

CYBERSÉCURITÉ

Patrick Lallement

Définitions
Concepts
Métiers

ellipses

CYBERSÉCURITÉ

Définitions ■ Concepts ■ Métiers

Patrick Lallement



Conception graphique couverture: Nathalie FOULLOY

ISBN 9782340-087309

© Ellipses Édition Marketing S.A., 2024

8/10 rue la Quintinie 75015 Paris



Le Code de la propriété intellectuelle n'autorisant, aux termes de l'article L. 122-5.2° et 3°a), d'une part, que les « copies ou reproductions strictement réservées à l'usage privé du copiste et non destinées à une utilisation collective », et d'autre part, que les analyses et les courtes citations dans un but d'exemple et d'illustration, « toute représentation ou reproduction intégrale ou partielle faite sans le consentement de l'auteur ou de ses ayants droit ou ayants cause est illicite » (art. L. 122-4).

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

www.editions-ellipses.fr

Avant-propos



Ce livre est une introduction générale à la cybersécurité et plus particulièrement à sa gouvernance. Il s'adresse à un public assez large, étudiants en informatique concernés par le sujet, parfois intégré à leur cursus, mais comme l'ouvrage ne se veut pas (trop) technique, il peut intéresser des étudiants dans des disciplines connexes : gestion, intelligence économique, risque assurantiel, risque industriel. Il s'adresse aussi à des apprenants en formation continue et plus encore à un public professionnel qui pourra y trouver des éléments de langage et de compréhension d'une problématique en évolution constante et qui concerne tout le monde, car tout le monde aujourd'hui utilise des technologies numériques.

Le point de vue de cet ouvrage est le suivant : on ne peut pas parler de cyber-risque, de menaces, de vulnérabilités, d'impacts, etc. sans d'abord rappeler à quoi cela s'adresse : les systèmes d'information, les données, les processus métier des entreprises. Il est donc nécessaire de rappeler (pour les informaticiens), présenter (pour les autres), au moins dans les grandes lignes, les aspects fonctionnels des systèmes d'information : les outils, les flux, les processus, ainsi que quelques éléments techniques : services réseau, éléments d'architecture, technologies de l'internet et du web, pour au moins souligner les tendances, les convergences et les mécanismes d'intégration technologiques à l'œuvre depuis des décennies. Cette mise en relation globalisée, grâce à des technologies conçues dans un but fonctionnel d'efficacité est aujourd'hui rattrapée par les nécessités et les besoins de la sécurité, longtemps ignorés, voire écartés. Car le risque est aujourd'hui trop évident. Les données sont partout, les technologies numériques structurent toutes les activités de l'entreprise. Le moindre dysfonctionnement causé par une action malveillante peut causer des dommages à tous les niveaux : technique, juridique, organisationnel, humain, commercial, communication, réputation. Pourtant l'antagonisme demeure. Pour les développeurs, les concepteurs, le fonctionnel prime toujours, au détriment de la sécurité. Le fonctionnel va dans le sens de la productivité, la sécurité est vue comme un frein. Cela met souvent les responsables de la sécurité des systèmes d'information (RSSI) mal à l'aise, tant qu'une attaque n'a pas été subie pour rappeler que la sécurité est là, d'abord à titre préventif, pour éviter à l'entreprise de perdre temps et argent, quand ça n'est pas pour éviter qu'elle ne dépose le bilan (PME notamment).

L'ouvrage est structuré en trois parties.

La première partie s'intitule "Qu'est-ce que le cyber-espace?". La plupart des éléments un peu techniques se trouvent dans cette partie. Les informaticiens peuvent

donc en faire l'économie. On y rappelle surtout l'évolution des technologies dans le sens d'une convergence (réseaux notamment) vers le tout numérique, une multiplicité des formats de données et des sources, notamment avec les objets connectés. Avec déjà quelques constats relatifs à la sécurité.

La seconde partie s'intitule "L'espace des risques". À partir de la notion de risque, on y définit les concepts : menace, motivation, cyber-attaque, vulnérabilité, faille, dommage, cyber-sécurité, cyber-défense, cybercriminalité, etc. Ces termes sont aujourd'hui du langage courant et sont souvent mal employés (par ex. on confond allègrement risque et probabilité!). Tous ces termes peuvent ensuite être reliés entre eux. Cette partie traite enfin d'un sujet peu enseigné : la réponse à incident. La troisième partie s'intitule "L'espace de confiance". Elle présente les différents acteurs et métiers qui structurent (en France) l'écosystème cyber et qui tous ont un rôle dans la lutte contre la malveillance, que ce soit pour assurer la défense des systèmes, ou bien pour lutter contre la cyber-criminalité : agences, associations, enquêteurs, juristes, consultants, constructeurs, développeurs, experts, formateurs, etc. Tous ces acteurs sont censés intervenir à différents niveaux et différentes étapes des procédures et des processus de gestion de la cyber-sécurité. Cela va du conseil en mode préventif à l'enquête et à la gestion des incidents.

Table des matières



1	Qu'est-ce que le cyber-espace ?	9
1.1	Les convergences	9
1.1.1	Évolution des architectures	9
1.1.2	Vers le tout numérique	10
1.1.3	Le multimédia	10
1.2	Les technologies de l'internet	10
1.2.1	Le réseau	10
1.2.2	L'adressage	12
1.2.3	Le protocole de transport	14
1.2.4	IP et la sécurité	15
1.2.5	Le pare-feu	15
1.3	Services de l'internet	17
1.3.1	Le web	17
1.3.2	Système DNS	18
1.3.3	Le web caché (<i>dark web</i>)	19
1.3.4	DNS et la sécurité	20
1.4	Le système d'information (SI)	21
1.4.1	Les fonctions du SI	21
1.4.2	Les processus	22
1.4.3	Du web 1.0 au web 2.0	24
1.4.4	Dimension importante du SI : l'être humain	25
1.4.5	Où on (re)parle d'intelligence artificielle	26
1.4.6	Éléments d'infrastructure	26
1.4.7	Configuration de base d'un poste de travail	29
1.4.8	Virtualisation	29
1.4.9	Le cloud computing	31
1.4.10	Aspects sécurité	33
1.5	Les systèmes cyber-physiques	33
1.5.1	Couplage physique/ logique	33
1.5.2	Les systèmes cyber-physiques	34
1.5.3	Les objets connectés	36
1.6	Un univers de données	40
1.6.1	Donnée/ Information	40
1.6.2	Les fichiers	40
1.6.3	Les données personnelles	42

1.6.4	Les méta-données	43
1.6.5	Le big data	44
1.7	Vers le cyber-espace	44
1.7.1	Aspects géopolitiques	44
1.7.2	Notion de puissance	45
1.8	Conclusion	45
1.9	Exercices	45
2	L'espace des risques	49
2.1	Qu'est-ce que le risque ?	49
2.1.1	Définition	49
2.1.2	Évaluation	49
2.1.3	Sûreté de fonctionnement	50
2.2	Qu'est-ce que le cyber-risque ?	51
2.2.1	Risque <i>vs</i> cyber-risque	51
2.2.2	Typologie du risque "cyber"	51
2.2.3	Risque sur les données	52
2.2.4	Critères DICP	52
2.2.5	Risque sur le système	54
2.2.6	Risque "sûreté" (<i>safety</i>)	54
2.2.7	Malveillance : de la menace aux dommages	54
2.2.8	Termes clés	56
2.3	Caractérisation du danger	56
2.3.1	La menace	56
2.3.2	Attaque	59
2.3.3	Vecteur d'attaque	59
2.3.4	Scénarios d'attaque	60
2.3.5	La matrice MITRE ATT&CK	60
2.3.6	Attaques de déni de service	64
2.3.7	Le malware	67
2.3.8	Cas particulier des rançongiciels (<i>ransomware</i>)	68
2.4	Caractérisation du système	71
2.4.1	Les actifs	71
2.4.2	Vulnérabilités	71
2.4.3	Faible <i>vs</i> vulnérabilité	72
2.4.4	Exploit	73
2.4.5	Analyse de vulnérabilités	73
2.4.6	Protection	74
2.4.7	Détection	74
2.4.8	Impact	75
2.4.9	Relations entre les concepts	77
2.5	La gestion des risques	80
2.5.1	Processus	80
2.5.2	P1-Identification	80
2.5.3	P2-Estimation	80
2.5.4	P3-Évaluation	81
2.5.5	P4-Traitement	82

2.5.6	Norme ISO 27005	82
2.5.7	Méthodes d'analyse de risques	83
2.6	Autres définitions	85
2.6.1	Cybersécurité	85
2.6.2	Sécurité des systèmes d'information	85
2.6.3	Lutte contre la cyber-criminalité	85
2.6.4	Cyber-défense	86
2.6.5	Cyber-guerre	86
2.7	La réponse à incident	87
2.7.1	Quelques définitions	87
2.7.2	Les incidents de sécurité	88
2.7.3	La procédure de traitement des incidents	89
2.7.4	Éléments de procédure	90
2.7.5	L'équipe de réponse à incident	93
2.7.6	Le processus de traitement	97
2.7.7	Le SIEM (<i>Security Information and Event Management</i>)	108
2.8	Les services de réponse à incident	110
2.8.1	Les CERT (ou CSIRT)	110
2.8.2	Les SOC	111
2.8.3	Différences entre CERT et SOC	111
2.9	Exercices	111
3	L'espace de confiance	121
3.1	Les lois	122
3.1.1	Évolution des lois	122
3.1.2	Loi informatique et libertés	124
3.1.3	Règlement général de la protection des données	124
3.1.4	Loi Godfrain	125
3.1.5	La cyber-criminalité dans le code pénal	125
3.1.6	Loi de confiance sur l'économie numérique - LCEN	126
3.1.7	Loi LOPSSI 2	127
3.1.8	Loi de programmation militaire - LPM	127
3.2	Les obligations légales	128
3.2.1	Conservation des données de connexion	128
3.2.2	Utilisation de la cryptographie	129
3.2.3	Cas du <i>cloud computing</i>	130
3.2.4	Les opérateurs d'importance vitale (OIV)	130
3.2.5	Les établissements financiers	131
3.2.6	La directive européenne NIS	132
3.2.7	Politique de sécurité du système d'information (PSSI)	133
3.2.8	Charte informatique au sein de l'entreprise	133
3.2.9	Les normes ISO	136
3.3	Les institutions	137
3.3.1	Agence nationale de la sécurité des systèmes d'information	137
3.3.2	Commission nationale de l'informatique et des libertés	137
3.3.3	Sous-direction de lutte contre la cybercriminalité	137
3.3.4	Brigade de lutte contre la cybercriminalité	138

3.3.5	La gendarmerie nationale	138
3.3.6	Direction générale de la sécurité intérieure	139
3.3.7	Traitement du renseignement et action contre les circuits financiers clandestins	139
3.3.8	Cyber-douanes	140
3.3.9	Les officiers de police judiciaire	140
3.3.10	La magistrature	141
3.4	Les associations	141
3.4.1	Le Clusif	141
3.4.2	Le CESIN	142
3.4.3	Le CeCyF	142
3.4.4	Signal Spam	142
3.4.5	CyberLex	142
3.4.6	Les pôles de compétitivité	142
3.5	Les métiers de la cybersécurité	143
3.5.1	La gestion de la sécurité et le pilotage des projets	143
3.5.2	Conception et maintien d'un SI sécurisé	144
3.5.3	Gestion des incidents et des crises	145
3.5.4	Le conseil	146
3.5.5	L'enseignement et la recherche	147
3.6	Exercices	148
Conclusion		153
Correction des exercices		155
3.7	Partie 1	155
3.8	Partie 2	158
3.9	Partie 3	163
Bibliographie		167

Chapitre 1



Qu'est-ce que le cyber-espace ?

1.1 Les convergences

1.1.1 Évolution des architectures

Jusqu'aux années 80, les systèmes informatiques sont restés fortement centralisés en terme de ressources de traitement et de stockage. Les ordinateurs dits centraux ou *mainframe* exécutaient l'ensemble des opérations, assuraient le stockage. La centralisation n'est pas en soi une idée obsolète (surtout si on veut établir du contrôle). Ce qui l'était, c'était la position dominante des constructeurs des systèmes informatiques, qui s'appelaient IBM, Digital Equipment, Bull, propres à établir eux-mêmes leurs propres standards de communication entre leurs machines. Pour éviter l'emprise des standards de ces constructeurs, des groupes de travail se sont constitués dans les années 70 pour définir des modèles d'architecture de communication indépendants de ces grands acteurs du marché. C'est le rôle général des groupes de travail que de définir des standards qui permettent l'interopérabilité des systèmes, issus de constructeurs différents. C'est le principe des systèmes ouverts. Les débits de transmission n'étaient pas très élevés, le support était majoritairement le cuivre et l'obsession était alors la fiabilité des communications, l'objectif était de détecter et de corriger les erreurs. Le modèle d'architecture de communication dit modèle OSI (*Open System Interconnection*, standard de l'ISO) est basé sur ce principe. Dans la même période, un autre modèle est à l'étude par des universitaires américains autour des protocoles TCP/IP, standards du futur internet, leur approche était d'abord de concevoir un modèle de communication résilient.

D'un point de vue sécurité, deux facteurs allaient dans le bon sens : un trafic limité en nombre de connexions et en durée, l'approche centralisée qui permettait de contrôler les accès.

À partir des années 80, la décentralisation des ressources va croissante, basée sur l'apparition des mini et micro-ordinateurs, dotés de plus d'autonomie. Ceci a eu un fort impact sur le poste de travail, avec l'apparition des PC (*Personal Computer*) et celle des réseaux locaux : Ethernet, Token Ring. La fibre optique fait son apparition avec par rapport au cuivre, des taux d'erreurs beaucoup plus faibles

et des débits beaucoup plus élevés. L'autonomie (traitement, stockage) a suivi le développement des microprocesseurs. Les nouveaux acteurs sont alors les constructeurs de ces microprocesseurs (Intel, Motorola, NEC, etc.) et l'éditeur de logiciels Microsoft (applications, systèmes d'exploitation). Les réseaux locaux permettent de structurer les échanges entre collaborateurs d'entreprise avec des outils dédiés comme la messagerie, le transfert de fichiers. Le concept de "système d'information" apparaît dans les années 90.

1.1.2 Vers le tout numérique

Dans les années 60, l'information était en grande partie analogique : textes, musique, images, téléphone, TV. Depuis les années 2000, tout est numérisable à des fins de transmission et de stockage. Ceci a pour conséquence que tout processus de communication, de bout en bout, revient à transporter de l'information numérique (des 0 et des 1). La deuxième conséquence est le développement de processeurs spécialisés pour numériser, coder, compresser les signaux analogiques (son et image) avant de les transmettre. De nombreux standards de codage et de compression existent dans ce domaine, surtout pour la voix depuis l'apparition des systèmes de communication mobile dans les années 90. Tout signal (son, image) est échantillonné de manière à remplir un buffer (mémoire tampon) de 0 et de 1 pendant un intervalle élémentaire. Chaque buffer constitue potentiellement un paquet à transmettre.

1.1.3 Le multimédia

Dans les années 90, la notion de données s'enrichit en se complexifiant. On parle de contenu multimédia pour désigner la nature hétérogène de l'information (à traiter, à transmettre, à stocker) : texte, son, image, vidéo. La messagerie voit l'extension MIME (*Multi-purpose Internet Mail Extension*) qui permet d'inclure dans un message des éléments de toute nature (voix, vidéo, photo).

Le web est inventé en 1990 et connaît un succès rapide, moteur du développement et de la démocratisation d'internet. Les sources d'information se multiplient, ce qui crée un nouveau problème : comment en retrouver 1 parmi N , ou comment retrouver une aiguille donnée dans une botte de foin qui ne cesse de grandir ? C'est le rôle des moteurs de recherche. De nouveaux acteurs apparaissent alors qui proposent des outils, Google est le plus connu.

1.2 Les technologies de l'internet

1.2.1 Le réseau

Le projet ARPANET (1964) avait pour but de concevoir une technologie résiliente de communication par paquets. Les principaux standards qui définissent les bases du modèle dit TCP/IP sont apparus dans les années 70 (IP, TCP, UDP,

DNS, etc.), un peu avant les concepts du modèle OSI (de l'ISO). Le standard TCP/IP s'est imposé comme réseau mondial à partir des années 90, *boosté* par l'apparition de l'application web. Le réseau n'est effectivement qu'un outil, au service des applications qui communiquent. Le web en est une, qui va dépasser toutes les autres. Le modèle TCP/IP est d'abord une technologie d'interconnexion (des réseaux existants) autour du protocole de transfert de paquets : IP (*Internet Protocol*) [1]. L'équipement clé de cette interconnexion est une passerelle appelée routeur (figure 1.1).

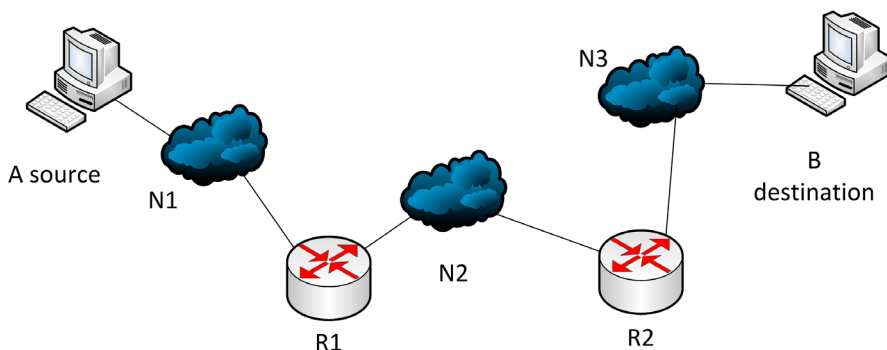


FIGURE 1.1 – Réseau internet

Internet est en fait un réseau de réseaux existants, interconnectés par des routeurs. Il peut même être simplement vu comme un réseau de routeurs (en faisant abstraction de la nature hétérogène des réseaux inter-connectés). Le routeur est d'abord une passerelle, pour passer d'un réseau à un autre, via une interface d'accès à une autre interface d'accès. Il est ensuite un aiguilleur de paquets. Les deux fonctions contribuent à l'acheminement des paquets de bout en bout, de la source jusqu'au destinataire final. Le réseau internet est l'aboutissement d'un projet né en pleine guerre froide dont la figure 1.2 rappelle les jalons.

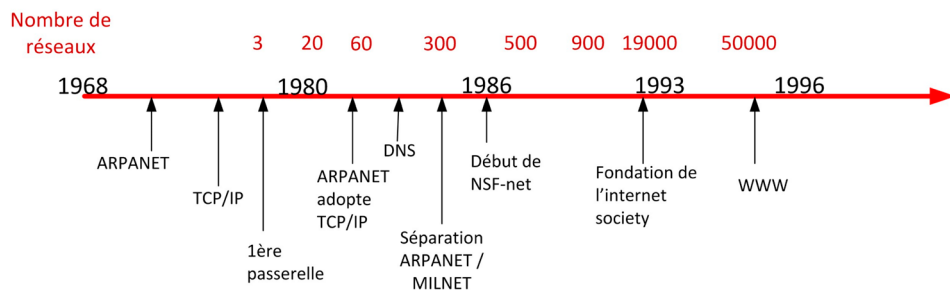


FIGURE 1.2 – Internet : les jalons

1.2.2 L'adressage

Principe

IP est le protocole d'interconnexion utilisé par l'internet pour l'acheminement des paquets. Ces paquets transitent donc de routeur en routeur avec l'adresse réseau (adresse IP) du destinataire.

Internet est aujourd'hui un réseau mondial, accessible à n'importe qui, ce qui lui confère un statut de réseau public. Par conséquent, joindre n'importe quel destinataire suppose que l'adresse de celui-ci soit publique (on doit pouvoir la trouver) et qu'elle soit unique.

Une adresse IP a un format unique structuré en deux parties : une partie publique (attribuée par les autorités de l'internet, ce qui garantit son unicité) et une partie privée (gérée par l'administration locale qui l'utilise), comme le montre la figure 1.3. Ce concept existait déjà avec les numéros de téléphone : par ex. dans une numérotation à 10 chiffres, les 6 premiers sont attribués à l'entreprise par l'opérateur (adresse de base visible dans un annuaire) et les 4 derniers sont laissés à la libre gestion et attribution par l'entreprise, ligne par ligne, pour la distribution finale, via son auto-commutateur privé.

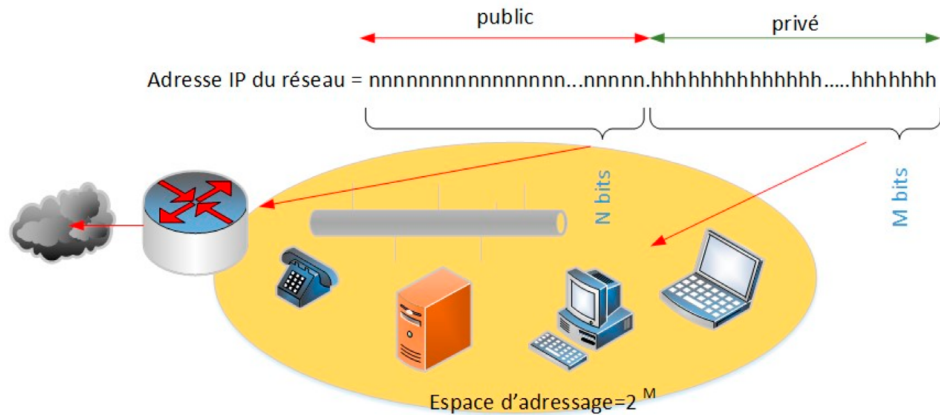


FIGURE 1.3 – Adressage IP

Format IPv4

L'adresse IP (notée ici @IP) est utilisée au format binaire par les machines et en décimal par les personnes (pour des raisons pratiques évidentes). Les chiffres (ou digits) sont séparés par des points.

Par exemple @IP=192.60.10.25 est une adresse IPv4 de 4 digits au format décimal, ce qui donne en binaire 1100000.00111100.00001010.00011001, c'est-à-dire 32 bits (4*8). La version décimale est plus facile à retenir.

Une adresse IP désigne en fait une interface d'accès à un réseau (et non pas un terminal!), ce qui veut dire que le routeur qui est une passerelle a au moins deux interfaces et a autant d'adresses que d'interfaces. Chaque adresse doit être conforme au plan d'adressage du réseau de rattachement.

À l'adresse IP on associe un masque de même longueur. À tous les bits contigus qui correspondent à la partie publique de l'adresse, correspond un 1 binaire dans le masque associé. Le masque permet par une simple opération (un ET logique) de retrouver l'adresse de base du réseau de rattachement. Par ex. si une entreprise se voit attribuer l'adresse @IP publique (en décimal) 195.60.10.0/24 cela veut dire que le masque associé a 24 bits à 1 consécutifs, soit (en décimal) : Masque = 255.255.255.0 = 11111111.11111111.11111111.00000000

Si on reprend l'adresse précédente @IP = 192.60.10.25 alors l'opération @IP ET Masque = 192.60.10.0, c'est-à-dire l'adresse de base du réseau d'appartenance de l'interface. Précision importante : une adresse de base de réseau ne peut pas être attribuée à une interface.

