation, reflétant sa stratégie de sécurité et spécifiant les moyens de la réaliser.

Porte dérobée (*backdoor, trap door*) – Fait le plus souvent référence à un morceau de code intégré dans des logiciels permettant l'accès dissimulé, la prise de contrôle d'un système, la copie d'information, etc. à l'insu de son propriétaire.

Prévention (*prevention*) – Ensemble de mesures prises pour prévenir un danger, un risque, qui tend à empêcher la réalisation de menaces, à réduire la fréquence des incidents dans une optique de protection.

Priorité (*priority*) – Fait de venir en premier, de passer avant les autres. Reflète le degré d'urgence avec lequel les solutions de sécurité doivent être mises en place, et l'ordre dans lequel doivent être appréhendés les risques selon leur degré d'importance, de gravité.

Privilège (*privilege*) – Droits d'accès, permissions, habilitations accordées à une entité pour effectuer certaines actions, attributs jouant un rôle déterminant pour la réalisation du contrôle d'accès aux ressources.

Privilège minimum (*least privilege*) – Les utilisateurs d'un système possèdent uniquement les priviléges strictement minimums à l'accomplissement de leur mission.

Profil utilisateur (*user profile*) – Liste des attributs concernant un utilisateur contribuant à effectuer la gestion du réseau et des systèmes auquel il se connecte (paramètres d'identification, d'authentification, droits d'accès, permissions et toutes autres informations utiles, à des fins de contrôle d'accès, de facturation, etc.).

Protection (*protection*) – Action, fait de protéger. Se dit d'une mesure de sécurité qui contribue à détecter, à neutraliser ou à diminuer les effets d'une agression.

Protection des données privées et de l'intimité numérique (*privacy protection*) – Mesures de protection qui permettent d'assurer que les informations, les activités des internautes, ne soient pas révélées à d'autres parties que celles voulues et ne soient pas utilisées à des fins contraires à celles consenties par leur propriétaire. Cela fait référence au droit des individus de contrôler les informations les concernant qui peuvent être collectées soit directement, soit indirectement par l'observation de leur comportement de navigation et des sites visités.

Rançongiciel (*ransomware*) - Logiciel malveillant prenant le contrôle des ressources d'un internaute afin de les lui rendre indisponibles pour exercer un chantage et exiger le paiement d'une rançon.

Rejeu (*replay*) – Type d'attaque basée sur la réutilisation de paramètres, de situation, etc. afin deurrer une entité.

Répudiation (*repudiation*) – Fait de nier d'avoir participé à des échanges, totalement ou en partie.

Réseau à sécurité robuste (*robust security network*) – Concept introduit par la norme 802.11i pour renforcer la sécurité dans les réseaux locaux sans fil 802.11. Un réseau à sécurité robuste est un réseau dans lequel toutes les stations communiquent d'une manière sécurisée à travers les associations de sécurité RSNA établies entre elles.

Réseau privé virtuel (RPV ou VPN, *Virtual Private Network*) – La notion de réseau privé virtuel fait référence à l'usage du protocole IPSec afin de créer un canal de communication sécurisé à usage privé, au travers d'un réseau public non sécurisé. Souvent mis en œuvre par une organisation, pour connecter ses différents sites *via* Internet afin d'assurer la confidentialité des données échangées.

Révocation (*revocation*) – Annonce qu'une clé privée a perdu son intégrité. Le certificat de la clé publique correspondante ne doit plus être utilisé.

Risque (*risk*) – Danger plus ou moins probable émanant d'une menace et pouvant se traduire en termes de probabilité d'apparition et de niveau d'impact.

Rootkit (outil de dissimulation d'activité) – Mot formé de la concaténation de *Root* (privileges de l'administrateur système sous Unix) et de *kit* (logiciel implantant un outil). Logiciel dont l'objet est de masquer l'exécution de codes malveillants afin de les rendre indétectables et de contourner les mesures de sécurité pour réaliser des cyberattaques.

RSA (*Rivest-Shamir-Adelman*) – Algorithme de chiffrement à clé publique, du nom de ses inventeurs Ronald Rivest, Adi Shamir et Leonard Adelman.