Tous les routeurs de transit dans l'internet ne connaissent (directement ou indirectement) que les adresses de base des réseaux. Seuls les routeurs de départ et d'arrivée connaissent l'adresse complète respectivement de la machine source et de la machine destinataire.

L'épuisement de l'espace d'adressage IPv4 est une des raisons qui ont conduit au développement d'une nouvelle version, IPv6, apparue dans les années 90 ([2]). Les principes restent les mêmes mais les deux protocoles sont incompatibles et les formats d'adressage différents. Aujourd'hui les routeurs doivent gérer les deux systèmes (IPv6 n'a pas remplacé IPv4) et les deux formats qui sont :

- IPv4 : adresses codées sur 32 bits soit 4 octets (espace d'adressage épuisé depuis 2014) ;
- IPv6 : adresses codées sur 128 bits soit 16 octets (espace d'adressage immense).

Les prévisions sur l'épuisement de l'adressage IPv4 se sont révélées exactes mais le scénario optimiste du remplacement de IPv4 par IPv6 ne s'est pas réalisé, même si la communauté mobile a fortement poussé à ce remplacement (les smartphones, apparus en masse dans les années 90, ont besoin d'une adresse IP).

Translation d'adresse (NAT)

Pour dépasser les limites de leur espace d'adressage avec l'adresse IPv4 dont elles disposaient déjà, les entreprises ont massivement utilisé un dispositif décrit dans le standard RFC 1918 [3]. Ce dispositif réserve des plages d'adresses utilisables dans la sphère privée, ce qui permet d'utiliser en privé un espace d'adressage beaucoup plus grand que l'espace publique qui a été attribué. Ces plages sont :

- 10.0.0.0/8 soit un espace d'adressage de $2^{32-8} = 2^{24}$;
- 172.16.0.0/12 soit un espace d'adressage de 2^{20} ;
- 192.168.0.0/16 soit un espace d'adressage de 2^{16} .

Tant que le trafic reste intra-entreprise (donc privé) cela fonctionne. Si la connexion doit sortir et donc passer dans le réseau public, cela n'est pas possible en l'état. Les adresses utilisées ne sont pas réservées exclusivement à des fins privées, elles ont aussi une existence publique quelque part (déjà attribuées dans le passé) et surtout elles ne sont pas uniques (elles peuvent être attribuées à plusieurs endroits en utilisant le standard RFC 1918). Pour réaliser la connectivité de bout en bout et passer de l'espace privé à l'espace public, il est alors nécessaire de translater l'adresse source privée en adresse source publique (l'adresse destination est forcément publique pour se connecter à un serveur externe publique).

Cette translation est réalisée au niveau du routeur par la fonction NAT (*Network Address Translation*), comme le résume la figure 1.4. Aujourd'hui presque tous les systèmes IPv4 utilisent le dispositif NAT pour adresser leurs machines dans l'espace privé, sans souci de croissance des besoins.

Ce dispositif prévu à des fins utilitaires a aussi un impact en terme de sécurité car vu de l'extérieur, l'adressage réel (privé) d'une machine est masqué. Il trouve sa place dans un schéma de connexion de type client (privé) vers serveur (public). Il pose problème par contre dans un schéma client privé vers client privé, ce qui est le cas de la téléphonie, car ne peut appeler de l'extérieur que des client dont on connaît l'adresse publique.

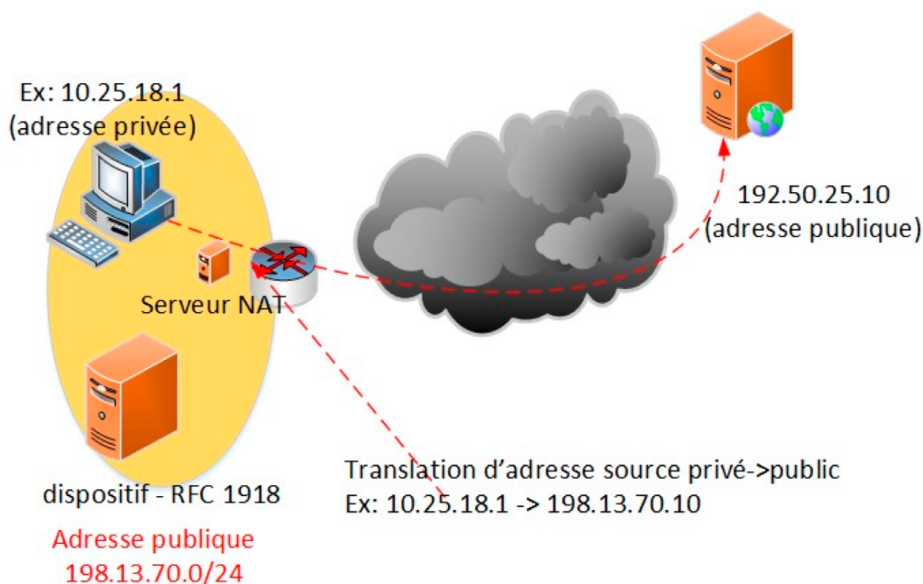


FIGURE 1.4 – Serveur NAT

1.2.3 Le protocole de transport

Le protocole IP ne contrôle ni la perte de paquet ni les erreurs. C'est le rôle du protocole de transport TCP (*Transport Control Protocol*) qui n'est exécuté qu'au

niveau des machines source et destinataire. Entre les deux, on ne voit plus qu'un tuyau virtuel. Comme plusieurs applications peuvent communiquer en même temps et utiliser le même interface IP, il est important de les distinguer par une adresse au niveau transport : le numéro de port. Il existe des ports statiques (référéncés pour toutes les applications connues) et aussi des ports dynamiques, non référéncés.

Il existe un protocole de transport non fiable (pas de contrôle des erreurs, ni de connexion préalable) qui est surtout utilisé pour des communications de 1 vers N ou des sessions multimédia : téléphonie, flux vidéo, vidéo conférence). C'est le rôle de UDP (*User Datagram Protocol*). Le système d'adressage est commun pour TCP et UDP.

1.2.4 IP et la sécurité

La technologie IP s'est massivement déployée au point de devenir le standard de transport de bout en bout, pour les données, la voix, l'image.

La convergence des technologies de communication vers un même standard protocolaire facilite les aspects fonctionnels, permet de réduire les coûts mais d'un point de vue sécurité, cela simplifie aussi la tâche de l'attaquant potentiel, surtout que les aspects sécurité ne figuraient pas dans le cahier des charges de ces standards de communication. Il faut attendre le protocole IPv6 dans les années 90 pour des mécanismes de sécurité soient prévus, en option : authentification, chiffrement. Mais IPv6 n'a pas remplacé IPv4. Il s'est ajouté. À mesure que les problèmes et les besoins sont apparus, il a fallu rajouter aux standards basés sur IPv4 des mécanismes plus ou moins complexes, selon le chemin à sécuriser, entre deux nœuds (au niveau IP) ou de bout en bout (au niveau des applications).

1.2.5 Le pare-feu

Définition

Le pare-feu (ou *firewall* FW) est un équipement placé en coupure entre deux réseaux, en premier lieu entre réseau public (internet) et réseau privé (voir figure 1.5).

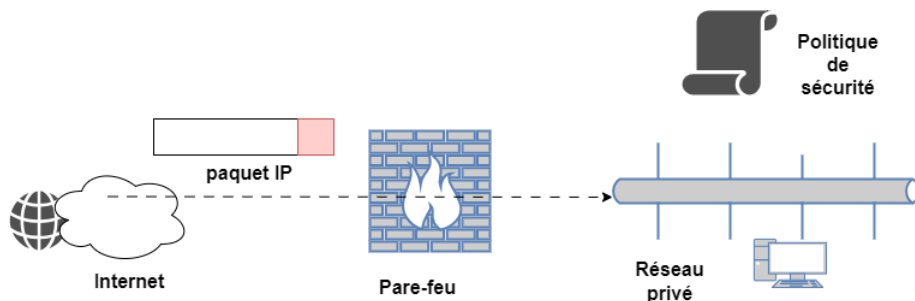


FIGURE 1.5 – Pare-feu (*firewall*)

Le FW implémente un mécanisme de filtrage basé sur des règles. Pour configurer un FW, il est nécessaire de définir au préalable une politique de sécurité.

Configuration

Pour filtrer un flux, deux stratégies sont possibles :

- tout ce qui n'est pas explicitement interdit est autorisé (liste noire) ;
- tout ce qui n'est pas explicitement autorisé est interdit (liste blanche).

Une règle de filtrage est une relation logique formalisée comme suit : SI <condition> ALORS <décision>. La décision est : laisser passer ou bloquer. Un filtre de paquets analyse chaque paquet IP et décide s'il est conforme ou non à la politique de sécurité du système où il veut entrer.

Les règles de filtrage sont couramment appelées des ACL (*Access Control List*).

Profondeur de filtrage

Pour décider de la conformité d'un flux, le FW utilise :

- des données de l'entête IP (niveau 3) ;
- des données de l'entête TCP (niveau 4).

Un pare-feu en coupure de l'internet inspecte tous les paquets entrants, ce qui constitue une charge de traitement importante. Pour cette raison les règles de filtrage utilisent des champs exploitables des entêtes IP et TCP.

- entête IP : adresses IP (source, destination) champ *Protocol* qui indique si le niveau 4 est TCP ou UDP ;
- entête TCP : numéros de port (source, destination).

On pourra se référer aux recommandations de l'Agence nationale de la SSI (ANSSI) [4] pour le paramétrage d'un pare-feu.

Pare-feu et DMZ

La fonction de FW est une fonction purement logicielle, comme le routage. Associées dans un même équipement, le filtrage/ routage permet de router les paquets acceptés vers un port physique associé à une zone démilitarisée ou DMZ. Une DMZ est une zone dite neutre mais qu'il faut sécuriser. C'est un segment de réseau séparé par un FW via un port spécifique dédié. La figure 1.6 en montre le principe qui suit une logique de segmentation des flux à des fins de sécurité. Il est conseillé d'utiliser ce mécanisme pour regrouper dans une même DMZ tous les serveurs publics (web, messagerie, DNS), car ils sont les plus exposés. Ainsi les paquets à destination de ces serveurs seront routés vers un port spécifique distinct des autres machines.

On peut aussi en suivant la même logique définir une DMZ pour regrouper les serveurs internes (bases de données, serveur intranet, serveurs métier etc.), qui ne doivent pas être vus par des personnes non autorisées.

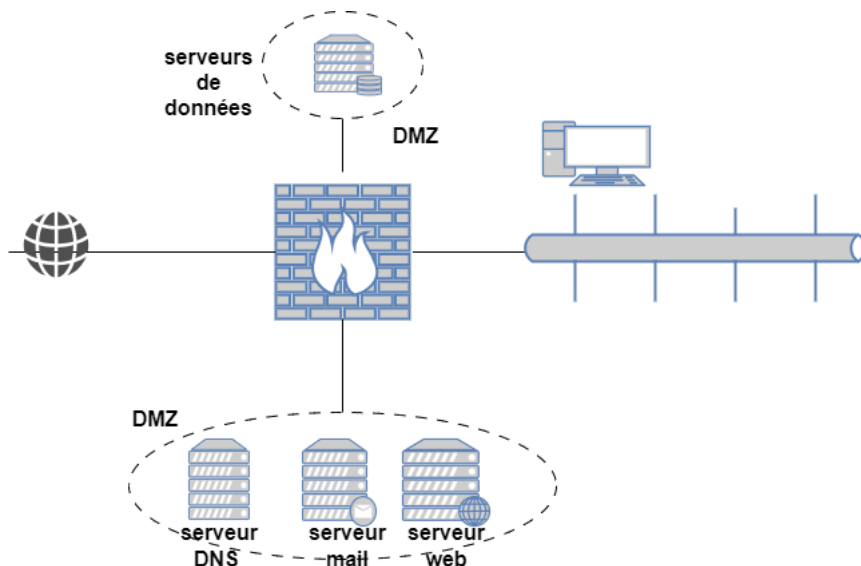


FIGURE 1.6 – DMZ : principe

1.3 Services de l'internet

1.3.1 Le web

Les années 90 sont marquées par l'apparition d'une nouvelle application : le web (Tim Berner-Lee, CERN, 1990). Jusqu'alors les applications communicantes s'appelaient jusqu'alors messagerie, transfert de fichier, émulation de terminal à distance. Dans le monde de l'internet on a parlé de "*killer*" *application*, car c'est l'application web qui a démocratisé l'internet jusque dans la sphère personnelle. Le service web utilise 3 concepts de base :

- le lien hyper-texte ou URL (*Uniform Resource Locator*) pour référencer tout document sur une machine distante (serveur) ;
- le langage HTML (*Hyper-text Media Language*) pour représenter les pages web ;
- le protocole de communication http (*Hyper-Text Transport Protocol*) pour assurer les échanges entre client et serveur.

L'URL est une chaîne de caractères structurée en 3 parties, qui correspondent à 3 éléments d'information (3 réponses à 3 questions) :

- le nom de la page ;
- sa localisation ;
- le protocole permettant d'y accéder.

Par exemple dans l'URL <http://www.w3.org/Protocols/rfc2616/rfc2616.txt>, on trouvera les éléments suivants :

- le nom de la page web (du fichier) : Protocols/rfc2616/rfc2616.txt ;
- la localisation (ce qui doit permettre de localiser le serveur) : www.w3.org ;
- le protocole (pour y accéder) : HTTP (*Hyper Text Transport Protocol*).

1.3.2 Système DNS

Le sigle DNS désigne en réalité trois aspects distincts :

- un schéma de nommage, basé sur une arborescence hiérarchique de noms de domaines (par ex. dans notre exemple d'URL : www.w3.org est un sous-domaine de w3.org qui lui-même est un sous-domaine de .org., lui-même sous-domaine de la racine de l'arbre) ;
- une base de données répartie, celle des serveurs DNS, qui participent à la résolution de nom (typiquement trouver l'@IP à partir de l'information de localisation) ;
- le protocole, qui permet d'échanger des messages DNS (interrogation, réponse) en mode client serveur.

La figure 1.7 donne une idée simple du principe de structuration hiérarchique DNS en domaines, sous-domaines, etc.

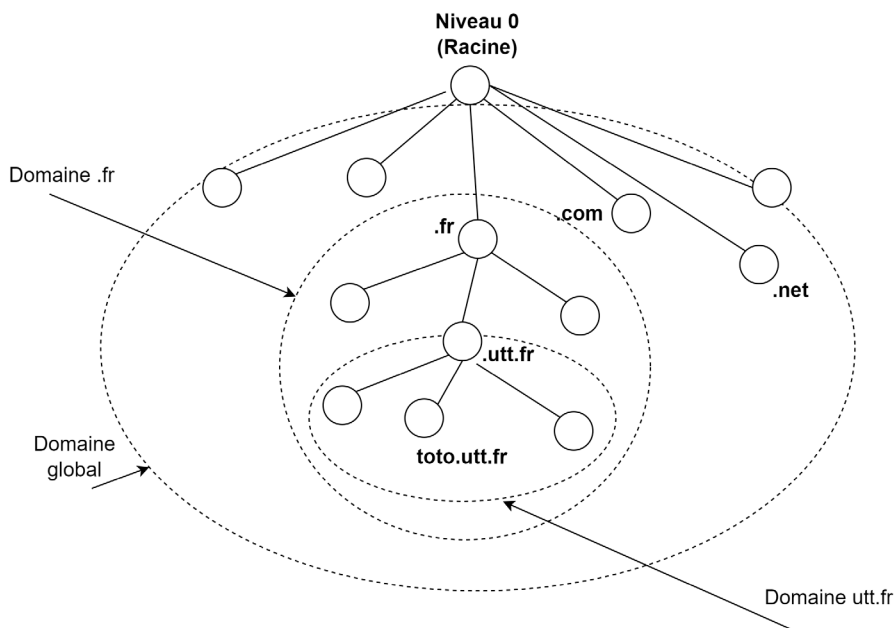


FIGURE 1.7 – DNS : arborescence des domaines

L'arbre fait apparaître une hiérarchie ascendante, des feuilles (les serveurs publics de données) vers la racine. Cela concerne :

- les domaines : par ex. utt.fr est un sous-domaine de .fr qui est lui-même un sous-domaine de la racine (non mentionnée explicitement) ;

- les serveurs : à chaque niveau se trouve (au moins) un serveur DNS, le serveur DNS du domaine Par ex. le serveur du domaine .fr connaît (parmi des millions d'autres) le serveur DNS du domaine utt.fr.

L'application qui veut accéder à un fichier distant à partir de son URL va implicitement interroger le système DNS (*Domain Name Server*), sorte de base de données répartie contenant toutes les références publiques de ressources d'information accessibles à distance. Dans l'exemple précédent, il s'agit de la partie `www.w3.org` de l'URL, appelée aussi FQDN (*Full Qualified Domain Name*), qui doit permettre de localiser le serveur, c'est-à-dire son adresse IP (v4 et/ou v6). Ainsi pour récupérer la page web distante donnée par l'URL de notre exemple, le protocole HTTP du poste client a besoin d'adresser des paquets vers une machine dont il ne connaît pas l'adresse IP. Le système DNS sera donc sollicité, selon la procédure donnée figure 1.8.

HTTP extrait la partie FQDN = `www.w3.org` pour interroger le système DNS afin d'obtenir l'adresse IP correspondante. Cette requête est par défaut adressée au serveur DNS local (flèche 1), celui du domaine de l'entreprise (il n'y en pas peut-être pas qu'un seul attention, mais il y en a toujours un à proximité, c'est un paramètre de configuration) qui ensuite va en mode récursif interroger un serveur au niveau $n+1$ (flèche 2) et ainsi de suite. La réponse suivra le chemin inverse (flèches 3 puis 4). À partir de là l'application HTTP peut générer des paquets IP avec l'adresse IP du serveur destinataire (flèche 5). Le tout s'exécute de façon transparente à l'utilisateur et ne prend que quelques ms.

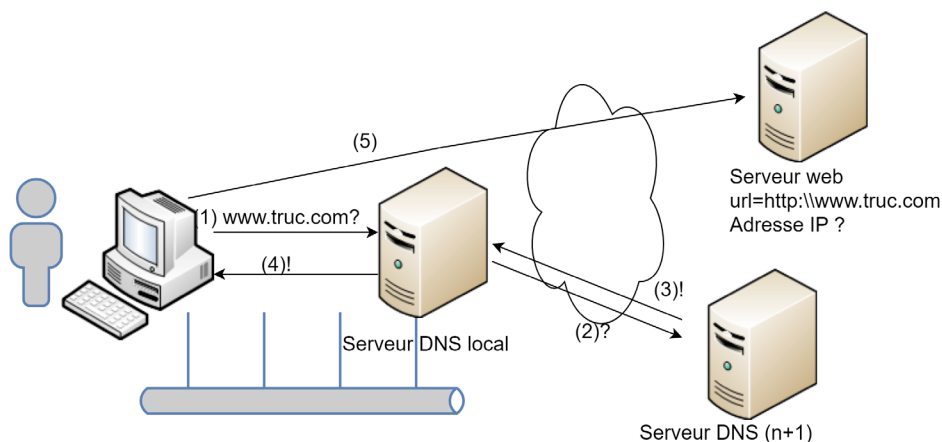


FIGURE 1.8 – Serveur DNS

1.3.3 Le web caché (*dark web*)

Le web profond (*deep web*) désigne les ressources non accessibles par les navigateurs connus parce que ces ressources ne sont pas publiées dans le système DNS. Par exemple les pages ne sont pas indexées par le moteur de recherche Google. Les flux de données utilisent l'infrastructure réseau publique mais les données ne sont

accessibles que via un navigateur spécial (navigateur Tor) qui permet d'utiliser internet de façon masquée (chaque routeur va masquer l'adresse IP effective par une autre avant reroutage). Utiliser le web profond n'a rien d'illégal, ce qui peut être illégal c'est ce qu'on y fait. Toutes les activités répréhensibles par la loi (code pénal) sont désignées par le terme d'internet sombre ou obscur (*dark web*) (trafics, blanchiment d'argent, importations illégales, activités terroristes, pédopornographie, etc.)

On présente souvent l'internet comme dans la figure 1.9 c'est-à-dire comme un iceberg dont la partie émergée représente la part des données publiques accessibles par le DNS, et la partie immergée représente l'internet caché voire illicite. Cette figure très connue illustre le caractère minoritaire de l'internet public.

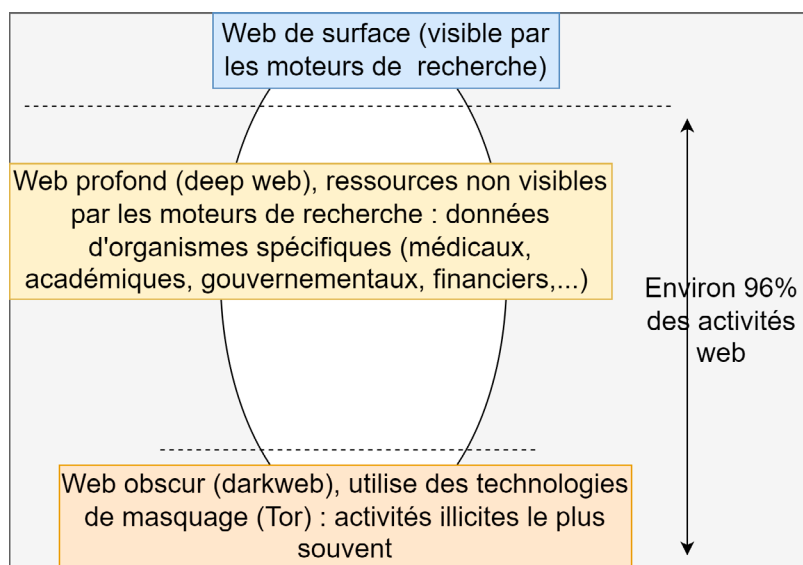


FIGURE 1.9 – Le web : public, profond, caché

1.3.4 DNS et la sécurité

Qu'est ce qu'un serveur public ? C'est un serveur visible de l'extérieur, et donc accessible via le système DNS. C'est-à-dire qu'il est enregistré par le serveur DNS de son domaine. C'est le cas d'un serveur de messagerie, du serveur DNS lui-même, d'un serveur web.

Attention : tous les serveurs web n'ont pas vocation à être publics (un serveur intranet ne l'est pas). Mais aujourd'hui les entreprises en ont au moins un, parfois plusieurs (selon leur taille et leur répartition géographique), parfois même elles ne savent plus combien elles en ont (même si le serveur est désactivé, l'adresse IP associée peut rester active) et c'est un problème.

Tout serveur public et donc visible de l'extérieur, constitue une porte d'entrée potentielle dans un système. Il convient donc de les connaître et de les protéger en particulier (dans une DMZ par ex.)

Le système DNS est souvent présenté comme un des talons d'Achille de l'internet. Cela concerne les serveurs (qui sont publics) et notamment les serveurs situés à un niveau hiérarchique élevé, de domaines importants (.fr est un exemple). On peut perturber tous les échanges de et vers un domaine géographique donné en portant atteinte à ces serveurs. Cela concerne aussi le protocole DNS et les données transportées dans les messages.