RSSI (responsable de la sécurité du système d'information) – Personne chargée de la sécurité se rapportant aux systèmes d'information.

Sabotage – Action malveillante, vandalisme, détérioration intentionnée tendant à empêcher le fonctionnement normal d'une organisation, d'une infrastructure, d'un service, d'une ressource et pouvant conduire à un sinistre.

Sécurité (*security*) – Situation dans laquelle quelqu'un, quelque chose n'est exposé à aucun danger. Mécanisme destiné à prévenir un événement dommageable, ou à en limiter les effets. Ainsi par exemple, la **sécurité physique** (*physical security*) est relative aux mesures permettant d'offrir une protection physique, matérielle des environnements, tandis que la **sécurité logique** (*logical security*) fait référence aux procédures et moyens logiciels de protection.

Sécurité de l'information (*information security*) – Ensemble de mesures techniques et non techniques visant à assurer la disponibilité, l'intégrité ou la confidentialité des données.

Sensibilité (*sensitivity*) – Caractéristique d'une entité qui indique sa valeur ou son importance.

Séquestration de clé (*key escrow recovery*) – Enregistrement et stockage des clés de chiffrement par une tierce partie de confiance qui peut être amenée à les révéler, sous certaines conditions, aux instances de justice et de police.

Serveur proxy (*proxy server*) – Serveur mandataire, intermédiaire qui réalise un service pour le compte d'une autre entité.

Sévérité perçue (*perceived severity*) – Niveau de gravité d'un problème tel que perçu par la personne le signalant.

S-HTTP – Version sécurisée du protocole HTTP permettant la sécurité des échanges entre un client et un serveur web.

Cybersécurité, sécurité informatique et réseaux

SIEM (*Security Information and Events Management*) – Composé du SEM (*Security Event Management*) et du SIM (*Security Information Management*), le SIEM collecte les événements de non-conformité, de vulnérabilités et d'attaques, recueillis par divers capteurs, et génère des rapports qui permettent de contrôler un système d'information.

Signature numérique (*digital signature*) – Par analogie à la signature manuelle, la signature numérique obtenue par un algorithme de chiffrement asymétrique permet d'authentifier l'émetteur d'un message et d'en vérifier l'intégrité.

SKEME et SKIP – Protocoles d'authentification mutuelle avec échange de clé, développé pour la version sécurisée du protocole IP.

Sniffer – Logiciel destiné à réaliser des écoutes passives des données transitant dans un réseau.

Sniffing – Action consistant à réaliser des écoutes passives afin de récupérer des paramètres de connexion qui seront par la suite utilisées à l'insu de leurs propriétaires légitimes afin de commettre des intrusions non autorisées.

SOC (*Security Operations Center*) – Centre de supervision, de contrôle et de gestion opérationnelle des activités de sécurité informatique.

Spam (pourriel) – messages électroniques à des fins publicitaires et/ou de diffusion de codes malveillants.

Spammer – Personne qui réalise le *spamming*.

Spamming – Technique qui consiste à envoyer des messages électroniques non sollicités.

Spoofeur – Personne qui pratique le *spoofing*.

Spoofing – Usurpation d'adresses IP à des fins d'intrusion.

SSL (*Secure Sockets Layer*) – Logiciel assurant la sécurité des échanges sur Internet, développé par Netscape et supporté par la majorité des navigateurs web du marché.

Stéganographie (*Steganography*) – Technique permettant de dissimuler une information dans une autre afin de la transmettre ou de la stocker clandestinement. Le marquage de document, le tatouage (*watermarking*), est une application de la stéganographie qui consiste à marquer une image de façon indélébile.

Système de détection d'intrusion (IDS, *Intrusion Detection System*) – Système permettant de détecter des incidents qui pourraient conduire à des violations de la politique de sécurité et permettant de diagnostiquer des intrusions potentielles.

Taux de faux négatifs (FAR, *False Acceptance Rate*) – Pourcentage d'actions, d'événements considérés comme étant corrects (et qui ne le sont pas) et acceptés par un système alors qu'ils auraient dû être rejetés.

Taux de faux positifs (FRR, *False Rejection Rate*) – Pourcentage d'actions, d'événements considérés comme étant incorrects (et qui ne le sont pas) et rejetés par un système alors qu'ils auraient dû être acceptés.

Test de pénétration/d'intrusion (*penetration test*) – Tests pratiqués pour analyser et tester le degré de protection des systèmes et la robustesse des mécanismes de sécurité.

TKIP (*Temporal Key Integrity Protocol*) – Algorithme de chiffrement utilisé dans le réseau local sans fil 802.11i. Cependant, cet algorithme est seulement une solution temporaire pour la transition vers le support de l'algorithme CCMP car une simple mise à jour logicielle est nécessaire pour que les équipements WEP puissent supporter TKIP.

Tolérance aux pannes (*failures tolerance*) – Capacité que possède un système à continuer de fonctionner en cas d'erreur ou de pannes. Aptitude d'un système informatique à demeurer fonctionnel malgré certaines pannes de ses composants.

Trace d'audit (*audit trail*) – Enregistrement des événements à des fins d'audit.

Triplet (*triplet*) – L'ensemble de trois valeurs (un numéro aléatoire, un numéro de réponse, la clé de chiffrement) qui est utilisé dans le processus d'authentification du réseau GSM.

Usurpation d'adresse (*address spoofing*) – Utilisation d'une adresse IP ou de messagerie électronique appartenant à un tiers, pour se faire passer pour lui, leurrer les systèmes et les personnes et éviter d'être identifié.

Usurpation d'identité (*identity theft*) – Emprunt de l'identité de personnes réelles pour obtenir frauduleusement des prestations en leur nom et place ou pour réaliser des actions délictueuses et leur faire porter la responsabilité de celles-ci.

Valeur de vérification d'intégrité (*ICV, Integrity Check Value*) – Valeur calculée par l'expéditeur sur l'ensemble des données à protéger et envoyée avec celles-ci. En utilisant le même algorithme, le destinataire recalcule l'ICV sur les données reçues et la compare à l'ICV originale. Si les deux valeurs sont identiques, il en déduit que les données n'ont pas été modifiées.

Valeur jetable (*nonce*) – Valeur unique. Nombre généré de façon aléatoire pour un message particulier et inclus dans la réponse pour empêcher des attaques basées sur le rejet.

Variable environnementale (*environmental variable*) – Valeur locale, dépendant d'un contexte particulier à prendre en considération lors de la prise de décision de l'autorisation ou non d'actions.

Vecteur d'authentification (*authentication vector*) – Ensemble de cinq valeurs (un numéro aléatoire, un numéro de réponse, la clé de chiffrement, la clé d'intégrité, un numéro pour l'authentification de réseau) utilisé dans le processus d'authentification du réseau UMTS.

Virus (*virus*) – Programme malveillant introduit, à l'insu des utilisateurs, dans un système. Il possède la capacité de se dupliquer — soit à l'identique, soit en se modifiant (virus polymorphe) —, de porter atteinte aux environnements dans lequel il s'exécute, et de contaminer les autres utilisateurs avec lesquels il est en relation. Différents types de virus sont distingués en fonction de leur signature, de leur comportement, de leur type de reproduction, de l'infection, des dysfonctionnements induits, etc. Les **vers, chevaux de Troie, bombes logiques** sont des codes malveillants de la famille générique des virus.

Vulnérabilité (*vulnerability*) – Défaut de sécurité qui pourrait se traduire soit intentionnellement soit accidentellement par une violation de la politique de sécurité.

Web Bug (mouchard web) – Espiongiciel, code implanté dans un site web pour surveiller la consultation à l'insu de l'internaute.

WEP (*Wired Equivalent Privacy*) – Algorithme de chiffrement utilisé dans les réseaux locaux sans fil 802.11.

Zero-day (jour 0) – Qualifie les vulnérabilités qui n'ont pas encore fait l'objet de contre-mesure de sécurité ou de correctif et qui peuvent être exploitées pour réaliser des attaques informatiques.