1.4 Le système d'information (SI)

1.4.1 Les fonctions du SI

Le système d'information peut se présenter en plusieurs niveaux (figure 1.10).

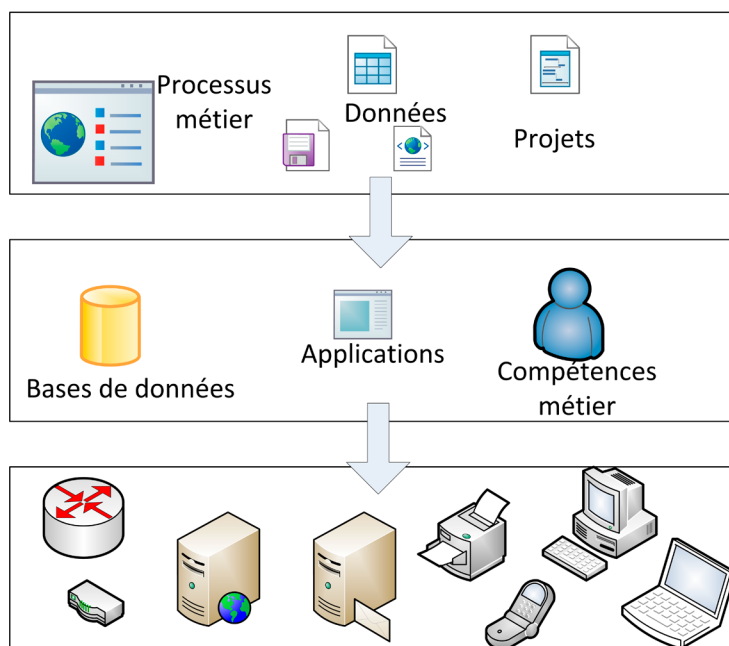


FIGURE 1.10 – Système d'information

Sa finalité est de consommer des données afin de réaliser les fonctions essentielles de l'entreprise (qu'on rangera sous le terme générique de processus : processus métier, processus support). Il s'appuie sur des ressources de stockage (data-centres, serveurs dédiés, bases de données), de traitement (applications), qui elles-mêmes utilisent des ressources matérielles : réseau, équipements réseau,

PC, serveurs. L'ensemble des ressources logicielles et matérielles du système d'information constitue ce qu'on appelle généralement le système informatique.

La finalité du SI est d'aider à la gestion des activités, soit plus précisément :

- la planification : spécifier, organiser ;
- l'exécution : mise en œuvre, pilotage ;
- le contrôle : mesure, diagnostic.

1.4.2 Les processus

Un processus est une série de tâches répétitives comportant des entrées (input) et des sorties (output) quantifiables et subissant des transformations à valeur ajoutée dans le but de produire un résultat matériel (par ex. des biens) et/ou immatériel (des informations) grâce à l'utilisation conjuguée d'hommes, de machines, de matériaux, de directives [5] Les tâches peuvent être regroupées en activités en fonction des métiers concernés. Les processus sont donc décomposables en activités, elles-mêmes découpées en tâches élémentaires, ces niveaux d'imbrication sont illustrés figure 1.11.

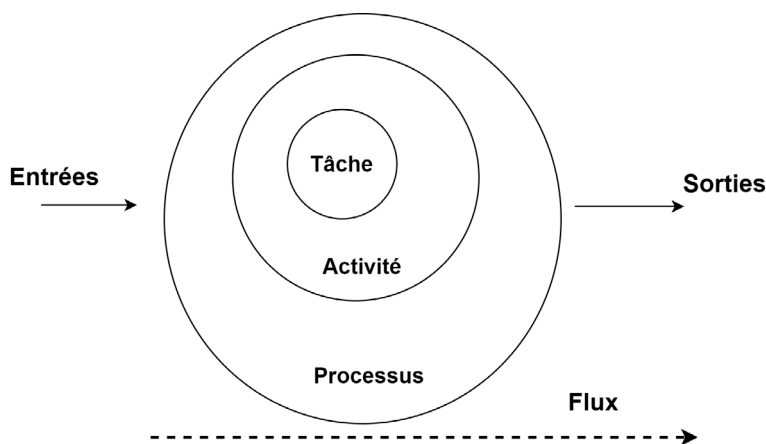


FIGURE 1.11 – Processus, activités, tâches

Processus, activités, tâches sont traversés par des flux : matière, énergie, information. Quelle est la différence entre processus et procédure ? Les procédures sont des modèles d'exécution. Les processus les réalisent, le facteur temps apparaît. Quel est alors l'intérêt de la modélisation ? Cela permet de décrire les procédures sous forme de tâches et d'activités. Cette modélisation permet de définir une relation entrée/sortie ou encore causes/effet et de définir des outils de pilotage des effets (sorties) à partir des causes (entrées, activités, tâches).

Ce qui nous intéresse ici est le rôle du système d'information et des outils utilisés.

- les outils du workflow, logiciel dédié à la gestion des procédures, il se base sur leur modèle et l'ordre d'exécution des tâches (voir l'illustration figure 1.12) ;

- les outils de travail collaboratif, entre plusieurs personnes pour réaliser une tâche ou une activité, réalisant la mise en commun de documents dans un espace partagé (voir figure 1.13) ;
- les progiciels de gestion intégrée (PGI en français, traduction éloignée de ERP *Enterprise Resource Planning*), qui permettent de gérer de façon synchrone toutes les ressources de l'entreprise (personnel, finances, stocks de matières premières, de produits finis, etc.) pour réaliser les processus métier de celle-ci (production, logistique, etc.) ou les processus support (RH, commercial, compta/finances). Le caractère intégré désigne le fait que chaque variable est représentée par une donnée unique dans le système (le caractère intégré). Voir figure 1.14.

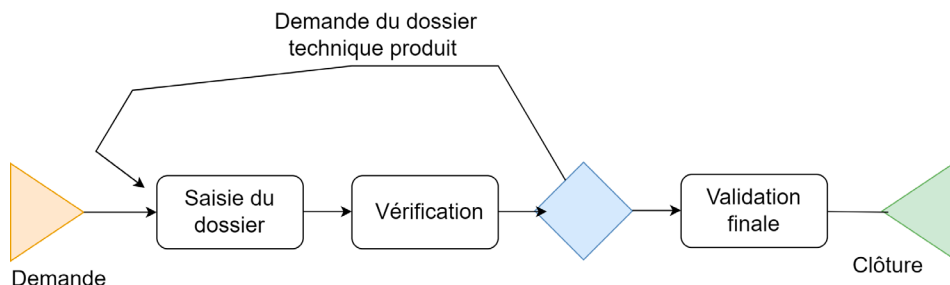


FIGURE 1.12 – Principes du workflow



FIGURE 1.13 – Espace de travail collaboratif

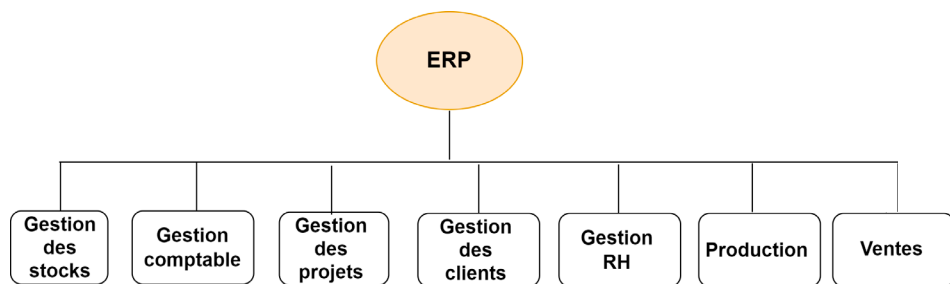


FIGURE 1.14 – Progiciels de gestion intégré (ERP)

1.4.3 Du web 1.0 au web 2.0

Dès l'apparition du web, on a assisté dans les années 90 à une multiplication des ressources d'information. Au niveau de l'entreprise et des administrations, des services en lignes sont apparus et à moindre coût :

- des pages d'information : administration, catalogues, annuaires ;
- des formulaires : inscription, commandes, déclarations ;
- des services commerciaux ou financiers : commandes, virements, consultations ;
- des services d'accès à distance des salariés mobiles.

Les informaticiens ont ensuite réfléchi à de nouveaux outils en introduisant un nouveau paradigme : une approche collaborative de l'information (structurer la botte de foin). Les principes introduits sont les suivants :

- la syndication de contenu, qui permet à un producteur d'information (sous forme de contenu web) de republier ce contenu vers d'autres sites web (fichiers structurés au format RSS-XML) ;
- l'étiquetage en utilisant des étiquettes (*tags*) pour améliorer la recherche sémantique ;
- l'étiquetage social ou folksonomie (on sélectionne les données selon son degré d'intérêt dans une communauté d'utilisateurs) ;
- la participation et le partage de l'information ;
- l'utilisation du langage XML (*eXtensible Markup Language*) et des mécanismes (méthodes) du protocole HTTP pour développer de nouveaux services web (ex. SOAP *Simple Access Object Protocol*).

Ces concepts ont conduit au développement de nouveaux services et outils :

- l'écriture en temps réel de documents (Google doc, wiki, etc.) ;
- les agendas web partagés ;
- la veille internet (flux RSS) ;
- la communication en ligne (blogs) ;
- la publicité ciblée (Yahoo Search Marketing) ;

- le E-commerce ;
- la gestion des connaissances (wikipedia) ;
- les réseaux sociaux (LinkedIn...).

1.4.4 Dimension importante du SI : l'être humain

La notion de travail a beaucoup évolué sous l'effet structurant des technologies de l'information (désignées maintenant sous le terme de technologies numériques) sur les processus et activités. Le poste de travail autour du PC constitue aujourd'hui l'unité de base du système d'information (figure 1.15). L'individu travaille avec une machine. Quelle est la part de l'un et de l'autre à l'ère de l'intelligence artificielle ?

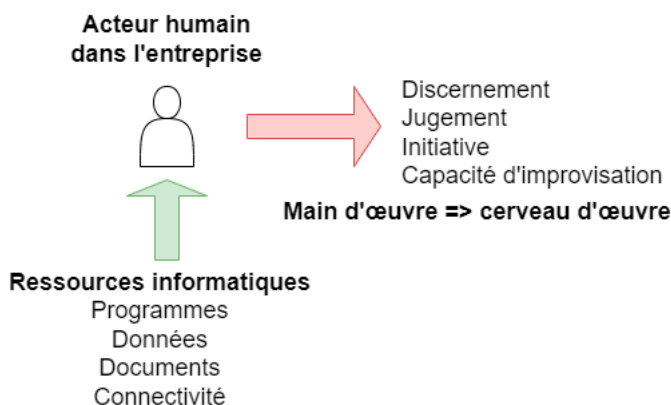


FIGURE 1.15 – L'unité de base du SI

L'être humain ne peut traiter à la fois plus de 7 données alors que la machine n'a pas de limite. Ceci a son importance en terme de décision. La machine est là pour aider les décideurs, pas pour décider à leur place. L'être humain fatigue, peut se tromper, pas la machine. La machine a donc sa place dans les tâches répétitives, sans fatigue, consommant beaucoup de données. Mais l'être humain peut improviser en cas de situation nouvelle. Ceci a son importance dans la gestion de crises. La comparaison résumée figure 1.16 peut néanmoins évoluer en faveur de la machine, douée de plus en plus de capacité avec des techniques d'intelligence artificielle. Néanmoins l'émotion, la pro-activité, l'innovation, l'improvisation sont encore du ressort de l'être humain.

La qualité d'un système d'information repose sur la séparation intelligente et optimale entre ce qui relève de l'humain et ce qui relève de l'automate. Les contre-exemples abondent et relèvent souvent des absurdités héritées de l'organisation scientifique du travail :

- enfermer les acteurs dans des consignes, programmer leurs actions ;
- empêcher les actions "non prévues par la machine" (quand elle n'a pas été programmée pour ça).

FIGURE 1.16 – Être humain *vs* machine

1.4.5 Où on (re)parle d'intelligence artificielle

Le but de l'intelligence artificielle est de faire simuler l'intelligence humaine par la machine. L'idée n'est pas nouvelle. Cette discipline comporte un certain nombre de corpus théoriques et de techniques logicielles qui se sont beaucoup développées entre les années 60 et 90. Un des grands principes est la notion d'apprentissage, dont la finalité est la compréhension de l'environnement (terme à contextualiser), par l'exploitation de données (du contexte). Cela permet de décider de l'action opportune. Ce qui a relancé cette discipline depuis plusieurs années, c'est la quantité de données dont on dispose, dont les sources sont multiples : données du SI, historiques, capteurs, objets connectés et dont les formats sont multiples (tableaux, signaux, images, échantillons statistiques, données textuelles...). Le terme Intelligence Artificielle a d'ailleurs un peu débordé de son cadre d'origine (des concepts d'inférence (raisonnement) développés par les informaticiens spécialistes d'IA) pour intégrer les boîtes à outils des traitements du signal et de l'image, les traitements statistiques.

1.4.6 Éléments d'infrastructure

Le SI s'appuie sur un système global inter-connecté. Le réseau joue donc un rôle clé. L'indisponibilité du réseau (local et surtout distant, accès à l'internet notamment) peut avoir un effet très pénalisant, selon le degré d'exposition à des ressources externes. L'infrastructure réseau d'une entreprise est ainsi constituée d'une

infrastructure locale (figure 1.17) mais aussi des ressources fournies par les opérateurs télécoms : pour accéder à internet, pour interconnecter les sites d'entreprise (figure 1.18), pour permettre aux itinérants d'accéder à l'intranet (figure 1.19), pour accéder aux données ou aux applications chez un hébergeur dans le nuage (*cloud*).

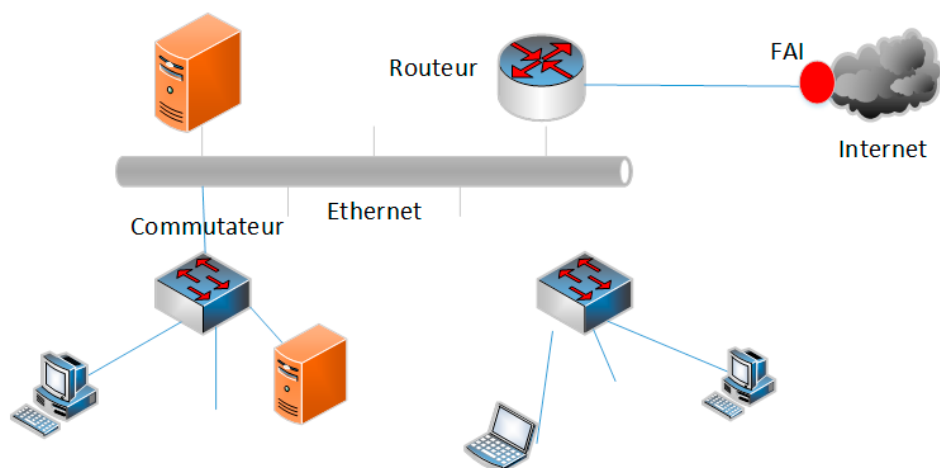


FIGURE 1.17 – Réseau local (LAN)

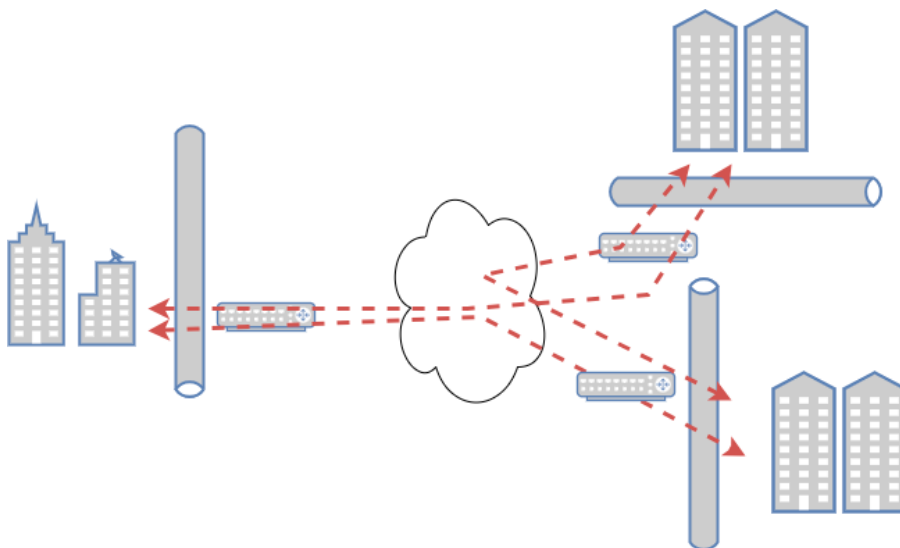


FIGURE 1.18 – Interconnexion

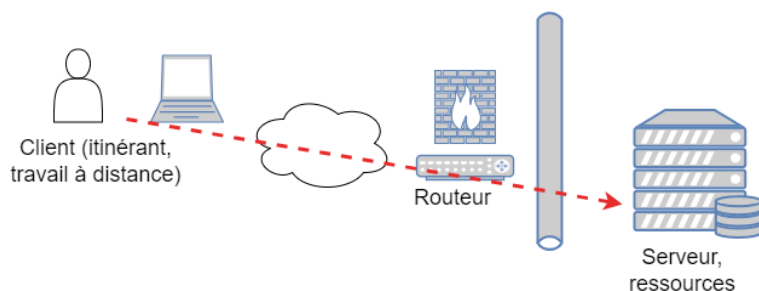


FIGURE 1.19 – Itinérance

L'infrastructure réseau d'une entreprise, quelle que soit sa taille, doit assurer aujourd'hui d'autres services qui se sont banalisés :

- l'accès sans fil par la technologie IEEE 802.11 ou Wifi (figure 1.20), celle-ci requiert une authentification des accès robuste ;
- l'accès à l'internet pour les visiteurs. En terme de sécurité ceux-ci ne doivent pas accéder aux ressources internes (figure 1.21).

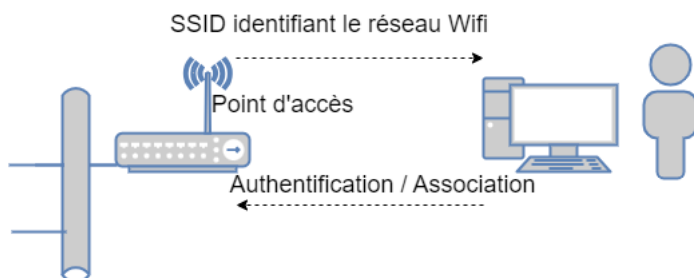


FIGURE 1.20 – Accès wifi

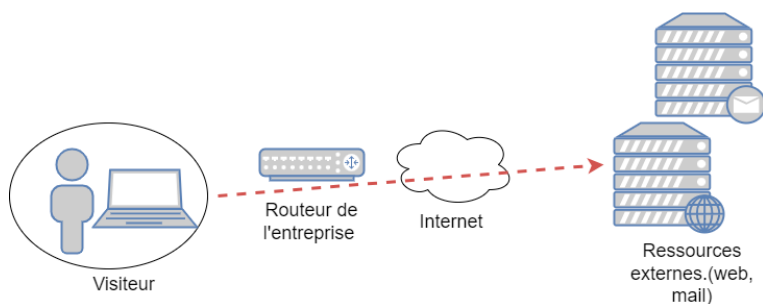


FIGURE 1.21 – Les visiteurs de l'entreprise

1.4.7 Configuration de base d'un poste de travail

Pour être opérationnel, en particulier pour accéder aux services en réseau, le poste de travail doit être configuré avec les éléments suivants :

- l'adresse IP du poste ainsi que le masque associé à son réseau de rattachement ;
- l'adresse IP de sa passerelle (le routeur) ;
- l'adresse IP du serveur DNS ;
- l'adresse IP du serveur DHCP (si le terminal a besoin d'un mécanisme d'attribution dynamique d'adresse IP).

On voit donc que plusieurs serveurs sont nécessaires pour réaliser un service réseau minimum. Certains sont publics, d'autres ne doivent absolument pas l'être :

- serveurs publics : serveur web, serveur de messagerie, serveur DNS ;
- serveurs privés : serveur DHCP, serveurs métiers, serveur intranet.

Rappelons une fois encore qu'un serveur public est un serveur visible par le système DNS. Pour cela les adresses IP (publiques) des serveurs publics doivent figurer dans les fichiers de configuration du serveur DNS du domaine.

1.4.8 Virtualisation

Le concept de virtualisation n'est pas nouveau. Le principe est le suivant (cf. figure 1.22) : une ressource (temps de travail d'un processeur) n'est pas utilisée à 100% du temps par un même utilisateur. L'idée est alors de centraliser sur un serveur (hôte) les ressources de la tâche à exécuter, entre plusieurs clients, sans que ceux-ci ne sachent rien de leur localisation. La ressource est seulement accessible à distance (peu importe où elle soit).

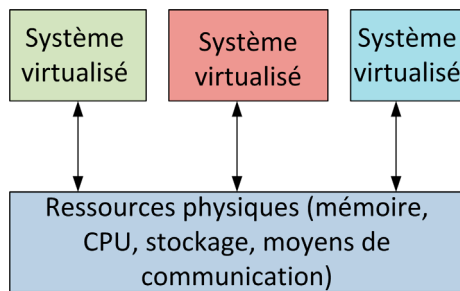


FIGURE 1.22 – Virtualisation

Tout ce qui relève du logiciel peut donc être virtualisé : système d'exploitation, application, gestion d'espaces de stockage, et même des fonctions réseau comme le routage (figure 1.23).

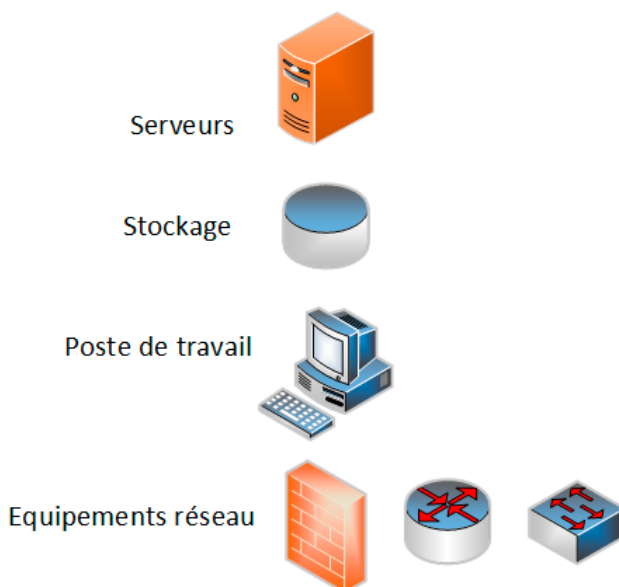


FIGURE 1.23 – Équipements virtualisables

Plus techniquement, la virtualisation consiste à créer des machines virtuelles (VM) à partir d'une "machine" réelle à l'aide d'un logiciel appelé hyperviseur. Les VM fonctionnent de la même manière que les machines réelles dont elles sont l'image, mais elles ne s'appuient sur les ressources que d'un seul système informatique, celui du serveur hôte. La virtualisation permet d'exécuter plusieurs systèmes d'exploitation sur un seul hôte. L'hyperviseur attribue des ressources (de traitement, de stockage) à chaque ordinateur virtuel, en fonction des besoins. Cette allocation flexible des ressources rend les opérations informatiques beaucoup plus efficaces et rentables. Les avantages sont les suivants :

- on réduit les coûts matériels ;
- l'administration est facilitée (elle est faite au niveau hôte, indépendamment du nombre de clients) ;
- on peut redémarrer après défaillance (en télé-chargeant l'image d'un poste par ex.) ;
- le contrôle des droits d'accès est facilité (conséquence de la centralisation).