Zombi (*zombie*) – Se dit d'un ordinateur infecté et piloté à distance par une entité malveillante et dont le contrôle échappe à son propriétaire.

INDEX

3-D Secure 292

A

accords de Bâle II 84

acheminement 196

adresse IP 196

AES 157

AFAI 138

AFNIC 202

algorithme

 AES 157

 Blowfish 157

 DES 157

 Diffie-Hellman 159

 ElGamal 159

 GEA 232

 IDEA 157

 RC2, RC4, RC5 157

 RSA 159

 SHA-1 160

 Triple DES 157

 WEP 240

analyse

 des risques 111

 du risque 70

antivirus 278

architecture de sécurité 16

ARP 197

ASN-1 199, 200

association de sécurité 191

attaque

 cheval de Troie 51

defacement attack 54

 en déni de service 53

 en déni de service distribué 45

 en force brute 50

keyloggers 56

 par dictionnaire 50

 portes dérobées 51

 sémantique 55

spyware 51

virus 57

AuC 229

audit 86, 132

auditabilité 5

authentification mutuelle 234

B

backdoors 51

Bâle II 84

best effort 186

Big Brother 97

Big Data 18

BIND 202

biométrie 212

 multimodale 213

bit quantique 161

bitcoins 36, 179

blanchiment d'argent 46

blockchain 179

Blowfish 157

bonnes pratiques 112

BOOTP 198

botnet 43

brute force attack 50

buffer overflow attack 54

business-to-business 290

business-to-consumer 290

BYOD 89, 302

C

cadre juridique 89

carte

 PCMCIA 52

 SIM 227

catastrophes naturelles 28

CC 143

CCO 85

CDO 85

CERT 125

- certificat
 numérique 172, 209
 X.509 173
 certification électronique 177
 CESTI 145
 charte informatique 15
 chefs de service 88
 cheval de Troie 51
 chiffrement
 algorithme 157
 asymétrique 157
 des données 153
 homomorphe 219
 par flot 237
 symétrique 156
 CIL 85
 CIO 84
 CISO 85
 classification des ressources 126
 clé
 d'intégrité 235
 de chiffrement 154
 de session 171
 privée 158
 publique 158
 quantique 163
 secrète 170
cloud computing 96, 217
 CobiT 138
 code de pratiques 114
 COFRAC 145
 commerce électronique 290
 commutation 204
 confiance 93
 confidentialité 1, 3, 230
 conformité juridique 92
 contrôle d'accès 206
 Convention sur la cybercriminalité du Conseil
 de l'Europe 42
 coopération internationale 91
 coût de la sécurité 80
 crime informatique 41
 Critères Communs 142
 CRL 210
 cryptanalyse 154, 159
 cryptogramme 153
 cryptographie 153, 154, 155
 à courbe elliptique 159
 quantique 161
 cryptomonnaies 47
 CSO 85
 CTO 84
 culture de la sécurité 55
 CVV 293
 cyberadministration 290
 cybercrime 41
 cybercriminalité 32
 cyberdéfense 99
 cyberdérives 19
 cyberdissidents 41
 cyberhacktivisme 40, 41
 cybermenace 11
 cybernétique 11
 cyberrésilience 98
 cyberrisque 34, 71
 cybersécurité 11
 cyberslacking 92
 cybersurveillance 92
 cyberterrorisme 38
- D**
- Dark web 45
 Darknet 29, 45
 Data Leak Prevention (DLP) 95
 DDoS 45, 53
 defacement attack 54
 défense en profondeur 145
 degré
 de criticité 127
 de sensibilité 127
 délai
 de fraîcheur 131
 de reprise 132
 démarche proactive et réactive 71
 dématérialisation 30
 DES 157
 DESX 157
 détection d'intrusion 267
 DHCP 198
 Diffie-Hellman 159
 dimension managériale 67
 disponibilité 1
 distillation 163
 DMZ (*DeMilitarized Zone*) 265
 DNS 202
 DNSSEC 206

Cybersécurité, sécurité informatique et réseaux

documents XML 296

DoS 53

DRM 300

droit

de révocation 295

fondamentaux 93

humains 97

DSA 169

DTLS 289

E

e-administration 290

EAP 243

e-banking 292

EBPP 292

e-commerce 290

écosystème cybercriminel 43

écosystème numérique 98, 99

EDI 292

e-mail 277

empreinte digitale 167

ENISA 219

en-tête

d'authentification (AH) 190

de confidentialité-authentification 190

erreurs 27

ethical hacking 53, 312

éthique

sécuritaire 15

ETSI 227

eXtended Markup Language 296

externalisation 312

externaliser 96

F

FAI 209

faux

négatif 270

positif 270

fingerprinting 300

firewalls 257

fonction digest 167

fournisseur d'accès Internet 209

G

GDES 157

gestion

des droits numériques 300

Google Wallet 294

gouvernance de la sécurité 68

GPRS 226

GSM 226

guerre

informatique 37

sémantique 40

H

hacker 52

hacking 52

handover 226

handshake 288

HLR 226

honey pot 266

HTTP 296

I

ICANN 202

ICMP 198

IDEA 157

IDS 267

IETF 188

IGC 171

IKE 193

impacts 130

imputabilité 4

IMSI 227

infoguerre 55

Information Security Forum 125

infrastructure

critique 37

de gestion de clés 171

ingénierie de la sécurité informatique 84

ingénierie sociale 47

intégrité 1, 3

intelligence

économique 95, 304

juridique 15, 94

sociale 304

Internet des objets 18

Internet Security Alliance 125

interopérabilité 311

intimité numérique 75

Intranet 255

intrusion 267

éthique 53

IPNG 187

- IPS 267
- IPSec 189
- IPv6 188
- ISACA 138
- ISAKMP 193
- ISDN 227
- ISO 13335 125
- ISO 15408 125
- ISO 27000 114
- ISO 27010 124
- ISO 27032 124
- ISO 27033 124
- ISO 27034 124
- ISO 27037 124
- ISO 38500 139
- ISO 9834 200
- ISO/IEC 27000/2016 115
- ITSEC 142
- K**
- Kerberos 169
- keyloggers* 56
- L**
- LDAP 203
- libertés civiles 97
- liste de certificats révoqués 210
- log 5, 24
- LTE 226
- lutte informatique
 - défensive 99
 - offensive 99
- M**
- MAC 190
- maintenance 8, 321
- malveillance
 - informatique 49
- marchés noirs 45
- MDM 303
- menace 11
 - origine 27
- messagerie électronique 277
- mesures
 - de dissuasion 128
 - de protection 128
 - de récupération 128
 - de sécurité 127
 - palliatives ou correctives 128
- préventives 128
- structurelles 128
- méthode
 - CobiT 138
 - OCTAVE 125
- métier
 - CCO 85
 - CDO 85
 - chef de service 88
 - CIL 85
 - CIO 84
 - CISO 85
 - CSO 85
 - CTO 84
 - de la sécurité informatique 84
 - responsable
 - des ressources humaines 88
 - sécurité 87
- métriques de sécurité 139
- MIKEY 286
- MIME 282
- mission de sécurité 76, 86
- MIT 169
- modèle
 - de Bell-LaPadula 126
 - de Brewer-Nash 126
 - de Clark et Wilson 126
 - de maturité 141
 - PDCA 116
- m-paiement 294
- MSC 226
- MSISDN 227
- MSSC 226
- N**
- NAT 262
- NCSA 125
- noms de domaine 200
- non-répudiation 4, 170
- norme 802.11 240
- O**
- Oakley Key Determination Protocol* 193
- OCDE 92
- ODR 296
- On-line Dispute Resolution* 296
- opt-in* 280
- opt-out* 280