Il existe aussi des inconvénients et des contraintes :

- une analyse préalable complète des installations est nécessaire avant mise en œuvre ;
- le parc informatique doit être homogène (tous les postes ont la même image) ;
- le système devient totalement dépendant de la disponibilité du réseau de l'opérateur ;

- toute défaillance au niveau hôte impacte tout le système, ce qui oblige à prévoir des redondances ;
- la consommation de ressources (poste client, hôte, réseau) et donc d'énergie est supérieure à ce qu'elle serait en mode local.

1.4.9 Le cloud computing

Principes

Le cloud-computing est un environnement en réseau (essentiellement internet) basé sur le principe du partage des ressources de traitement et de stockage. Les opérateurs de cloud utilisent les technologies de la virtualisation combinées avec des mécanismes d'utilisation optimale des ressources via leur infrastructure réseau à haut débit (plusieurs Tera-octets). La performance du service cloud repose sur :

- des ressources en libre service ;
- l'accès au service en tout lieu et depuis n'importe quel interface ;
- l'allocation dynamique et à la demande des ressources ;
- le temps de réponse et (en apparence) sans plafonnement de capacité.

Il existe 3 types de services cloud (voir figure 1.24), SaaS, PaaS et IaaS. Il existe trois modèles de cloud : public, privé, hybride.

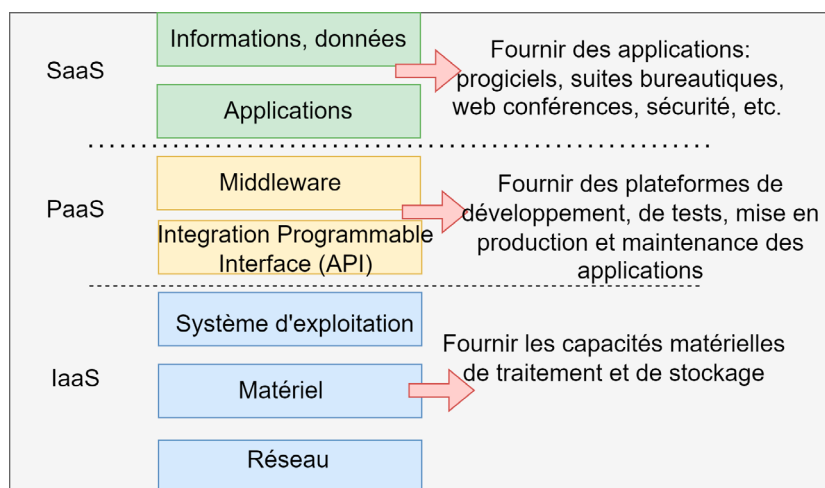


FIGURE 1.24 – Les types de cloud

Software as a Service (SaaS)

Le client a la possibilité d'utiliser les logiciels fournis sans se soucier des problèmes de mise à jour, correctifs (*patches*) de sécurité ou compatibilité. Les logiciels sont accessibles via un portail web ou installés en local sur les machines concernées. Le client ou l'entreprise loue ce service via un forfait, ce qui implique qu'il ne possède pas les licences des logiciels qu'il utilise via ce système.

Platform as a Service (PaaS)

Le client peut louer des ressources matériels (hardware) et logiciels (software) de bas niveau telles que les systèmes d'exploitation ou des gestionnaires de bases de données, principalement dans le but de disposer d'un environnement de travail et de développement sans les contraintes matérielles et logicielles habituelles.

Infrastructure as a Service (IaaS)

Le prestataire met à disposition des ressources informatiques, telles que des serveurs de stockage ou des réseaux, dans un environnement virtualisé. C'est-à-dire que le fournisseur offre un accès immatériel à ses différents data-centres qui peuvent se trouver à des lieux différents et qui forment une infrastructure globale. La société est alors dispensée des coûts d'achats dans des infrastructures physiques onéreuses, tout en gardant le contrôle sur le déploiement de son réseau et des applications qu'elle souhaite installer ou utiliser.

Cloud public

Il constitue le modèle standard de cloud computing. Un ou plusieurs fournisseurs de services louent des ressources, en fonction des besoins : serveurs de stockages, logiciels de communication ou tous autres éléments dont la société a besoin. Ils sont le plus souvent facturés via un abonnement. Les données des clients sont stockées dans des data-centres externes à l'entreprise. La sécurité des données est l'apanage du fournisseur de ressources. On peut citer les cloud Citrix, Google, Amazon AWS, Microsoft Azure.

Cloud privé

Il se distingue par la localisation, la sécurité, la gestion et le financement. Les data-centres appartiennent aux entreprises. Ils peuvent être sur le site ou dans des locaux externes. Les données sont stockées exclusivement sur des serveurs privés et à usage limité aux seuls ayant-droits. La politique de sécurité peut donc être adaptée et au besoin renforcée par l'entreprise détentrice. Les services virtualisés dans un cloud privé doivent être gérés par un administrateur réseau, employé ou non de l'entreprise. Celui-ci est garant du fonctionnement. Enfin, un service de cloud privé représente un coût fixe pour les entreprises. Elles doivent prévoir le remplacement des infrastructures mais également le coût financier d'une migration ou d'une extension du réseau.

Cloud hybride

C'est une combinaison de cloud privé et de cloud public. Ce modèle accroît les possibilités d'adaptation et de gestion. Les données sensibles, comme des logiciels applicatifs particuliers, peuvent être hébergées sur une partie privée tandis que les éléments de communication ou de stockages (messagerie instantanée, documents de travail) peuvent être externalisés sur un cloud public. Le plus gros défi de ce modèle réside dans sa complexité à faire fonctionner deux éléments et de répartir la

charge de travail entre les deux catégories de serveurs dans le sens d'une efficacité optimale.

1.4.10 Aspects sécurité

Les données constituent le carburant des processus et notamment les processus métier, censés créer de la valeur ajoutée. Le bon fonctionnement du SI repose donc sur le bon fonctionnement de deux niveaux :

- N1 : le niveau matériel (système informatique, infrastructure) ;
- N2 : le niveau données (applications, processus) qui dépend du bon fonctionnement de N1.

Le bon fonctionnement nécessite donc de sécuriser à la fois l'infrastructure (le système) et le niveau applicatif (la partie utile). Un système perturbé fait dysfonctionner les processus qui l'utilisent tout comme des données falsifiées le perturbent, impliquant des tableaux de bord faux, des décisions biaisées voire inopérantes. L'un et l'autre doivent donc être protégés.

La décentralisation des tâches vers des postes de travail plus performants implique aussi la décentralisation des besoins de sécurité, ce qui implique les utilisateurs et les responsabilise.

En terme de sécurité, la virtualisation des postes peut être bénéfique : homogénéité du parc, possibilité de réinitialiser les postes à partir de leur image (principe du bureau virtuel). L'inconvénient repose sur la place centrale de l'hyperviseur. Si celui-ci est attaqué, ce sont toutes les machines virtuelles (VM) qui sont menacées. Autre problème pour les clients de solutions cloud : la forte dépendance aux opérateurs télécoms pour accéder aux ressources à distance. L'indisponibilité du réseau (et donc des données) bloque tous les processus qui l'utilisent. Ce que les clients de service cloud attendent donc, c'est la performance et la sécurité.

1.5 Les systèmes cyber-physiques

1.5.1 Couplage physique/ logique

Dans le domaine industriel, la réalité des actions, des processus, des tâches, peut être vue à distance sous forme de données, fournies par des capteurs. Par quoi ? Par des systèmes centralisés de contrôle. La notion de distance est ici très large, cela va du niveau local (site, chaîne de production) à un niveau distant et centralisé. La figure 1.25 représente le principe du contrôle d'un processus industriel. Le processus est initialisé avec (entre autres) des données (des objectifs), des consignes et le pilotage consiste à vérifier au cours de l'exécution que l'état du processus est conforme à ce qui est attendu, c'est-à-dire dans un intervalle de valeurs satisfaisant. Cette vérification continue repose sur le suivi de variables d'action, mesurées par des capteurs, mesures communiquées à un niveau de contrôle centralisé. Toute dérive du processus peut ainsi conduire en retour à activer des moyens d'action (des actionneurs) à des fins correctives. Ces corrections peuvent être déclenchées de façon automatisée mais aussi par décision humaine.

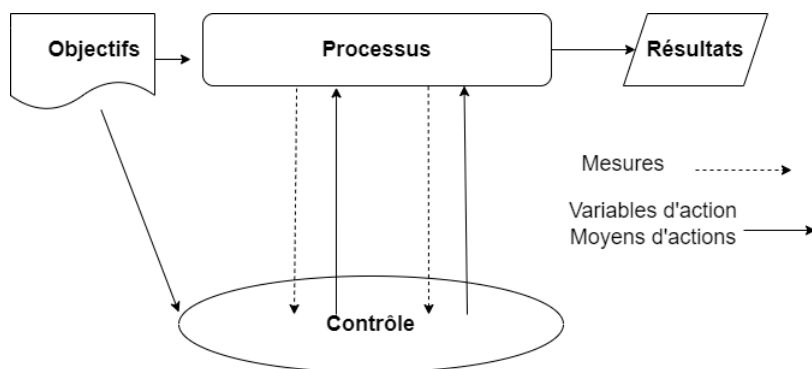


FIGURE 1.25 – Contrôle des processus physiques

Dans le domaine industriel le contrôle requiert des experts (technicien, ingénieur), des moyens automatisés, des interfaces représentant de façon synthétique les données de ce qui se passe à distance. Si ces données sont perdues ou falsifiées, cela revient donc à falsifier la perception du réel par celui qui contrôle à distance. Quelles sont les activités humaines concernées ? Tout ce qui relève de la perception de l'environnement, de la décision, du contrôle.

1.5.2 Les systèmes cyber-physiques

La relation physique / logique entre processus et son contrôle est généralisée dans les systèmes cyber-physiques (appelés aussi socio-techniques). Ces systèmes sont souvent répartis, de grande taille (ex. un réseau de transport, un réseau de distribution d'eau ou d'énergie). Le système de contrôle nécessite d'être structuré et hiérarchisé en assurant le contrôle au niveau régional, puis au niveau national. La figure 1.26 illustre le découplage du système en deux plans : le plan physique et le plan contrôle.

Le plan physique regroupe tous les éléments / ressources destinées à faire fonctionner le processus physiquement (automates, capteurs, actionneurs). Le plan contrôle contient toutes les ressources destinées au contrôle, au pilotage, aux décisions opérationnelles (applications spécialisées, serveurs de données, historiques de données, interfaces homme / machine).

Dans le plan physique le réseau interconnecte des nœuds de production, distribution : réseau électrique, réseau de transport, réseau d'eau...

Dans le plan contrôle le réseau est un réseau de communication où circulent des trames / paquets contenant des données des capteurs ou en retour des ordres envoyés aux actionneurs. Le plan contrôle est celui où on traite et où circulent les avatars numériques du monde réel.

Le modèle d'interaction entre processus physique et contrôle est présenté figure 1.27.

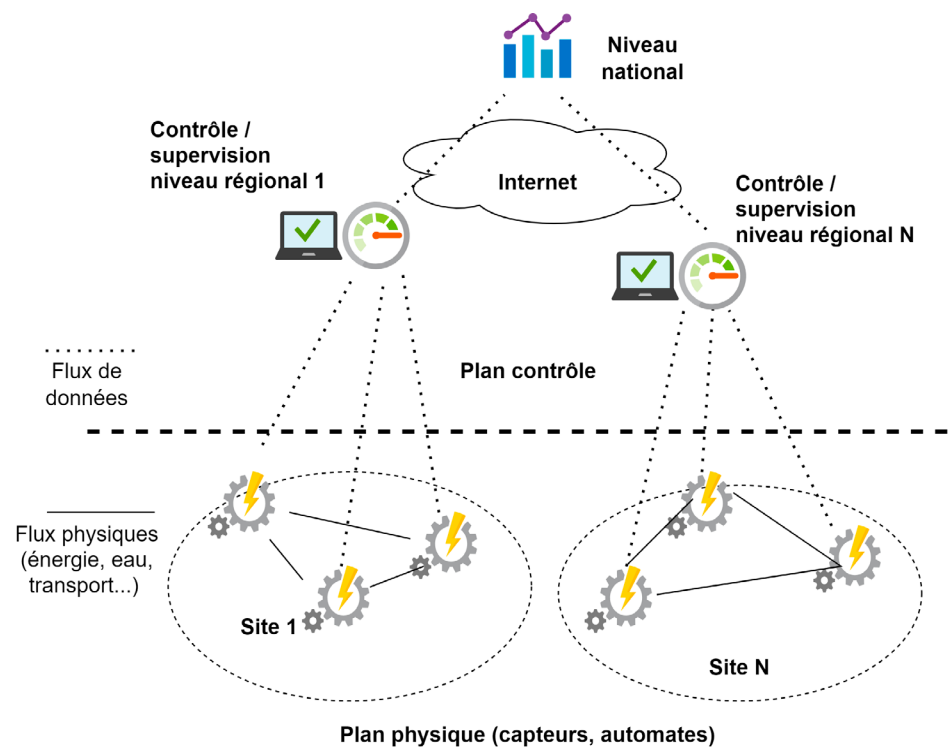


FIGURE 1.26 – Systèmes cyber-physiques

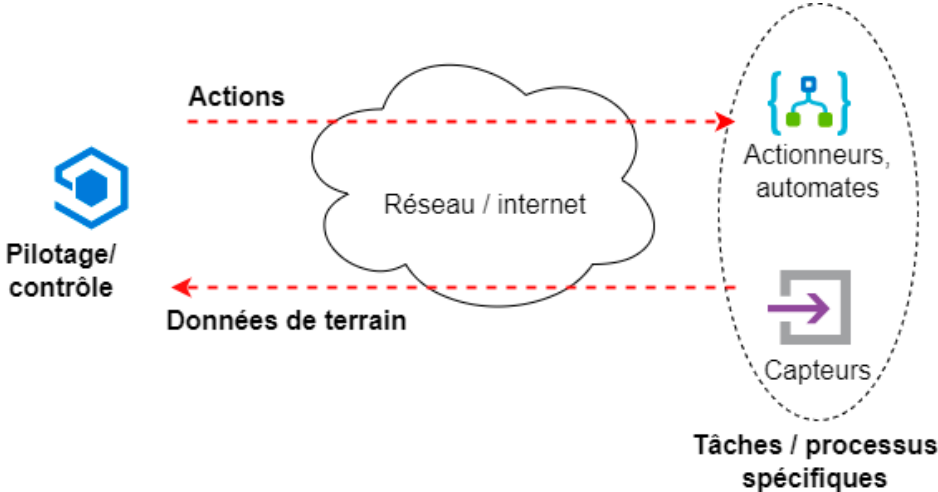


FIGURE 1.27 – Interactions physique/contrôle

1.5.3 Les objets connectés

Définitions

Le terme "internet des objets" se veut une traduction de *Internet of Things (IoT)*, qui veut dire "internet des choses". La chose en question désigne un objet très élémentaire.

L'IoT intègre à la base des technologies connues : capteurs, technologie RFID *Radio Frequency Identification*, technologie NFC *Near Field Communication*, technologies des liaisons radio (WPAN, bluetooth, Zigbee), cloud, technologies du web 2.0, ingénierie logicielle orientée service, etc.

Le terme "internet des objets" désigne en réalité un ensemble indéfini dans lequel on trouve généralement :

- l'objet technologique, plus ou moins autonome, composé d'au moins un capteur (qui mesure) et souvent aussi d'un actionneur (qui modifie son environnement) ;
- une interaction plus ou moins distante avec le plus souvent une liaison sans fil (pour interagir avec l'objet).

L'idée de base est de faire agir entre eux une variété d'objets pour réaliser un but commun. Pour cela ils ont besoin de communiquer via l'internet, d'avoir une identité propre et unique. Les objets sont en réalité définis par le domaine applicatif qui les utilise.

Il existe 3 visions de l'internet des objets, issues de communautés différentes ([6]) :

- la vision "thing", issue de la communauté RFID, où l'IoT est un réseau global d'objets via un adressage unifié et utilisant des protocoles standards. Le problème est ici d'améliorer la visibilité de l'objet : le localiser, le tracer, surveiller son état ;
- la vision "internet", issue de la communauté IPv6, où le problème est d'étendre l'internet de l'équipement (*device*) à l'objet via des protocoles allégés et donc moins consommateurs d'énergie ;
- la vision sémantique, issue de la communauté du web, où on s'intéresse ici à l'information (nouvelle) produite par les objets (du monde physique) et à dépasser l'objet-chose vers une notion d'objet intelligent. La problématique est ici de représenter, stocker, interconnecter, indexer, interagir avec des contextes sociaux, environnementaux, des usagers...

Les applications IoT

L'espace des applications est vaste mais elles vont toutes s'appuyer sur le même concept, résumé figure 1.28. Les capteurs et actionneurs sont de nature physique, biophysique, physico-chimique : pression, mouvement, température, position, accélération, hygrométrie, etc. Les nanotechnologies permettent aujourd'hui de miniaturiser les capteurs et donc de les disséminer plus facilement. Ils communiquent avec un contrôleur plus ou moins distant. La contrainte est souvent l'autonomie en énergie de ces objets.

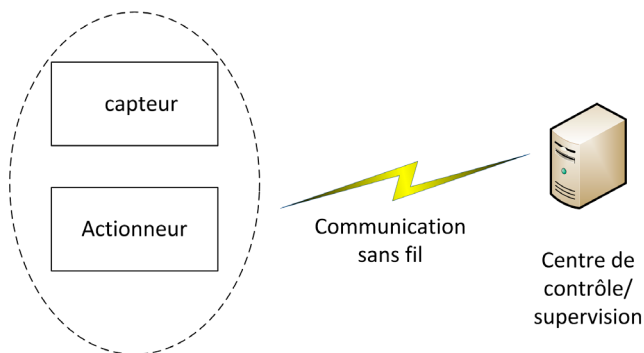


FIGURE 1.28 – Objet connecté

Des exemples

Les exemples d'applications ne manquent pas. On peut les regrouper par secteur :

- le secteur hospitalier : autour du lit médicalisé par ex. (voir figure 1.29) ;
- la ville intelligente : gestion de la circulation, des ressources urbaines, des déchets, de l'énergie (voir figure 1.30) ;
- la gestion des flux : eau, énergie ;
- les véhicules connectés : maintenance, diagnostic à distance ;
- la logistique : suivi d'une commande faite via un site de e-commerce ;
- la gestion technique des bâtiments (GTB) : sécurité physique, énergie, ventilation, fluides, ascenseurs...

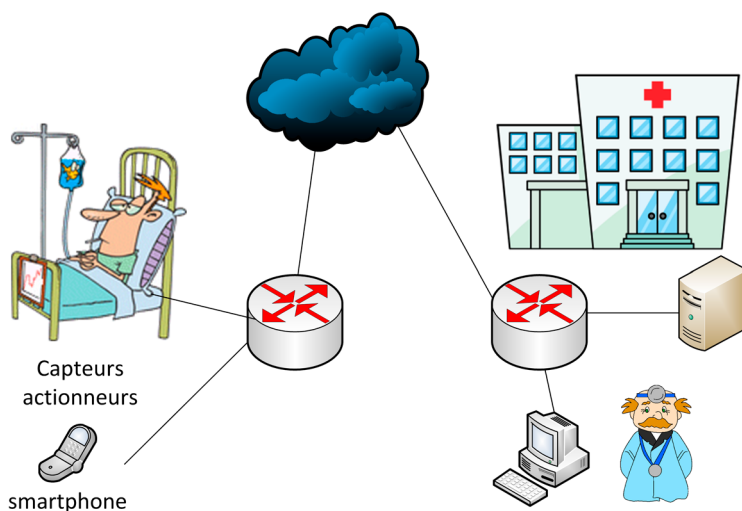


FIGURE 1.29 – IoT et E-santé

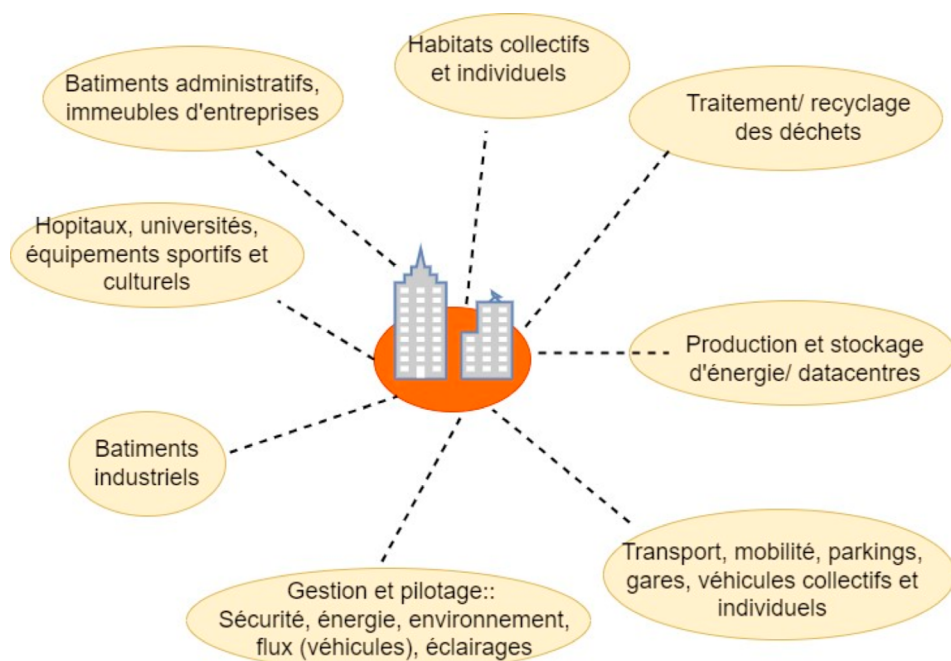


FIGURE 1.30 – Villes intelligentes

L'IoT est à la base des systèmes dits intelligents (*smarts systems*). Les idées directrices sont les suivantes :

- apporter flexibilité, fiabilité, efficacité dans les opérations liées aux infrastructures ;
- réduire les coûts et la main d'œuvre ;
- améliorer la sécurité des biens et des personnes.

IoT dans l'entreprise

La figure 1.31 présente un exemple d'usage de l'IoT dans l'entreprise : les extincteurs connectés [7].

La figure 1.31 montre surtout les interactions créées par les objets connectés et l'externalisation des services qui les utilisent. Pourquoi connecter l'extincteur ? Pour connaître son état sans avoir à se déplacer (en l'occurrence le prestataire chargé de son installation et de sa maintenance). Mais ce prestataire n'est pas le concepteur. Les fonctionnalités logicielles (et donc ses évolutions) sont du ressort du concepteur du dispositif IoT associé à l'extincteur.

En cas de sinistre, ce sont les pompiers qui ont accès physiquement à l'extincteur. Les extincteurs connectés sont situés dans l'enceinte privé de l'entreprise et utilisent une partie de l'infrastructure réseau de celle-ci pour communiquer de et vers l'extérieur. Il y a donc de fait une interdépendance entre système de sécurité

connecté à des tiers et système d'information de l'entreprise, c'est-à-dire entre deux systèmes dont les niveaux de sécurité (et les exigences) sont a priori dissemblables. Le canal de communication entre extincteur connecté et prestataire extérieur représente donc potentiellement une porte dérobée pour s'introduire dans le système d'information.

De façon générale, les entreprises externalisent nombre de fonctions comme la gestion technique des bâtiments, mais aussi la maintenance des équipements industriels auprès de prestataires extérieurs qui disposent ainsi de droits d'accès aux équipements qu'ils gèrent à distance. Ceci constitue potentiellement la principale porte d'entrée pour perturber un système d'information et pire encore en terme d'impact : un système industriel.

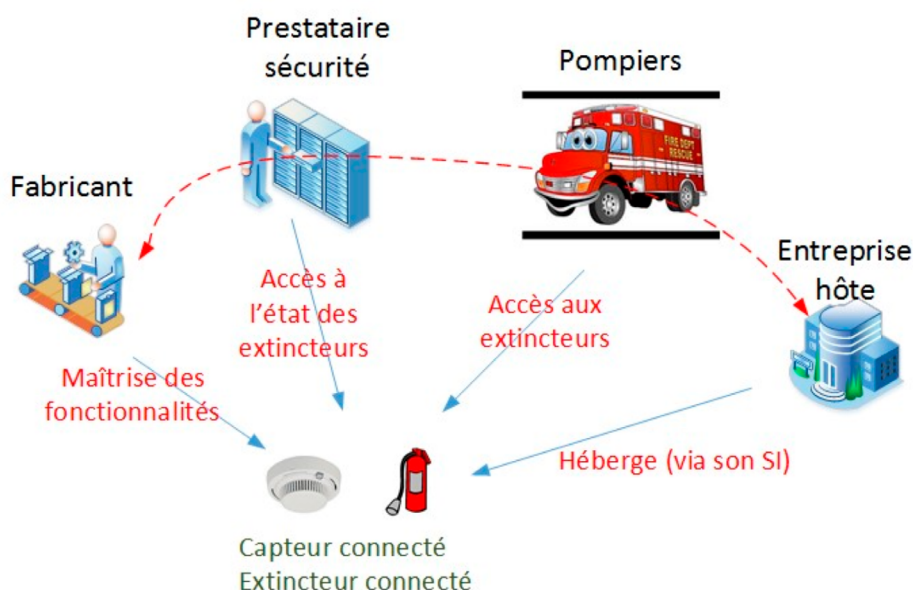


FIGURE 1.31 – Extincteurs connectés (d'après [7])

Effet de masse

On annonçait plus de 250 milliards d'objets connectés en 2020. À vrai dire le comptage n'a pas d'intérêt sauf pour illustrer la généralisation du concept IoT pour intégrer des technologies autour d'applications à la fois grand public et professionnelles (dans le monde industriel on parle de I-IoT). Les pouvoirs publics des pays industrialisés s'en sont emparés. Dans les années 2010 l'IoT faisait partie des 34 points du plan de reconquête industrielle de la France. La Chine veut être le pays de l'IoT (autour de la surveillance et du contrôle des citoyens). L'Allemagne a privilégié les applications industrielles autour des technologies M2M (*Machine to Machine*) ; les USA autour de la santé et de l'hôpital. Des pays asiatiques comme

la Corée ou la Malaisie développent autour des villes intelligentes (l'Asie comporte les plus grandes métropoles).

1.6 Un univers de données

1.6.1 Donnée/ Information

L'information est le socle sémantique de l'entreprise. Il est l'élément clé de l'innovation, elle fait partie de ce qu'on appelle le capital informationnel. Elle a une valeur d'usage pour qui sait l'interpréter.

La donnée est définie par une sémantique et une valeur. La donnée est indépendante de l'application qui l'utilise et donc du fichier qui la contient. Elle a un format, pour être stockée, traitée, affichée.

La différence entre donnée et information tient dans l'interprétation, comme le montre la figure 1.32.

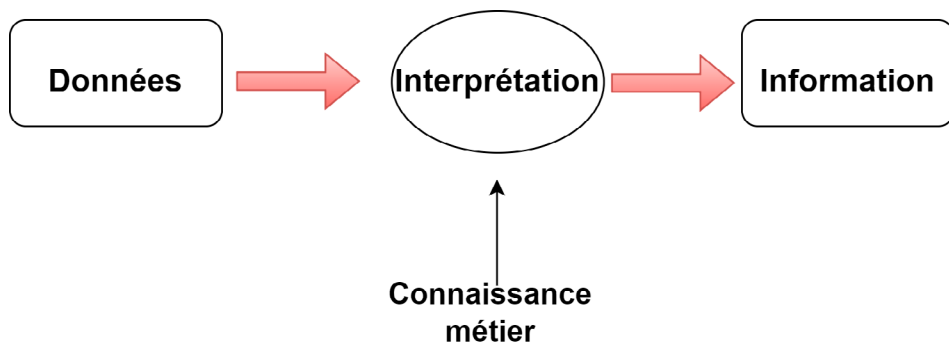


FIGURE 1.32 – Données *vs* information

1.6.2 Les fichiers

Les fichiers contiennent les données. Ils dépendent de l'application pour : la création, l'affichage, la modification, la conversion...

Un document est un fichier composite qui peut intégrer plusieurs documents élémentaires. Les fichiers .pdf ou .docx peuvent être vus comme des documents intégrant des objets d'origine diverse (images, tableaux).

Les fichiers ou documents ont une durée de vie qui dépend souvent de la communauté qui les utilise. Le domaine juridique ou le domaine médical peuvent ainsi avoir des cycles de vie très longs pour certains documents, au-delà même de la durée de vie des personnes dont il est question dans les dossiers. La figure 1.33 synthétise les différentes phases de ce cycle de vie.

Du fait de la dématérialisation des procédures les fichiers peuvent être générés à toutes les tâches qui exploitent des outils numériques. L'ordinateur personnel, les serveurs mais aussi les imprimantes et les photocopieurs qui conservent dans leur disque dur une copie fichier de toutes les opérations qu'elles enregistrent.

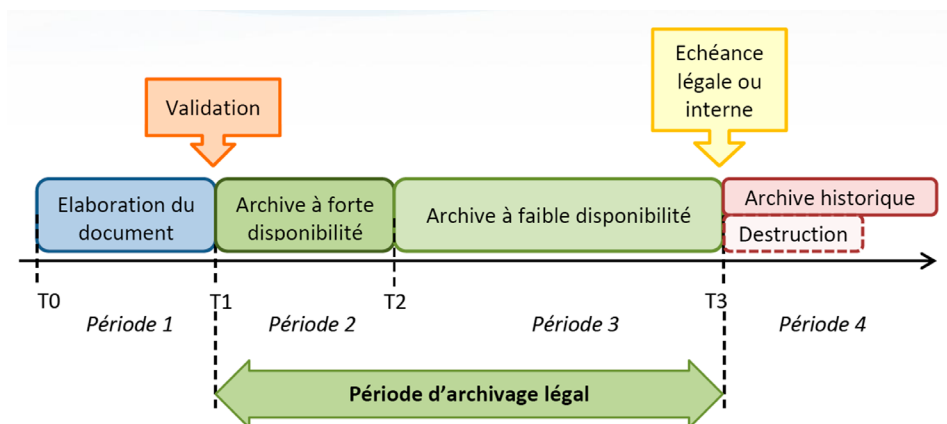


FIGURE 1.33 – Cycle de vie d'un document

La figure 1.34 synthétise les différentes sources de dématérialisation aboutissant à la création de fichiers.

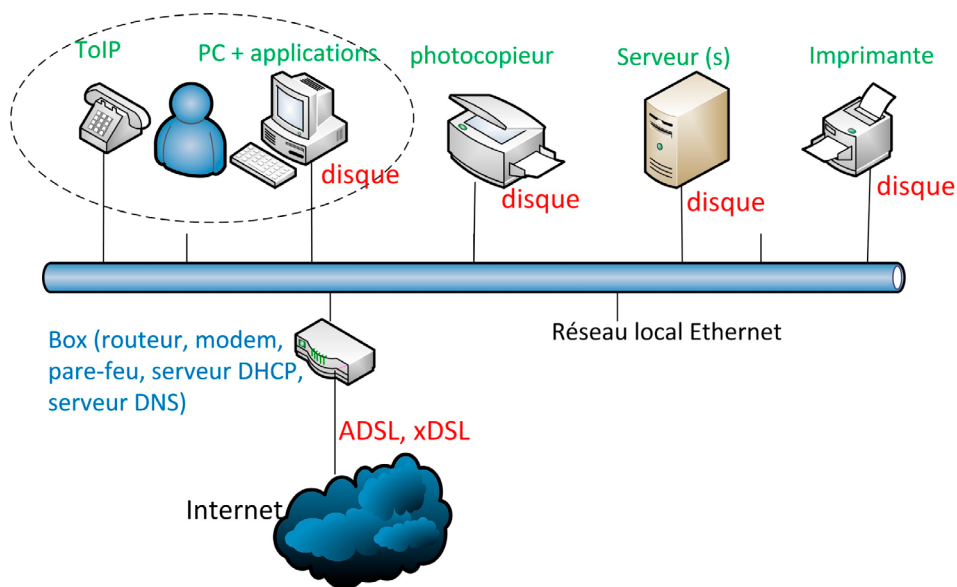


FIGURE 1.34 – Sources de dématérialisation

1.6.3 Les données personnelles

Qu'est-ce qu'une donnée personnelle ?

Une donnée personnelle est une donnée qui permet d'identifier une personne en particulier, notamment : état civil, adresse, numéro de téléphone, numéro de sécurité sociale, plaque minéralogique, adresse IP (même dynamique), photo, vidéo, dossier médical, enregistrement de la voix...

Où sont les données personnelles ?

La question se pose dans toute entreprise. La plupart des services sont concernés :

- les ressources humaines (employés, stagiaires, prestataires) ;
- les services juridiques (prestataires, clients) ;
- les services commerciaux (clients) ;
- les services achat (fournisseurs) ;
- les services production (prestataires) ;
- les services financiers (actionnaires) ;
- les services communication (partenaires, prestataires) ;
- la direction (membres du conseil d'administration).

La difficulté est de recenser les processus de l'entreprise qui utilisent / génèrent des données personnelles. C'est le rôle du DPO (*Data Privacy Officer*), nouveau métier qui a remplacé le CIL (Correspondant Informatique et Liberté) suite à la mise en application en 2018 de la réglementation européenne sur la protection des données personnelles.

Beaucoup de données sont physiquement stockées dans le nuage. C'est d'ailleurs une des motivations des attaquants de cloud que de voler par ex. des données médicales car elles représentent une valeur marchande.

Insistons ici sur d'autres espaces de stockage des données personnelles dans l'entreprise, souvent ignorés, comme le montre la figure 1.35.

Les imprimantes et autres photocopieurs conservent sur leur disque dur interne une copie au format pdf de tout document photocopié. Or beaucoup de ces documents contiennent des données personnelles mais aussi des données confidentielles pour l'entreprise, voire sensibles. À la fin du cycle de vie de la photocopieuse, celle-ci est reprise par le prestataire, avec son disque dur. Or ce disque fait partie des consommables, il devrait être retiré avant cession par l'entreprise et ensuite physiquement détruit.

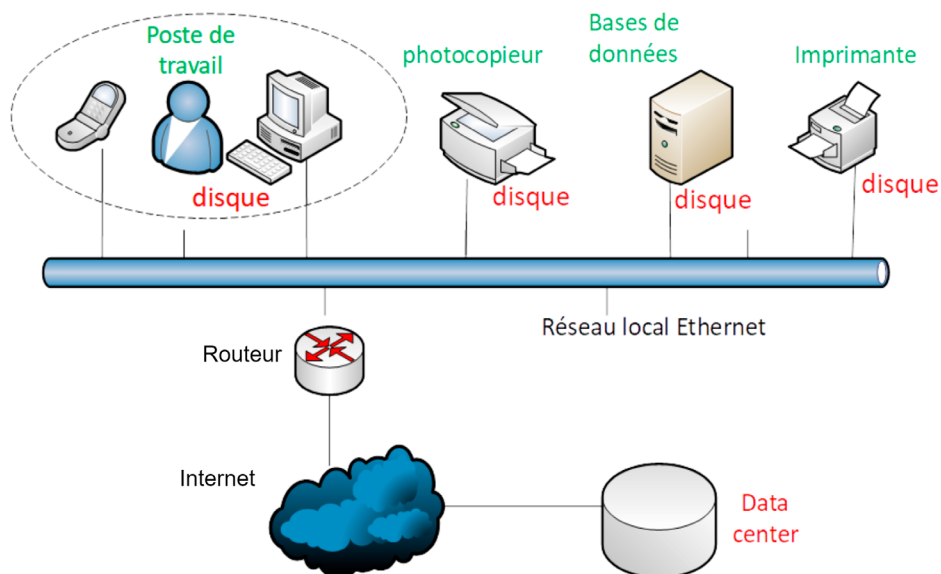


FIGURE 1.35 – Sources de données personnelles

1.6.4 Les méta-données

Un fichier comprend les données (partie utile) et des méta-données. Les méta-données renseignent sur le "quoi" des données. Elles sont générées par défaut par l'application. Elles peuvent être complétées par l'utilisateur.

Elles comportent des mots-clés qui peuvent ensuite être exploités pour l'indexation, le référencement. On trouve ainsi des méta-données :

- générales : nom, type, taille, créé le, modifié le, dernier accès le ;
- descriptives : titre, objet, mots-clés, commentaires ;
- d'origine : auteur, dernier enregistrement, numéro de version, nom de programme, entreprise ;
- de contenu : état, nombre de mots, nombre de caractères, nombre de ligne, etc.

Les méta-données dites Exif concernent les photos :

- les caractéristiques de l'appareil ;
- les caractéristiques de la photo (ses paramètres) ;
- les coordonnées GPS ;
- l'horodatage.

Comme on le voit, les méta-données ont un potentiel informationnel important qui peut contenir des données personnelles, il est souvent ignoré. Les méta-données de description sont vides par défaut. Les autres sont remplies de façon automatique. Elles sont renseignables, anonymisables, modifiables, falsifiables.

1.6.5 Le big data

Le concept de big data cumule les effets de trois lignes directrices :

- *too big* : on accumule des quantités faramineuses de données, mesurables en péta-octets ;
- *too fast* : on peut stocker des événements en temps réel : par ex. un clic de souris ;
- *too hard* : les outils construits autour des bases de données ne sont plus adaptés.

Les données proviennent de toutes sources susceptibles d'en produire (notamment et surtout les objets connectés). Les formats sont hétérogènes : texte, image, son, statistiques, etc. On utilise des outils du *data mining*, devenus souvent *big data mining and analysis* pour explorer les données, définir des modèles, faire des prévisions. Comme on l'a déjà mentionné, l'être humain ne sait pas décider à partir de plus de 7 données à la fois, les outils du *visual analytics* doivent permettre au décideur d'interagir avec des interfaces qui visualisent des données de traitement avec une ergonomie synthétique et adaptée : courbes, graphiques, tableaux...

Le big data est à l'origine d'une révolution épistémologique. Autrefois (il y a encore 20 ans) on disposait de peu de données, et on raisonnait sur des modèles. Maintenant on n'a pas de modèle a priori mais on dispose d'une quantité faramineuse de données et on construit des modèles par apprentissage en utilisant les techniques de l'intelligence artificielle. On est ainsi capable de faire des prévisions sans théorie ni modèle préalable. Le phénomène touche notamment les sciences humaines (psychologie, sociologie, études du comportement). L'utilisation principale des technologies du big data est surtout de constituer des profils comportementaux : citoyen, consommateur...

1.7 Vers le cyber-espace

1.7.1 Aspects géopolitiques

Dans les années 2000, il y avait 250 millions d'internautes. L'internet était un environnement universel auto-régulé, sans frontière. Il a été un moteur économique et commercial (bulle de l'internet).

En 2020 il y avait près de 5 milliards d'internautes, dont environ 850 millions de Chinois contre 244 millions d'Américains. On retrouve donc dans cette projection le poids démographique des pays respectifs.

Tous les systèmes d'information sont interconnectables (ils ne le sont pas directement, mais peuvent l'être de façon indirecte). Chaque entreprise a son écosystème : fournisseurs, partenaires, distributeurs, etc., ce qui se traduit par le fait que les SI respectifs sont interconnectés pour des échanges de données. Chacun de ces partenaires ayant lui-même son écosystème on voit donc que de proche en proche, le réseau des interdépendances / interconnexions atteint l'échelle Monde.

1.7.2 Notion de puissance

Le cyber-espace dépasse l'échelle technique pour devenir un enjeu de puissance (entre états). Les conflits s'y déplacent, les affrontements s'y multiplient. Pour la défense américaine, le cyber-espace est devenu le cinquième espace de bataille (après la terre, la mer, le ciel et l'espace).

Les États peuvent être évalués selon 4 leviers de puissance :

- les infrastructures télécoms : points d'échange internet, connectivité internationale, data-centres ;
- les capacités scientifiques et technologiques : centres de recherche, brevets ;
- la base industrielle et technologique : industrie du composant (hardware), du logiciel, économies des services et des contenus ;
- le niveau de sécurité et de régulation du réseau, les capacités de cyber-défense.

1.8 Conclusion

Le cyberspace est l'espace des possibles. Cela concerne tout le monde : particuliers, groupes, entreprises, états. On peut d'un simple clic commander une voiture, réserver un billet d'avion...

Mais on peut aussi :

- rançonner une entreprise sans bouger de sa chaise ;
- bloquer le fonctionnement d'un hôpital avec une pièce jointe ;
- perturber le trafic ferroviaire ou aérien à partir d'un smartphone ;
- désactiver à distance un processus industriel.

En 2017, des cyber-attaques massives ont pu avoir lieu et toucher des centaines de milliers de machines connectées de par le monde : WannaCry, NotPetya. Cet effet de propagation est certes dû au caractère auto-répliquant des logiciels utilisés mais aussi et surtout à la densification du cyberspace. Une attaque à l'origine ciblée, peut en réalité déborder de sa cible, se propager de proche en proche (contaminer) par les interactions entre les systèmes. L'attaque NotPetya visant l'Ukraine via l'infection d'un logiciel de comptabilité uniquement connu dans ce pays a pourtant infecté les milliers de machines dans le monde quelques heures plus tard. Cela illustre que l'attaquant ne maîtrise pas les effets domino de ce qu'il déclenche. Ce ne sont que quelques exemples.

1.9 Exercices

1) Le réseau internet a-t-il un propriétaire ?

2) Par rapport à internet, que désigne le terme intranet ? Un serveur intranet est-il un serveur public ?

3) Si des paquets IP vont de la source 192.25.10.5/24 vers le destinataire 191.76.13.25/24 comment est-ce que la machine source sait que le destinataire n'est pas sur le même réseau ? Vers quelle interface envoie-t-elle le paquet ? Quel est le réseau d'appartenance de la source et du destinataire ?

4) Quelle est la différence entre acheminement et transport ?

5) Dans un paquet IP on mentionne l'adresse source et l'adresse destination ? Quelle adresse est utilisée pour le routage ? À quoi sert l'autre adresse ?

6) Si source et destinataire sont sur le même réseau, un routeur est-il nécessaire ?

7) Dans l'URL <https://www.yvert.com/CT-1345-autoadhesifs.aspx>, quelle est la partie utile pour le système DNS ? Combien de domaines apparaissent ? Quel est le domaine le plus haut dans la hiérarchie ? Déclinez les sous-domaines de rattachement. Décomposez les étapes qui aboutissent à la récupération de l'adresse IP de la machine distante.

8) Quelles fonctions réseau sont exécutées dans une box internet ?

9) Un industriel et une PME fournisseur ont leurs SI respectifs inter-connectés, pour quelles raisons ? Comment cela se traduit-il concrètement ? Quels risques potentiels ?

10) Dans un projet de conception d'une nouvelle voiture un constructeur implique différents acteurs de différents corps de métier : lesquels a priori ? Sont-ils tous de la même entreprise ? De quoi ont-ils besoin pour interagir et travailler ensemble ? De quels outils ?

11) En quoi les outils collaboratifs (partage de données, communication) posent-ils des questions relatives à la sécurité ?

12) Le BYOD (*Bring Your Own Device*) désigne le fait que les salariés peuvent utiliser leurs terminaux personnels dans l'espace professionnel et réciproquement. C'est une pratique qui s'est imposée à l'usage et les entreprises ont mis du temps à réagir avant d'essayer de contrôler le phénomène. Citez des exemples. Cette pratique a-t-elle des avantages et pour qui ? A-t-elle des inconvénients en terme de sécurité et lesquels ?

13) Dans un fichier Word, y a-t-il des données personnelles possiblement présentes dans les méta-données ? Lesquelles ?

14) Citez un outil permettant d'éditer les méta-données d'un fichier *.pdf. D'un fichier image (type *.jpg)

- 15) Tous les objets connectés ont-ils besoin d'une adresse IP ?
- 16) Soit un détecteur de monoxyde de carbone dans un appartement (obligatoire). Quel est le capteur ? Quel est l'actionneur ? Dans quel cas cet équipement aurait-il besoin d'être connecté et pourquoi ?
- 17) À partir des objets connectés on peut définir des services logiciels qui ensuite peuvent être composés dans un cadre applicatif plus large. Parmi les fonctions suivantes, lesquelles relèvent d'un service ? D'une application ? a) Relevé de température, b) Régulation par thermostat, c) Détection de présence, d) Gestion de l'énergie, e) Gestion d'ouverture des portes ?
- 18) Questions ouvertes : Le smartphone est-il un objet connecté ? La voiture ? La caméra de vidéo-surveillance ? Le drone ? La chaudière ? Le vélo d'appartement ? Vous-même ?
- 19) Quelles sont les fonctions d'une ville (intelligente) qu'on ne trouve pas dans le monde de l'entreprise ?
- 20) Le GTB (Gestion technique des bâtiments) désigne la gestion technique des bâtiments, réalisée par des prestataires extérieurs, qui utilisent des capteurs et des actionneurs répartis. Dans le cadre d'un immeuble d'entreprise, quelles sont les fonctions élémentaires à gérer ?

Chapitre 2



L'espace des risques

2.1 Qu'est-ce que le risque ?

2.1.1 Définition

Le risque est défini par le triplet (S_i, p_i, D_i) où :

- S_i est un scénario redouté ;
- p_i est la probabilité qu'il survienne ;
- D_i mesure les dommages causés.