organe de révision 86

Orwell 97

outsourcing 96

P

paiements en ligne 290, 292

paires de photons intriqués 164

paradis digitaux 30

pare-feu 257, 258

 applicatif 262

stateful packet 261

stateless packet 260

stateful packet 261

patrimoine numérique 95

PayPal 294

PCMCIA 52

PDCA (*Plan, Do, Check, Act*) 116

PEM 281

périmètre de sécurité 265

PGP 281, 282

phishing 50

PKI 171

plan

 d'action 136

 d'action sécurité 72

 de continuité 129

 de continuité d'activité 129

 de reprise d'activité 129

 de secours 133, 134

politique

 de routage 204

 de sécurité 109

porte dérobée 51, 282

principes de précaution 95

projet d'entreprise 71

protection

 de la sphère privée 92

 persistante 301

protocole

 BB84 164

 DTLS 289

 EAP 243

 HTTP 296

 IPSec 189

 IPv6 188

 LDAP 203

 MIME 282

 PEM 281

PGP 281

RTP 286

S/MIME 281, 282

S-HTTP 289

SMTP 281, 282

SNMP 325

SRTP 286

SSH 289

TCP 186

TFTP 51

TKIP 246

TLS 289

proxy 262

Q

QKD 165

qualité de service 316

qubit 161

R

RARP 197

RC2 157

RC4 157

RC5 157

RDES 157

référentiel de sécurité 16

rejeu 190

réseau

 ad hoc 240

 cellulaire 226

 GPRS 226, 231

 GSM 226, 227

 social 303

 UMTS 226, 234

 WPAN 248

 résilience 12, 98

 responsabilité 15

 responsable

 des ressources humaines 88

 sécurité 87

 rétro-ingénierie 154

 risque 13, 70

 analyse des ~ 111, 70

 appréciation du ~ 70

 d'exploitation 8

 écologique 98

 évaluation du ~ 70

 gestion du ~ 70

- pour client 291
- pour l'entreprise 291
- résiduel 74
- systémique 37
- traitement du ~ 70
- roaming* 230
- robustesse 155
- ronde 160
- routage 204
- routeur filtrant 264
- RRH 88
- RSA 159
- RSNA 242
- RTP 286

- S**
- S/MIME 281
- SCADA 12
- scellement 154
- sécurité
 - applicative 8
 - de l'exploitation 7
 - des télécommunications 9
 - logique 8
 - physique et environnementale 6
 - stratégie de ~ 71
- sécurité informatique
 - ingénierie 84
 - métiers 84
- serveur
 - de noms 199, 211
 - DHCP 198
 - DNS 202
- SET 292
- S-HTTP 289
- SIEM 319
- signature
 - d'intrusion 269
 - détachée 297
 - digitale 173
 - DSA 169
 - enveloppée 297
 - numérique 167
 - XML 297
- SIM 227
- Smart Card 52
- SMSI 116
- SMTP 281, 282
- sniffer 50
- SNMP 325, 327
- SOC 318
- social engineering* 47, 49
- soft law* 296
- SOX 93
- spam 278
- SPIM 285
- SPIT 285
- spyware 51
- SRTP 286
- SSH 289
- SSL 287
- SSLv3 289
- stéganographie 300
- stratégie
 - criminelle 32
 - de sécurité 71
- structure organisationnelle 78
- sûreté publique 37
- surveillance 97, 320
- système de détection d'intrusion 267

- T**
- table de routage 204
- tatouage 299
 - numérique 299
- TCP 186
- TCSEC 142
- téléphonie Internet 284
- tests de conformité 144
- TFTP 51
- TKIP 242, 246
- TLS 287, 289
- TMSI 228
- ToIP 284
- traçabilité 5
- traitement des données à caractère personnel 92
- Triple DES 157

- U**
- UMTS 226
- URI 297
- utilisateur 89
- UYOCS 303

Cybersécurité, sécurité informatique et réseaux

	V	
variable continue	164	WiMax 248
virus	57	WPAN 248
VLR	226	
VoIP	284	X.509 173
VPN	194	XML 296
vulnérabilité	28	Encryption 297
		Signature 297
	W	xml-encryption 299
watermarking	299	
WEP	240	
Wi-Fi	225	
		Z
		zone démilitarisée 265

74734 (I) OSB 80° EPR-API
Dépôt légal: Octobre 2016
Jouve
1, rue du Docteur Sauvé, 53100 Mayenne
Imprimé en France