Dans le domaine du risque industriel, il y a une notion de danger (et donc de hasard, d'où la mesure par une probabilité).

Le risque se mesure de la façon suivante : $R_i = p_i * D_i$.

On voit que par sa définition, le risque a une structure d'espérance mathématique, celle des dommages causés.

Risque et probabilité sont des mots du langage courant, souvent utilisés de façon confuse. Par ex : risque d'un incendie, risque de tremblement de terre. Ces expressions sont erronées. Le risque ne porte pas sur des événements mais sur le résultat, ce que les assureurs savent bien. S'il n'y a pas de dommage alors il n'y a pas de risque. On devrait dire : risque lié à l'incendie, risque lié à un tremblement de terre, probabilité d'incendie, probabilité de tremblement de terre. Par contre on peut dire : risque d'avoir sa maison détruite. À vrai dire, le résultat est sans doute le même (maison détruite), mais les causes sont différentes. On voit déjà qu'il ne faut pas confondre les causes et les effets car les traitements préventifs pour limiter les risques ne sont pas du tout les mêmes. Dans la formule du risque, les causes sont représentées par le terme p et les effets par D .

2.1.2 Évaluation

On voit d'après la formule du risque que deux termes doivent être évalués : p et D . Dans le domaine industriel le terme p résulte de mesures (statistiques) ou d'estimation (pour les événements rares), de calculs probabilistes, de simulations. Le monde industriel a développé depuis longtemps des méthodes d'analyse de risques, qui ne sont pas l'objet de cet ouvrage. Ce sont des méthodes quantitatives.

L'évaluation des dommages est plus ardue. Elle dépend des systèmes concernés. Plusieurs causes très diverses pouvant aboutir aux mêmes effets, il convient donc d'utiliser des grandeurs sommables. Il en existe deux a priori : le temps et l'argent. Pour la victime ou pour l'assureur, les dommages se mesurent en euros.

Comme on ne peut pas couvrir toutes les causes et donc tous les risques, il est donc important de mesurer l'ensemble des risques pour ensuite pouvoir les hiérarchiser. Idéalement, les événements les plus probables doivent être ceux qui conduisent aux dommages les plus faibles et a contrario les dommages les plus grands doivent être associés aux probabilités les plus faibles, ainsi que le montre la courbe de la figure 2.1, dite courbe iso-risque. Tous les risques évalués au-dessus de cette courbe doivent être traités et réduits.

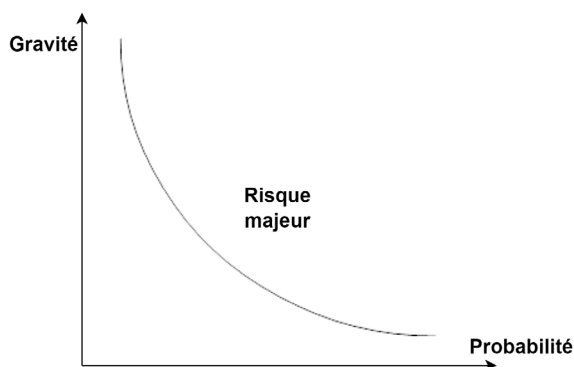


FIGURE 2.1 – Courbe $p * G$

2.1.3 Sûreté de fonctionnement

La sûreté de fonctionnement (SdF) est une discipline qui s'intéresse aux pannes et aux réparation des systèmes. L'événement redouté est ici la panne, soumise aux lois du hasard. L'approche probabiliste est ici la clé pour modéliser le processus panne/réparation. Tous les systèmes technologiques sont concernés et en particulier les systèmes informatiques. Cet aspect sera bien sûr à prendre en compte. Les termes clés (les critères) utilisés dans le monde SdF sont : Fiabilité, Maintenabilité, Disponibilité, Sécurité (critères FMDS).

La sécurité fonctionnelle (*safety*) est un sous-ensemble de la SdF.

Attention à ce terme ! Dans le domaine industriel, la sécurité est liée à la notion d'accident et la sûreté est liée à la malveillance tandis que la qualité est associée à l'erreur (humaine, procédurale). Dans le domaine informatique, la sécurité est associée à la malveillance tandis que la sûreté (*safety*) désigne l'accident, qui peut être la conséquence d'un incident de sécurité (cyber-attaque), c'est-à-dire une atteinte aux biens et aux personnes. Nous reviendrons sur ce point.

2.2 Qu'est-ce que le cyber-risque ?

2.2.1 Risque *vs* cyber-risque

Au niveau de l'entreprise en général (pas forcément industrielle), le risque global est multi-factoriel. On parle généralement de risque :

- financier ;
- technologique ;
- juridique ;
- social ;
- environnemental ;
- sûreté.

Par rapport au risque global d'une entreprise, le risque cyber est une nouvelle composante, comme le montre la figure 2.2. Cette composante n'est pas indépendante des autres, à vrai dire, elle les impacte presque toutes. Dans le domaine industriel (Seveso notamment) même le risque environnemental peut être la conséquence d'un incident de cybersécurité. Les technologies numériques ont aujourd'hui un effet structurant sur tous les processus et toutes les activités de l'entreprise. Toute atteinte au système d'information, en particulier sur les données, a par conséquent un impact potentiel sur toutes les activités qu'il alimente. Le risque sûreté dépasse le seul périmètre des données, car des données falsifiées, indisponibles ont un impact sur les processus cyber-physiques, ce qui à grande échelle peut porter créer un problème de sécurité globale.

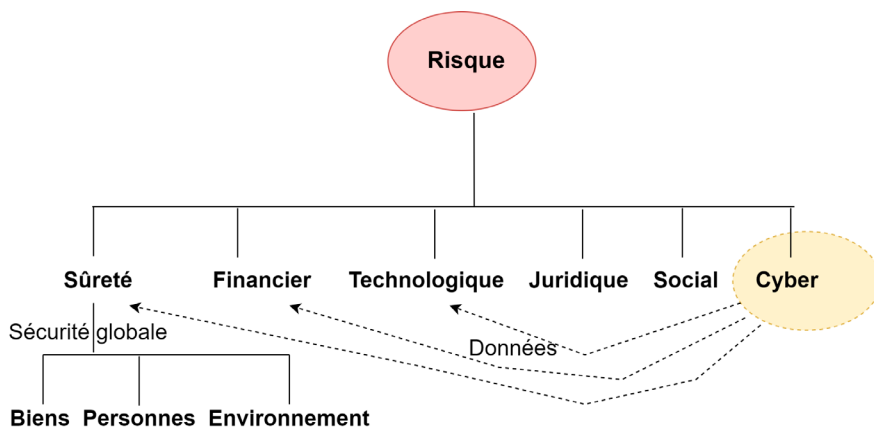


FIGURE 2.2 – Risque cyber

2.2.2 Typologie du risque "cyber"

Le risque " cyber " ou cyber-risque peut faire l'objet d'une typologie liée à la nature du risque lui-même, c'est-à-dire à l'origine des incidents :

- R1) malveillante (les cyber-attaques) ;
- R2) technologique : lié à la fiabilité des technologies, la défaillance matérielle ou logicielle ;
- R3) physique : endommagement, destruction (accident, incendie, inondation, séisme) ;
- R4) organisationnelle / humaine : mauvaises pratiques, maladresses, absence de prise en compte du danger, baisse de vigilance, défaut de veille, etc.

Le risque R1 caractérise la cyber-sécurité : ici le danger est dû à la malveillance. Attention, celle-ci peut être externe mais aussi interne.

Le risque R2 relève de la sûreté de fonctionnement (risque fonctionnel). Tout système technologique est soumis à des aléas de panne. Cela concerne le poste de travail, les serveurs (disque dur par ex.), la conséquence est ici la perte de données. Cela peut concerner un équipement réseau, mais aussi l'accès à internet chez le fournisseur d'accès. Le risque est ici celui de l'interruption de service.

Le risque R3 relève de la sûreté (risque accidentel) : le système informatique peut être endommagé par un dégât des eaux, un incendie.

Le risque R4 relève plus des procédures qualité. L'erreur humaine peut conduire à des dommages : perte de fichier, erreur de manipulation, mauvais paramétrage, mauvaise perception, mauvaises décisions... Le risque est ici la perte ou la corruption de données.

2.2.3 Risque sur les données

Certaines causes peuvent avoir les mêmes effets. La panne d'un disque dur ou le vol malveillant conduisent au même résultat : les données sont perdues. Ce que résume la figure 2.3.

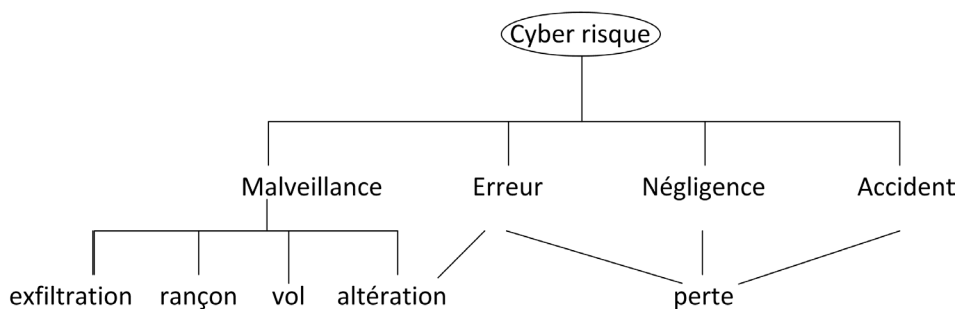


FIGURE 2.3 – Risque sur les données

2.2.4 Critères DICP

Le monde de la sûreté de fonctionnement utilise les critères FMDS (voir plus haut). Dans le monde de la cyber-sécurité, on utilise les critères DICP (Disponibi-

lité, Intégrité, Confidentialité, Preuve). La disponibilité est le seul terme en commun entre le monde de la sûreté de fonctionnement et celui de la cyber-sécurité.

Disponibilité

La disponibilité s'applique essentiellement aux données, qui alimentent les activités et donc des processus : elles doivent être disponibles quand on en a besoin. Mais pour accéder aux données il faut accéder à la ressource qui la détient. La disponibilité peut s'appliquer à la ressource système (le serveur) mais aussi à un service (accès à internet par ex.).

La disponibilité d'une ressource ou d'un service peut se mesurer par un indicateur A (pour *availability*). $A = MTBF / (MTBF + MTTR)$ où :

- $MTBF$: *Mean Time Before Fail* ou temps moyen de bon fonctionnement ;
- $MTTR$: *Mean Time To Repair* ou temps moyen pour remettre le système en état.

C'est donc un indicateur statistique facile à maintenir dans le temps (par ex. chaque année) en tenant à jour le journal des incidents ayant conduit à des interruptions (par ex. l'accès à internet fourni par un opérateur). Il est exprimé en pourcentage.

Intégrité

La donnée ne doit pas avoir été altérée ou détruite par autrui non autorisé. Le **hachage** permet d'assurer l'intégrité. Le principe est de calculer un condensat (empreinte numérique) de taille fixe à partir d'un fichier F de taille quelconque. Le condensat (ou hash) $H = h(F, k)$ où :

- H : condensat ;
- F : fichier ;
- k : clé de chiffrement possible si on utilise un algorithme à clé ;
- h : algorithme de hachage, souvent dérivé d'un algorithme de chiffrement (d'où l'utilisation d'une clé).

Confidentialité

La donnée ne doit être accessible qu'aux personnes autorisées. Le **chiffrement** permet d'assurer la confidentialité. $X = f(C, k)$ où :

- X : chiffré ;
- C : clair ;
- k : clé de chiffrement ;
- f : algorithme de chiffrement.

Preuve

Elle doit permettre de retrouver les circonstances d'un changement d'état de la donnée, ce qui implique :

- la traçabilité des actions ;
- l'authentification des utilisateurs ;
- l'imputabilité du responsable de l'action.

Ceci peut s'avérer pertinent vis-à-vis de certaines données sensibles avec accès multi-utilisateurs : un dossier médical par ex.

2.2.5 Risque sur le système

Le principal risque qui concerne le système est l'atteinte à la disponibilité. L'atteinte à la disponibilité a pour but d'empêcher le système de fonctionner, généralement en saturant ses ressources : bande passante du réseau, capacité d'un serveur, ou bien en le faisant dysfonctionner (via un message erroné). C'est ce qu'on appelle une attaque de **déni de service (DoS)**. Nous y reviendrons.

2.2.6 Risque "sûreté" (*safety*)

Cela concerne les risques sur les biens et les personnes. Comment les mettre en danger à partir d'un cyber-incident ? En perturbant les données de contrôle des processus cyber-physiques (rupture d'intégrité" sur les données transmises), cela peut provoquer un effet domino entre monde logique (qui contrôle) et monde physique (contrôlé). Cela peut être causé par une cyber-attaque.

Par exemple en 2014, une usine métallurgique allemande a été sévèrement endommagée, à partir d'un mail et d'une simple pièce jointe.

Cela peut aussi être dû à un accident initial. Un réacteur de la centrale de Fukushima au Japon a explosé parce que les serveurs de contrôle se sont retrouvés noyés sous les eaux suite à un tsunami, causé par un tremblement de terre au large. On a ici un double effet domino physique->logique->physique : un accident (tremblement de terre au large, tsunami) cause un cyber-incident (sur le système de contrôle) ce qui provoque à son tour un autre accident (explosion, pollution radioactive de l'air et de l'eau).

2.2.7 Malveillance : de la menace aux dommages

Dans la formule du risque, le terme p peut être explicité comme le produit de 5 termes :

- p_1 : probabilité que le système soit menacé ;
- p_2 : probabilité d'une action malveillante sachant que le système est menacé ;
- p_3 : probabilité qu'une vulnérabilité (ou faille) soit exploitée sachant que le système est attaqué ;
- p_4 : probabilité que la cible soit atteinte sachant qu'une vulnérabilité a été exploitée ;

- p_5 : probabilité que des dommages soient causés sachant que la cible a été atteinte.

Ceci est résumé dans la figure 2.4.

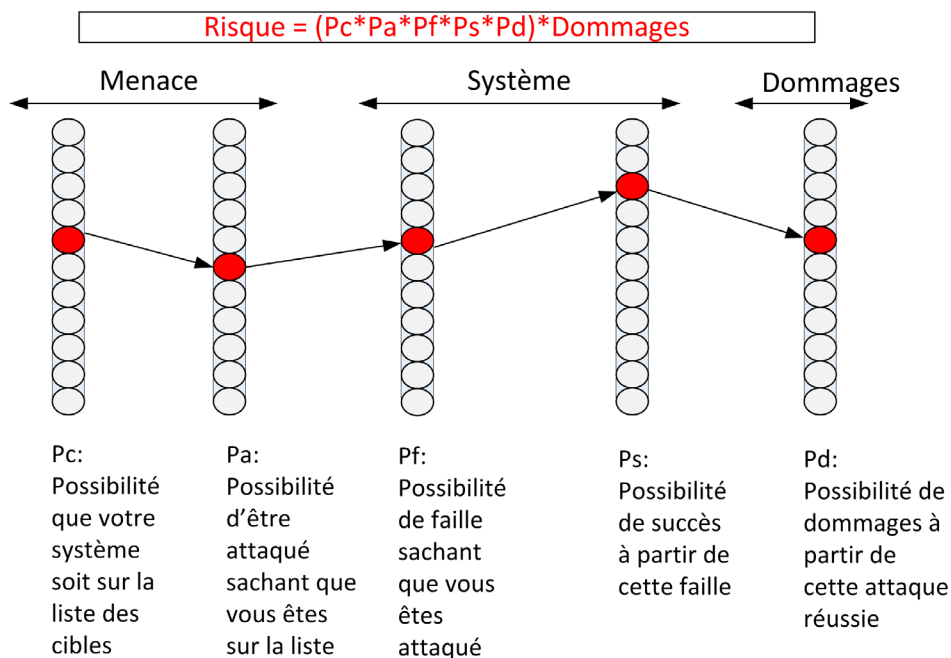


FIGURE 2.4 – De la menace aux dommages

On passe donc de la menace potentielle à une menace qui passe à l'acte (attaque) et qui exploite une ou plusieurs vulnérabilités pour ensuite atteindre sa cible et causer des dommages. Entre le danger et les dommages causés, on a un filtre à 5 couches.

Les questions qui se posent sont alors : comment réduire le risque ? Sur quoi peut-on agir ? Comme le montre la figure 2.4, le périmètre du responsable de la sécurité du système concerne les termes p_3 , p_4 et p_5 . Son rôle est de réduire chacun de ces termes.

Les termes p_1 et p_2 caractérisent le niveau de danger. Un responsable sécurité n'a pas la possibilité de réduire la menace. Par contre il peut essayer d'en savoir plus sur elle : qui sont les attaquants potentiels, leurs motivations, leurs moyens d'actions habituels, leurs outils ? C'est ce qu'on appelle l'intelligence de la menace (*Threat Intelligence*), activité assez récente et qui s'apparente au renseignement. À partir d'informations exploitables il est alors possible aux responsables sécurité de prendre des mesures préventives, de mettre en place des moyens de défense plus adaptés au profil de cette menace.

Le terme p_3 caractérise à la fois la porosité du système (en terme de sécurité) et l'habileté de l'attaquant à l'exploiter. Réduire p_3 consiste d'abord à identifier les vulnérabilités et à les réduire.

Le terme p_4 caractérise la possibilité pour l'attaquant à atteindre sa cible, une fois l'intrusion réalisée. Cette cible correspond généralement aux actifs du système : serveurs de données sensibles, processus clés. Réduire p_4 peut se faire en identifiant et en réduisant les chemins d'attaques à l'intérieur du système, et aussi à mettre en place un système de détection, capable de générer une alerte, d'assurer la traçabilité de l'incident en cours.

Le terme p_5 mesure l'impact de l'attaque en terme de dégâts causés : pertes de données, serveurs indisponibles, processus bloqués, dommages matériels et personnels. Réduire p_5 suppose d'avoir une procédure de gestion des incidents qui soit réactive, efficace, c'est-à-dire capable de prendre les contre-mesures pertinentes, d'assurer le retour à la normale rapidement.

2.2.8 Termes clés

Les termes clés sont ici les suivants : menace, attaque, vecteur d'attaque, cible, vulnérabilités, dommages. On peut les situer sur la figure 2.5.

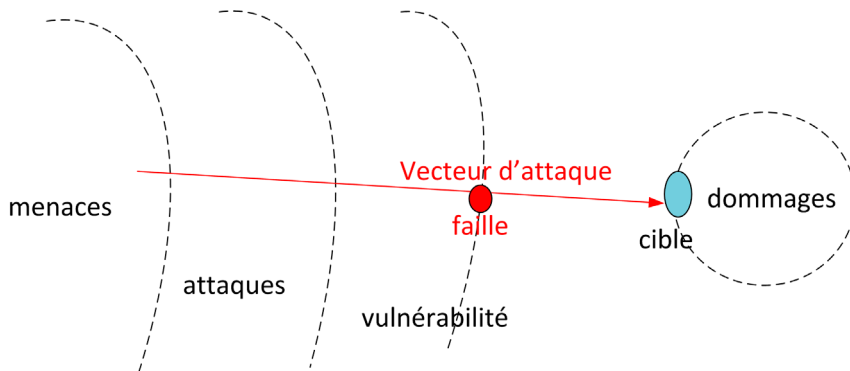


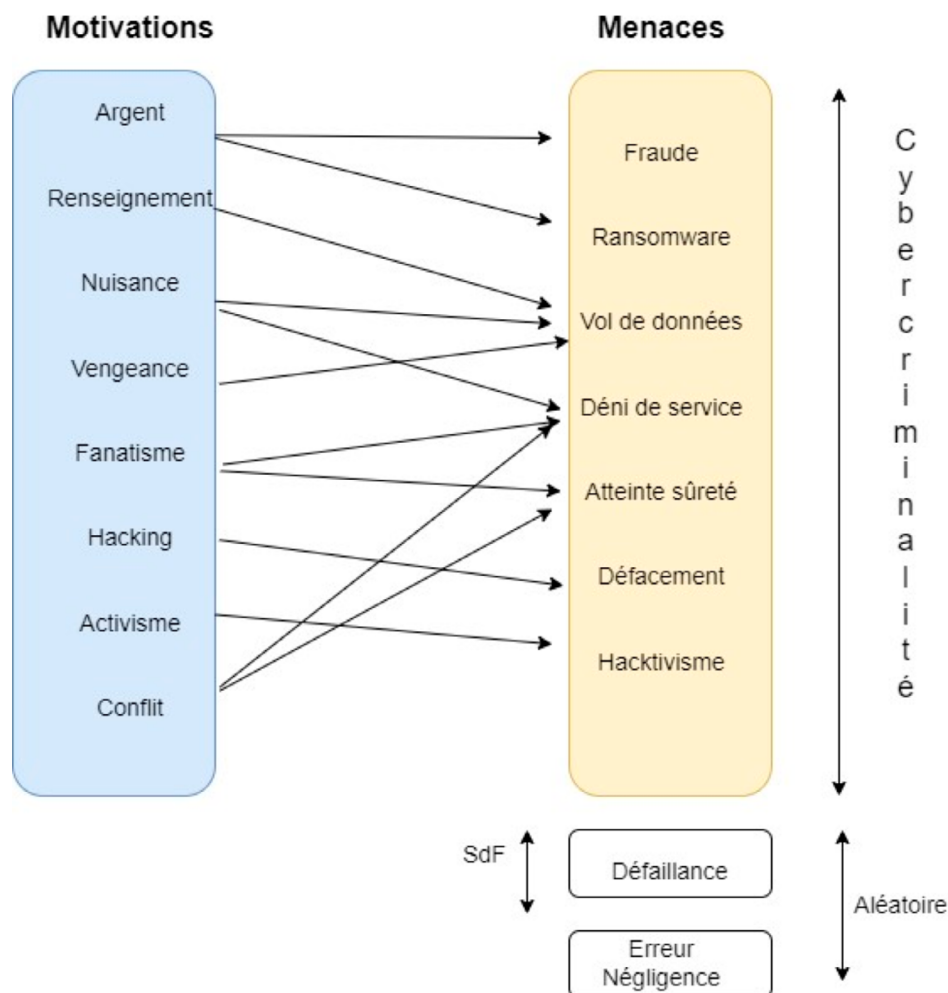
FIGURE 2.5 – Termes clés

2.3 Caractérisation du danger

2.3.1 La menace

La menace correspond ici à la malveillance potentielle. C'est l'équivalent du danger dans le monde industriel, sauf que la malveillance n'est pas caractérisée par le hasard, mais plutôt par la motivation. La figure 2.6 essaye ainsi de relier menace et motivation (s). Cette figure est assez généraliste et les motivations ne sont pas pondérées, ce qu'il faudrait faire pour tenir compte du type d'entreprise ou d'activité. Par exemple une entreprise de e-commerce ne suscite pas les mêmes motivations qu'une administration ou une PME industrielle.

L'argent est la motivation la plus importante, ce qui concerne tout le monde. Elle peut être assouvie de façon directe (fraude, rançongiciel), mais aussi indirecte (vol de données, certaines données ont une valeur marchande).

FIGURE 2.6 – Menaces *vs* motivations

D'autres menaces doivent néanmoins être citées.

Les situations géopolitiques tendues, le terrorisme, peuvent potentiellement générer des attaques de grande ampleur contre des systèmes administratifs, des systèmes d'importance vitale, à des fins de blocage (déni de service) voire de destruction. Les cibles potentielles sont connues (ministères, opérateurs d'importance vitale) et ces attaques sont souvent conduites par des groupes de cyber-activistes, nationalistes, avec des compétences de niveau élevé et des moyens financiers fournis par des états.

L'hacktivisme désigne les activités de groupes de cyber-activistes qui ciblent des entreprises qui ne correspondent pas à leurs valeurs. Cela peut concerner le domaine nucléaire, pétrolier, bancaire, certains grands groupes... La motivation première est ici de nuire à la réputation des entreprises, souvent en publiant des données confidentielles.

La menace interne a pour motivation la vengeance personnelle. Cela concerne potentiellement toutes les entreprises. Des salariés (mais aussi des sous-traitants, des partenaires) mécontents peuvent user de leurs droits internes, même limités dans le temps, de leur connaissance de l'entreprise pour conduire des actions malveillantes. C'est un sujet connu (de nombreux cyber-incidents ont révélé ce problème), complexe (à anticiper, à traiter), protéiforme (vol, destruction, bombes logiques à retardement, atteinte à l'image de l'entreprise...) Par rapport à la figure 2.6, l'étape supplémentaire est d'associer les menaces aux cibles. On voit figure 2.7 que les serveurs en général constituent la cible la plus fréquente. Le réseau est une cible dès lors qu'on cherche à rendre indisponible les services ou qu'on cherche à dégrader les temps de réponse de ce réseau dans le cas de processus critiques avec des contraintes de temps sévères.

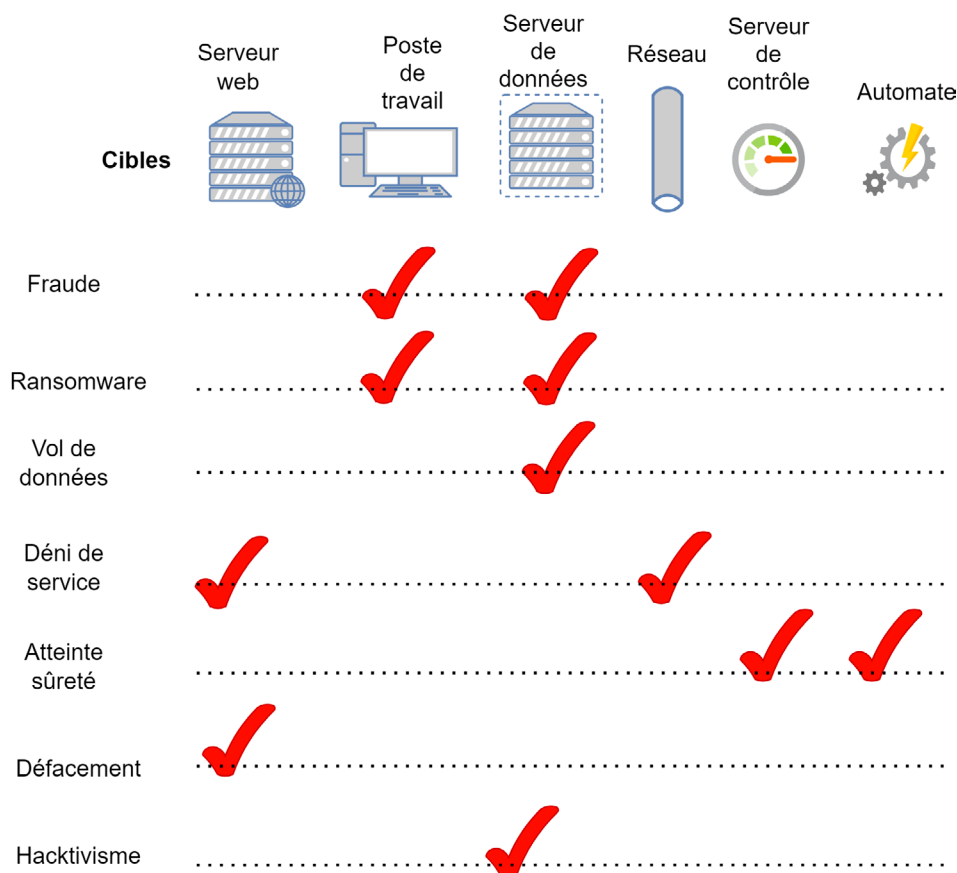


FIGURE 2.7 – Cibles *vs* menaces

2.3.2 Attaque

L'attaque désigne le passage à l'acte de la menace, les actions pour porter atteinte à la sécurité : des données, des services, des biens, des personnes.

Une attaque peut être longue quand elle s'inscrit dans la durée (exfiltration de données, cyber-espionnage), ce qui implique qu'elle ait été conçue pour rester furtive, c'est-à-dire non détectable, que ce soit par l'utilisateur ou par le système de surveillance (quand il existe).

2.3.3 Vecteur d'attaque

Il désigne le point d'entrée d'une attaque, exploitant une faille ou une vulnérabilité. Cela peut être l'utilisation d'une clé usb pour introduire un malware (en interne), l'envoi d'une **pièce jointe** frauduleuse associée à un courriel, l'envoi d'un courriel comportant un lien URL actif, associé à des techniques d'**ingénierie sociale** pour rédiger un message qui inspire confiance et incite à activer le lien.

La figure 2.8 présente des vecteurs d'attaques classiques.

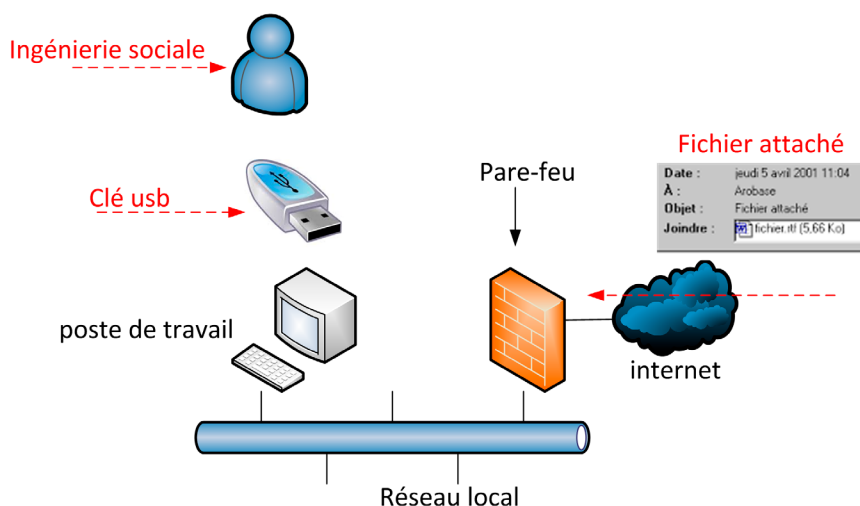


FIGURE 2.8 – Exemples de vecteurs d'attaques

L'**hameçonnage** (ou *phishing*) consiste à exploiter le maillon faible qu'est l'être humain en abaissant son niveau de vigilance pour lui soumettre un faux courrier, une page web infectée, dont le but est d'induire de sa part une action, susceptible ensuite de fournir des données exploitables (identifiants, comptes bancaires...) ou de déclencher une action. La figure 2.9 illustre le principe de l'hameçonnage.

On peut mentionner ici la technique du **point d'eau** qui consiste à infecter un site web couramment utilisé par l'entreprise ou par un usager de celle-ci. La connexion à ce site peut conduire l'utilisateur à télécharger un malware à son insu et ainsi l'introduire dans le système.

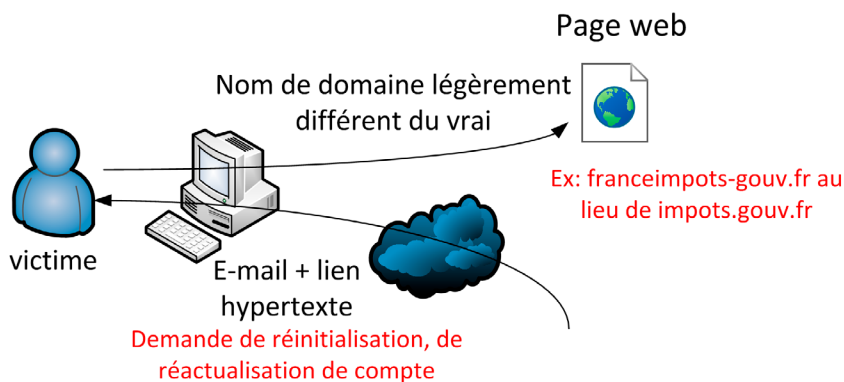


FIGURE 2.9 – Principes de l’hameçonnage (*phishing*)

2.3.4 Scénarios d’attaque

Le scénario représente la stratégie de l’attaquant pour atteindre son but, ce qui suppose plusieurs étapes pour mener une attaque à son terme. À chaque étape, les techniques peuvent varier, notamment pour que l’attaque reste non détectable. Un scénario peut se dérouler sur le temps long (des semaines, des mois).

2.3.5 La matrice MITRE ATT&CK

MITRE est une organisation américaine à but non lucratif (créée en 1958), intervenant dans le domaine de l’ingénierie des systèmes et les technologies de l’information. Elle a constitué une base de connaissances permettant de cartographier les divers types de **tactiques, techniques et procédures (TTP)** utilisées par les attaquants [8]. Le résultat est connu sous le nom de matrice MITRE ATT&CK (*Adversarial Tactics, Techniques and Common Knowledge*). C’est plus un tableau qu’une matrice. Il constitue un référentiel incontournable aujourd’hui pour modéliser les cyber-attaques. Cette matrice recense 14 tactiques connues et pour chacune l’ensemble des techniques utilisées, chacune référencée par un identifiant. Pour chacune de ces techniques, des contre-mesures sont proposées, avec là aussi pour chacune un identifiant. Sans entrer dans les détails techniques, il paraît important de présenter ici les 14 tactiques recensées.

Précisons que tout scénario d’attaque comporte un sous-ensemble de ces 14 tactiques (au moins les premières), correspondant au déroulement de son scénario propre, de la phase de compromission du système jusqu’à la cible finale.

T1-Reconnaissance

L’adversaire essaye de rassembler des informations qu’il pourra utiliser pour planifier des opérations futures.

Ces informations peuvent inclure des détails sur l’organisation, l’infrastructure ou les personnes. Il peut ainsi utiliser tous les moyens de recherche en **source**

ouverte, c'est-à-dire accessibles dans l'espace public : notamment les sites web où figurent des informations utiles, le système DNS pour obtenir des adresses IP. Ces informations pourront être exploitées dans les phases ultérieures.

Exemple de technique : la collecte d'informations sur les machines du système (T1592).

T2-Développement de ressources

Techniques qui impliquent que des adversaires créent, achètent ou compromettent ou volent des ressources qui peuvent être utilisées contre la cible. Elles peuvent être exploitées pour aider dans les phases ultérieures de l'attaque (utilisation de domaines achetés (T12 - Commande et contrôle), de comptes de messagerie pour le hameçonnage (*phishing*) (T3 Accès initial), le vol de certificats de signature (T7 - Furtivité). Ces ressources incluent de l'infrastructure, des comptes ou des capacités.

Exemple : la compromission de comptes existants (T1586).

T3-Accès initial

Ensemble de techniques qui utilisent divers vecteurs d'entrée pour s'implanter au sein d'un réseau. Cela comprend le hameçonnage ciblé, l'exploitation de vulnérabilités de serveurs Web publics. Les positions acquises grâce à l'accès initial peuvent permettre un accès continu (comptes valides, utilisation de services distants) ou à usage limité en raison de la modification des mots de passe.

Exemple de technique : l'hameçonnage (T1566)

T4-Exécution

Techniques qui entraînent l'exécution d'un code logiciel contrôlé par l'adversaire sur un système local ou distant. Souvent associées à des techniques référencées dans d'autres phases tactiques pour atteindre des objectifs plus larges (exploration du réseau, vol de données).

Exemple : utilisation d'un logiciel interpréteur des commandes tapées au clavier (T1059)

T5-Persistance

Techniques utilisées pour conserver l'accès au système malgré les redémarrages, les modifications d'informations d'identification et d'autres interruptions susceptibles de couper leur accès. Les techniques utilisées incluent tous les changements d'accès, d'action ou de configuration qui permettent de conserver l'emprise sur les systèmes, comme le remplacement ou le détournement de code légitime ou l'ajout de code de démarrage.

Exemple : Manipulation de compte (T1098)

T6-Escalade de privilèges

Techniques utilisées pour obtenir des autorisations de niveau supérieur sur un système ou un réseau (Niveau "root", administrateur local, compte utilisateur avec accès de type administrateur, comptes d'utilisateurs avec accès à un système spécifique ou exécutant une fonction spécifique). Les approches courantes consistent à tirer parti des faiblesses, des erreurs de configuration et des vulnérabilités du système.

Exemple : Utilisation abusive des mécanismes de contrôle des privilèges (T1548).

T7-Furtivité

Techniques permettant d'éviter d'être détecté tout au long de la compromission. Elles incluent la dés-installation ou dés-activation de logiciels de sécurité, le chiffrement des données et des scripts.

Les attaquants exploitent et abusent également des processus de confiance pour masquer et masquer leurs logiciels malveillants.

Exemple : modification de la politique de gestion de domaines dans le logiciel Active Directory de Microsoft (T1484). Ce logiciel est très couramment utilisé en entreprise pour gérer les comptes et les droits.

T8-Accès aux informations d'identification

Techniques permettant de voler des informations d'identification telles que des noms de compte et des mots de passe. Elles incluent le traçage des touches frappées au clavier (*keylogging*) ou la copie en mémoire des informations d'identification. L'utilisation d'informations d'identification légitimes peut permettre ensuite d'accéder aux systèmes, de les rendre plus difficiles à détecter et offrir la possibilité de créer davantage de comptes pour atteindre leurs objectifs.

Exemple : test par brute-forçage de toutes les combinaisons d'un mot de passe ou d'un identifiant (T1110).

T9-Découverte de l'environnement

Techniques pour acquérir des connaissances sur le système et le réseau interne, pour observer l'environnement, aider à s'orienter avant de décider comment agir. Permettent aussi aux adversaires d'explorer ce qu'ils peuvent contrôler et ce qui se trouve autour de leur point d'entrée afin de découvrir comment cela pourrait profiter à leur objectif actuel. Les outils de l'OS natif sont souvent utilisés pour atteindre cet objectif de collecte d'information après compromission.

Exemple : Découverte des comptes, comptes locaux, domaine, messagerie, compte cloud (T1087).

T10-Mouvement latéral

Techniques utilisées pour entrer et contrôler des systèmes distants sur un réseau. Poursuivre l'objectif principal nécessite souvent d'explorer le réseau pour trouver la cible et ensuite y accéder. Cela implique souvent de passer par plusieurs

systèmes et comptes. Les adversaires peuvent installer leurs propres outils d'accès à distance pour effectuer un mouvement latéral ou utiliser des informations d'identification légitimes avec des outils de réseau et de système d'exploitation natif, ce qui peut être plus furtif.

Exemple : Exploitation de services distants pour obtenir des accès non autorisés une fois introduit dans le réseau (T1210).

T11-Collecte

Techniques pour recueillir des informations à partir de sources cibles jugées pertinentes. Souvent, le prochain objectif après la collecte de données est de voler (exfiltrer) les données. Les sources cibles courantes incluent divers types de lecteurs, navigateurs, fichiers audio, vidéo et e-mail. Les méthodes courantes de collecte incluent la capture d'écran et la saisie au clavier.

Exemple : capture de flux audio (T1123).

T12-Commande et contrôle (C&C ou C2)

Techniques que les adversaires peuvent utiliser pour communiquer avec les systèmes sous leur contrôle au sein d'un réseau victime. Le but est généralement d'imiter le trafic normal attendu pour éviter la détection. Il existe de nombreuses techniques avec différents niveaux de furtivité en fonction de la structure du réseau et des défenses de la victime.

Exemple : Utilisation de services réseau comme le DNS, la messagerie, le web, le transfert de fichier, dont les protocoles ne sont jamais filtrés. (T1071).

T13-Exfiltration

Techniques que des adversaires peuvent utiliser pour voler des données sensibles à partir du réseau cible. Une fois les données collectées, elles sont re-conditionnées pour éviter d'être détectés (compressées, chiffrées). Elles sont exfiltrées via un canal C2 ou un autre canal.

Exemple : Exfiltration automatisée (T1020).

T14-Impact

Techniques pour manipuler, interrompre voire détruire le système et/ou les données. Les techniques utilisées peuvent aboutir à des destructions de comptes, destruction/ falsification de données. Dans certains cas, les processus métier peuvent sembler corrects, mais peuvent avoir été modifiés au profit des objectifs adverses. Exemple : chiffrage de données (T1486).

Intérêt de la matrice MITRE ATT&CK

L'intérêt premier est de constituer une base de connaissances, multi-environnements (Windows, Linux, MacOS, Saas), multi-sources d'information.

Le second intérêt est de proposer des contre-mesures pour chacune des techniques recensées.

Le troisième intérêt est de constituer un modèle de référence, pour modéliser les attaques, définir des signatures d'attaques, pour effectuer des simulations, pour aider à faire des analyses de vulnérabilités, pour élaborer des stratégies de sécurité.

2.3.6 Attaques de déni de service

L'objectif de l'attaquant est de saturer les ressources du système informatique pour attenter à la disponibilité de ces ressources :

- bande passante du réseau, disponibilité d'un serveur : l'attaquant génère un trafic vers sa cible de manière à saturer ses capacités de traitement et donc à rendre les temps d'accès hors limite ;
- épuisement de l'espace adressage d'un serveur DHCP qui fournit à la demande des adresses IP dynamiques, tant qu'il en reste disponibles.

On peut aussi générer des dysfonctionnements au niveau applicatif ou niveau du système d'exploitation (paquets mal formés pour faire rebooter une machine), requêtes http non terminées, ce qui est plus rare aujourd'hui car nombre de correctifs logiciels ont été apportés depuis longtemps pour éviter ce type d'incident. Autre variante : le chiffrement de données par un *wiper*, ce qui a été le cas de l'attaque NotPetya en 2017 (chiffrement sans contre-mesure prévue). Un disque dur chiffré devient de fait inexploitable.

La figure 2.10 résume les différents modes d'action du déni de service.

Les attaques de déni de service visent surtout les serveurs web publics et les infrastructures des opérateurs de cloud.

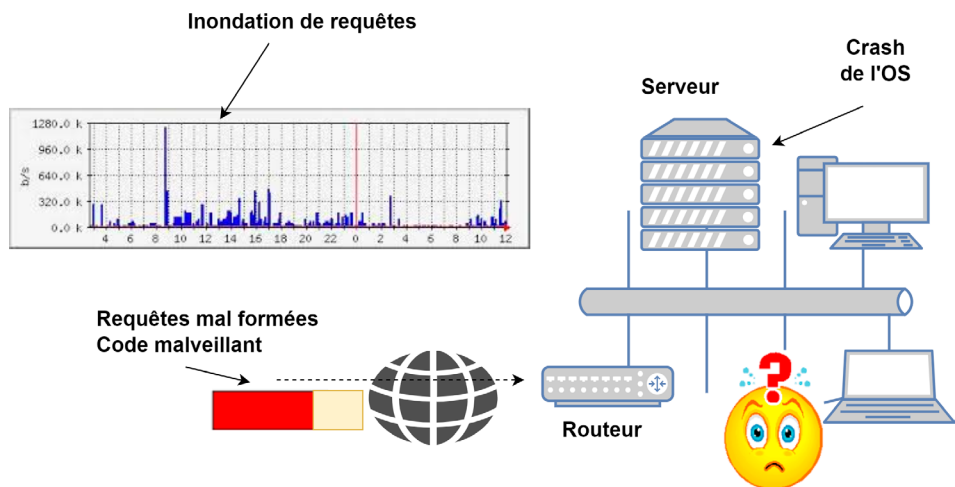


FIGURE 2.10 – Attaque DoS

La puissance d'une attaque DoS repose sur la capacité à générer un trafic de saturation pour épuiser la bande passante vers une cible donnée. Cette puissance se mesure en débit : bits/s ou nombre de requêtes /s. Le but est donc de générer rapidement et massivement un débit élevé. Les techniques pour y arriver reposent

sur un mécanisme d'amplification comme le montre la figure 2.11. Elle consiste à infecter des milliers de machines (appelées bot) qui vont générer (à leur insu) de façon coordonnée un trafic vers une même cible. C'est le principe des attaques par botnet.

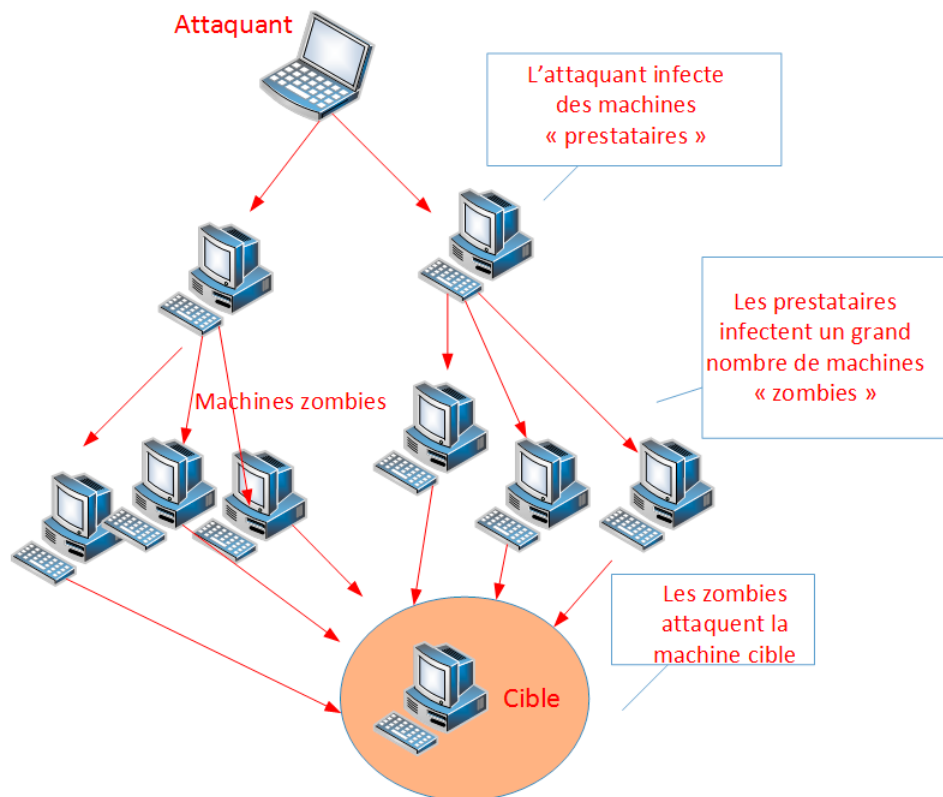


FIGURE 2.11 – Attaque de type botnet

Les protocoles de l'internet présentent à la base des vulnérabilités qui peuvent être exploitées. L'avantage de ces protocoles est qu'ils sont indispensables au bon fonctionnement du système et donc impossible à filtrer ou à bloquer sur la base de leur numéro de port (UDP ou TCP) : DNS, http, NTP (*Network Time Protocol*, protocole de synchronisation des horloges). Le principe repose sur le fait qu'une requête a un format limité en taille mais que les réponses aux requêtes peuvent être beaucoup plus longues. Si on arrive à détourner le trafic des réponses vers une même cible alors on met en place un mécanisme d'attaque par réflexion/amplification. Les possibilités diffèrent selon le protocole utilisé. La figure 2.12 en résume le principe.

Dans cette figure on voit qu'une simple ligne de commande suffit à l'attaquant *A* pour générer une requête vers une machine relais *B* en falsifiant l'adresse de la source qui ici n'est pas *A* mais la cible *V*. *B* génère alors automatiquement une réponse vers *V*.

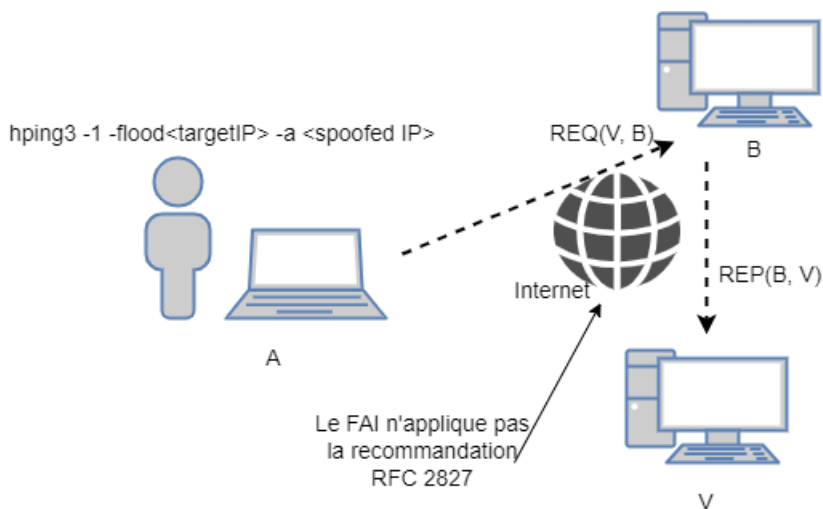


FIGURE 2.12 – Attaque par réflexion/ amplification

Rappelons que le trafic généré par une réponse est supérieur à celui d'une requête, parfois beaucoup plus, ce qui se mesure par un facteur d'amplification. Les facteurs d'amplification qu'on peut atteindre avec les protocoles usuels sont (en théorie) :

- DNS (UDP 53) : 179 ;
- NTP (UDP 123) : 556 ;
- CLDAP (UDP 389 ; protocole d'accès "léger" aux annuaires LDAP) : 70 ;
- Memcached (UDP 11211, système distribué de mise en cache des données) : 51200.

On voit qu'un mécanisme de réflexion / amplification combiné à un mécanisme d'attaque distribuée (type botnet), on peut générer un trafic résultant très important vers une cible donnée. Les débits des attaques DoS utilisant ces mécanismes peuvent atteindre :

- DNS : 1 Gbps ;
- NTP : 400 Gbps ;
- CLDAP : 24 Gbps ;
- Memcached : au-delà de 1 Tbps (1.6 Tbps atteints lors de l'attaque contre OVH en 2018).

Récemment une nouvelle technique est apparue, dite de réinitialisation rapide. L'attaque DDoS sur Google Cloud en 2023 a atteint le record de 398 millions de requêtes par seconde. En 2022 Cloudflare et AWS avaient également été ciblés par des attaques semblables, de respectivement 201 millions et 155 millions de requêtes par seconde.

2.3.7 Le malware

Le terme malware désigne un logiciel (ou code) malveillant. C'est un terme très général qui ne précise pas ce qu'il est censé faire. Ils sont conçus pour être résidents (actif en mémoire de façon permanente), furtifs (à l'insu de l'utilisateur), persistants (capables de se relancer après extinction ou de se réinstaller en cas de désinstallation). Les malwares dits APT (*Advanced Persistent Threat*) sont conçus pour fonctionner dans la durée de manière furtive, souvent pour exfiltrer des données. Leur détection est difficile et nécessite souvent des algorithmes de traitement des signaux faibles par les technologies du big data. Le traitement de ce type d'incident est long et complexe.

Le vecteur d'intrusion d'un malware est la clé usb (en interne), la pièce jointe d'un message, la technique du point d'eau.

Le malware relève des techniques les plus avancées de l'ingénierie logicielle. Il est important de préciser ici que les concepteurs de malwares ne sont plus ceux qui les exploitent. Un malware peut être loué, acheté, fourni à quiconque avec service après vente, comme n'importe quel outil logiciel du commerce.

La figure 2.13 présente une typologie fonction de son mode de fonctionnement.

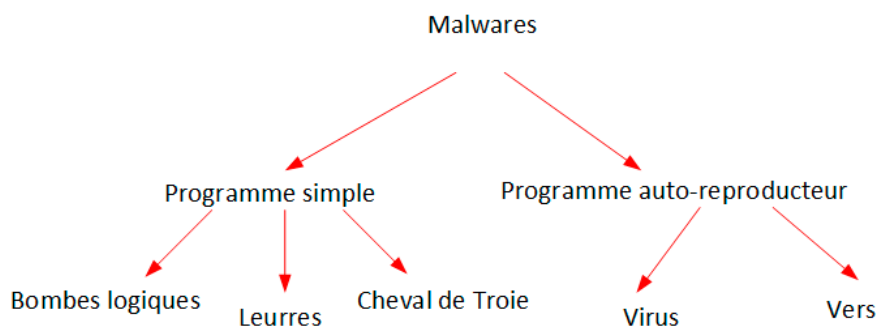


FIGURE 2.13 – Types de malwares

Bombe logique

La bombe logique attend un événement pour s'exécuter (date, action, donnée).

Cheval de Troie

Le cheval de Troie est un malware qui fonctionne en mode client (extérieur) et serveur (introduit dans le système, ayant accès aux ressources internes).

Virus

Le virus désigne un code malveillant auto-reproducteur, qui nécessite l'action d'un utilisateur (ex. frappe au clavier). Il est capable d'être furtif et de muter.

Ver

Le ver n'infecte pas les fichiers mais il réside en mémoire vive (RAM) de la machine où il se trouve et il est capable de se répliquer en utilisant les canaux de communication disponibles. Suite à son introduction dans le système, son fonctionnement et son évolution ne sont plus liés à l'action de l'utilisateur.

Rootkit

Le *rootkit* désigne un malware conçu pour infecter une machine, installer une boîte à outils permettant par ex. d'enregistrer des frappes au clavier, de capturer des mots de passe, de voler des comptes, de communiquer avec l'extérieur, d'accéder à une machine cible... Il a des chances d'être furtif s'il se fait passer pour un logiciel légitime.

Certains malwares sont conçus pour attaquer une cible précise et nécessitent une ingénierie de haut niveau, de mois de développement et de mise au point comme le malware Stuxnet en 2010, assimilable à un vers, conçu à un niveau étatique pour détruire les centrifugeuses d'enrichissement d'uranium du site de Natanz en Iran. Il a vraisemblablement été introduit par une clé usb. Par rapport au référentiel MITRE, toutes les tactiques étaient exécutées sauf (a priori) T13 (exfiltration).

En matière d'ingénierie, il est à prévoir que des malwares intègrent des techniques d'intelligence artificielle comme l'apprentissage automatique, lui permettant d'être autonome pour analyser le contexte où il se trouve et ainsi adapter son fonctionnement. Néanmoins le malware se doit d'avoir une taille limitée et ne peut pas déployer en local des techniques d'IA. Cela nécessitera certainement le recours à un serveur extérieur via un canal de type Control and Command (C2), serveur qui lui aura la capacité de traitement afin d'optimiser la stratégie du malware et de lui retourner les outils adaptés par le même canal.

2.3.8 Cas particulier des rançongiciels (*ransomware*)

Quelques exemples

C'est sans doute le type d'attaque de malware le plus connu aujourd'hui, en forte augmentation depuis 2018. Il en existe plusieurs : Ryuk, Maze, Egregor, Netwalker, Sidinobiki... À chaque rançongiciel est associé une infrastructure et un des groupes criminels qui l'exploitent. Le rançongiciel Emotet, à la base un cheval de Troie, a sévi pendant des années avant d'être démantelé (acteurs, infrastructure) début 2021 grâce à une coopération internationale. Cela correspond à des centaines de serveurs de par le monde.

Principe

Le principe du rançongiciel est de chiffrer des données pour les rendre indisponibles, de demander une rançon pour permettre à la victime de les déchiffrer. Un

double chantage peut alors s'exercer : chiffrer les données mais aussi les exfiltrer, avec menace de les publier. Certaines données peuvent aussi être exfiltrées et revendues au marché noir (par. ex. des données personnelles, des données médicales). Par rapport au référentiel MITRE, le rançongiciel déploie généralement les tactiques : T1-Reconnaissance (du système à infecter), T3-Compromission initiale (d'une machine), T4-Exécution (déploiement), T5-Persistance, T10-Mouvement latéral (pour migrer vers la cible), T13-Exfiltration (des données qui seront chiffrées), T14-Impact (Chiffrement).

Typologie

Il faut distinguer plusieurs type d'attaques par rançongiciel([9]) :

- les attaques non ciblées, peu sophistiquées, à faible coût, où le principe est d'infecter massivement des machines, généralement peu protégées ;
- les campagnes massives automatisées comme WannaCry en 2017 ;
- les attaques de type *Big Game Hunting*, ciblées, furtives, contre des systèmes préalablement reconnus afin d'identifier les ressources à infecter et à définir le montant de la rançon en conséquence. Elles sont menées par des groupes disposant de ressources : compétences, infrastructure, moyens financiers.

Modèle économique

Les attaquants n'ont généralement pas la compétence technique pour concevoir et maintenir les malwares. Ceux-ci peuvent être utilisés sous forme d'abonnement, de partenariat, de souscription, selon un modèle économique de type RaaS (*Ransomware as a Service*), avec des services additionnels comme le déploiement et le maintien d'une infrastructure de négociation, de paiement, de distribution, des services de type *back-office* comme : le support technique, l'interfaçage de négociation.

Vecteurs d'attaques

Les vecteurs d'attaques sont : les courriels d'hameçonnage, la technique du point d'eau (un URL envoyé par courriel ou bien d'un site web utilisé par l'entreprise mais préalablement compromis), voire l'exploitation de certaines vulnérabilités, souvent des logiciels de gestion à distance, d'accès à distance.

Souvent le ransomware se compose de 2 parties :

- le chargeur (*loader*), qui infecte en premier la victime, ce logiciel télécharge ensuite via le réseau la partie chiffrante ;
- la charge utile proprement dite qui va se propager jusqu'à la cible et chiffrer les données.

Il est aussi possible d'utiliser une infection préalable par un cheval de Troie, réalisée par un autre groupe criminel qui ainsi proposerait le service (payant) d'utiliser une compromission initiale déjà réalisée.

Entre l'infection initiale et le chiffrement de la machine cible, il peut s'écouler quelques heures voire des jours, d'où l'importance d'un système de surveillance pour détecter ce type de compromission.

Architecture

L'attaque par rançongiciel utilise :

- un code de chiffrement ;
- une infrastructure de type Contrôle-Commande, par ex. pour permettre au code loader de télé-charger la partie utile chiffrente à partir d'un serveur extérieur ;
- une infrastructure de distribution ;
- des interfaces d'administration, de paiement, de négociation avec les victimes ;
- un site internet de divulgation de données exfiltrées (si la victime refuse de payer) ;
- une interface de communication avec les médias ;
- un support utilisateur.

La rançon

Une fois le chiffrement effectué, la victime est avertie et peut contacter les attaquants, soit par une adresse de courriel, d'un site accessible via le *dark web*, un site alternatif. La rançon est exigée en monnaie virtuelle convertible. L'interface de négociation peut être utilisée pour réduire la rançon si la monnaie choisie est moins traçable (que le bitcoin notamment). Si paiement accepté et réalisé, les fonds sont alors transférés vers une plateforme d'échange qui convertit la somme en crypto-monnaie. Elle entre alors dans un circuit de blanchiment. Entre demande de rançon et paiement éventuel, peuvent intervenir d'autres intermédiaires :

- les spécialistes de l'extorsion : pour menacer les victimes (divulgation de données, harcèlement, démarchage agressif par téléphone, réseaux sociaux, attaques de déni de service...) et les faire céder au chantage ;
- les spécialistes du blanchiment.

Pourquoi payer ?

La rançon est le plus souvent fixée à hauteur du niveau de solvabilité de l'entreprise. Elle est aussi inférieure au coût de remédiation. Elle peut aussi être couverte (tout ou en partie) par une assurance. Sans oublier qu'à partir de la publication de leurs exigences, les attaquants usent de moyens de pression : décompte du temps, augmentation à mesure que le temps s'écoule, techniques de harcèlement.

Pourquoi ne pas payer ?

La première raison est qu'on encourage ce type de criminalité. Des raisons plus techniques sont à considérer. La victime n'a aucune garantie sur les conditions de déchiffrement. Elle n'a de plus aucune garantie que les données chiffrées (et déchiffrées) n'ont pas été exfiltrées au préalable. Même si la victime paye une rançon et que l'attaque cesse, rien ne dit que des résidus du malware ne sont pas encore présents dans le système. Il faudra donc

le remettre en l'état. Cela veut dire que le coût de remédiation existe quoi qu'on décide.

Il faut aussi prendre en compte les effets à plus long terme sur l'image de l'entreprise dans son écosystème (clients, fournisseurs, partenaires), surtout si l'affaire a été médiatisée.

2.4 Caractérisation du système

2.4.1 Les actifs

Les actifs désignent ce qu'il faut protéger. Il est important pour l'entreprise de les connaître : données, processus métiers. Il ne faut pas oublier que le système d'information n'est qu'une ressource globale de support aux activités. Le perturber revient à porter atteinte aux actifs de l'entreprise.

Dans le monde de l'intelligence économique, les données constituent le capital informationnel, c'est-à-dire la partie formalisée d'un ensemble plus vaste appelé le capital immatériel de l'entreprise, comme le montre la figure 2.14.

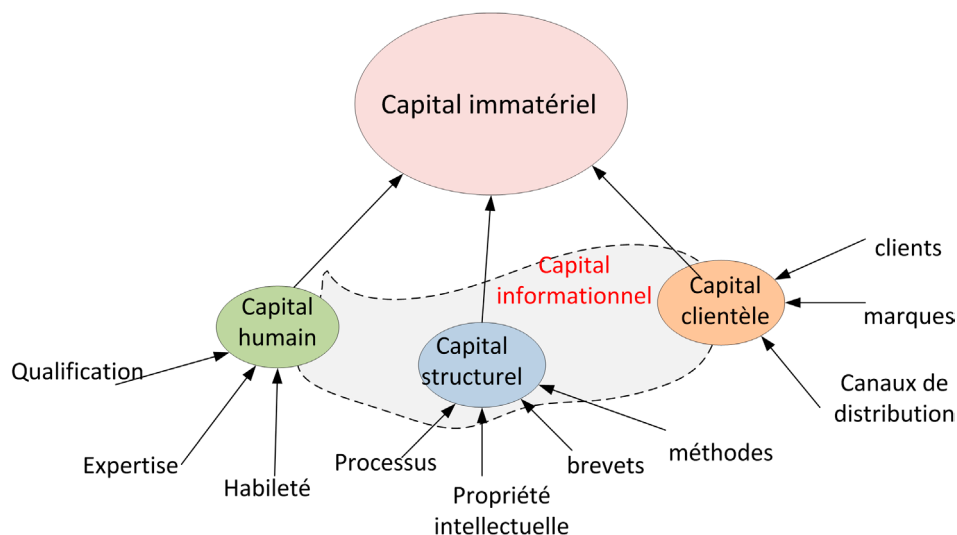


FIGURE 2.14 – Capital informationnel/ immatériel de l'entreprise

2.4.2 Vulnérabilités

Les vulnérabilités caractérisent un périmètre fonctionnel non sécurisé, et donc exploitable par la malveillance. Ce terme du langage courant peut se décliner à divers niveaux, pour désigner des vulnérabilités :

- organisationnelles : absence de classification des données, pas de politique relative à l'usage des smartphones, pas de politique de sauvegarde ;

- humaines : faible compétences de l'utilisateur en terme de technologies numériques, pas de sensibilisation aux risques, à la menace ;
- techniques : logiciels pas mis à jour, hétérogénéité des versions, mauvais paramétrage des applications...

Les vulnérabilités organisationnelles relèvent de l'absence de politique de sécurité, de l'absence de méthode, ce qui est du domaine de la prévoyance.

Les vulnérabilités humaines relèvent d'un niveau de perception du risque faible. On a coutume de dire que l'utilisateur est le maillon faible du système. Il constitue potentiellement un point d'entrée.

Les vulnérabilités techniques sont diverses. Toute vulnérabilité découverte dans un logiciel (par un laboratoire d'essai, un laboratoire de recherche, un expert) fait l'objet d'un signalement à l'éditeur avant publication pour que celui-ci la corrige. Elle est ensuite recensée sous un identifiant et publiée sous le code CVE-Année-Numéro (CVE = *Common Vulnerabilities and Exposures*). Toutes les vulnérabilités / failles connues sont mentionnées avec leur identifiant. La base de données des CVE est gérée par l'organisme MITRE.

Il existe aussi dans les entreprises en général des facteurs aggravants qu'on peut considérer comme des vulnérabilités supplémentaires :

- les PME se considèrent souvent pas ou peu concernées ;
- des systèmes de production critiques exposés de façon non protégée à internet ;
- un manque de sécurité des applications utilisées, des tests de sécurité médiocres ;
- la productivité (l'efficacité) est toujours préférée à la sécurité ;
- quand les contrôles sont trop contraignants, les utilisateurs cherchent à les contourner.

2.4.3 Faille vs vulnérabilité

Il y a peu de différence entre faille et vulnérabilité. Elles sont exploitables de la même manière. Généralement, faille désigne une brèche en terme de sécurité. Vulnérabilité a un sens plus large. Tout ce qui permet à un attaquant en phase de reconnaissance (T1), de prédire un comportement peut constituer une vulnérabilité. Par exemple si un dirigeant a l'habitude de se connecter tous les jours sur le même site web (par. un site de cotation, un site d'information) devient une vulnérabilité exploitable au sens où ce comportement devient prédictible et que le site visité régulièrement pourra être infecté selon la stratégie dite du point d'eau, de manière à infecter par rebond la machine du visiteur, ce qui constitue une technique d'accès initial (T2).

Le mot faille a un sens plutôt technique (on ne parle jamais de faille humaine). Une brèche de sécurité non connue et non corrigée découverte dans un logiciel (et donc exploitable par un attaquant) est appelée faille 0-day.

Même si une vulnérabilité / faille est connue et publiée, elle est toujours potentiellement exploitable par un attaquant dès lors que les mises à jour ne sont pas faites alors qu'elles sont disponibles.

2.4.4 Exploit

Un exploit (au sens de exploitation) ou code d'exploitation, désigne un composant logiciel capable d'exploiter une vulnérabilité ou faille de sécurité, soit localement, soit via un réseau. Tous les malwares sont conçus pour exploiter des vulnérabilités.

2.4.5 Analyse de vulnérabilités

Le rôle d'un audit de sécurité est d'abord de découvrir les vulnérabilités. Les méthodes sont statiques ou dynamiques. Le mode statique consiste à vérifier la présence de vulnérabilités / failles d'après une liste de contrôle. Ceci peut être fait de manière automatisée. Les outils appelés scanners de vulnérabilités, utilisent le réseau pour identifier, tester, générer un rapport de sécurité sur tout ce qui est IP-adressable : ordinateurs, serveurs, routeurs, pare-feux, smartphones, objets connectés, sites web, automates, robots, téléphones.

Une méthode plus dynamique consiste à faire des **tests d'intrusion** (*penetration tests* ou *pentests*). Ce qui est recherché ici c'est la découverte de vulnérabilités par un expert qui va simuler le comportement d'un attaquant. Le but est bien sûr de ne pas créer des dommages mais de découvrir les vulnérabilités exploitables pour le faire. Les tests d'intrusion peuvent se faire selon 3 méthodes :

- boîte noire : le testeur se comporte comme un attaquant externe, il ne connaît rien au système, il doit donc exécuter la phase T1 (Reconnaissance) ;
- boîte blanche : le testeur simule soit l'attaquant externe qui a réussi les phases T1, T3, T6, T8 notamment, soit l'attaquant interne : il connaît l'architecture du système, les applications utilisées, les comptes utilisateurs ;
- boîte grise : intermédiaire, il se comporte comme s'il avait déjà la possibilité de s'authentifier notamment.

Les tests dit de *Red Team* sont des tests sans limite de durée ni de périmètre. Les tests d'intrusion sont aujourd'hui à la base de l'audit de vulnérabilités. La limite de ces audits (et sans doute la frustration de ceux qui les commandent) est leur caractère non exhaustif. Si l'entreprise fait réaliser un audit avec un prestataire, un autre prestataire générera un rapport différent. C'est-à-dire qu'il n'existe aucune garantie que toutes les vulnérabilités potentielles du système soient découvertes.

Il existe des audits de vulnérabilité plus ciblés comme par exemple les tests de hameçonnage *phishing* ou *spear phishing*. Le but est de tester le niveau de vulnérabilité humaine (soit massivement, soit de façon plus ciblée) à la réception de certains mails conçus spécialement selon les techniques d'ingénierie sociale adaptées, les messages comportant un URL actif ou une pièce jointe. Le but est d'enregistrer combien (et qui ?) font ce qu'il ne faut pas faire, c'est-à-dire cliquer sur le lien, ouvrir la pièce jointe.

2.4.6 Protection

Protection est le premier mot-clé de la sécurité des systèmes d'information (SSI). Il s'agit ici de protéger les actifs de l'entreprise. Il convient donc de les identifier d'abord, de les cartographier dans le système d'information. Le périmètre est à la fois technique, organisationnel, juridique.

Ce qu'on entend par technique concerne le système informatique (infrastructure, réseau, implémentation, machines (tout ce qui est IP-adressable), applications, logiciels).

Ce qui relève de l'organisationnel concerne de façon générale la politique de sécurité ou PSSI (il faut en avoir une et l'appliquer), la définition et la mise en place d'un système de management de la sécurité (SMSI), les méthodes préventives comme les plans de secours et plan de continuité (en cas d'incident/ accident), de politique de sauvegarde des données, et de façon curative, la gestion (technique, organisationnelle) des incidents.

Ce qui relève du juridique concerne les obligations (lois, règlements). Cela dépend du domaine de l'entreprise mais toutes sont concernées par la protection des données personnelles.

2.4.7 Détection

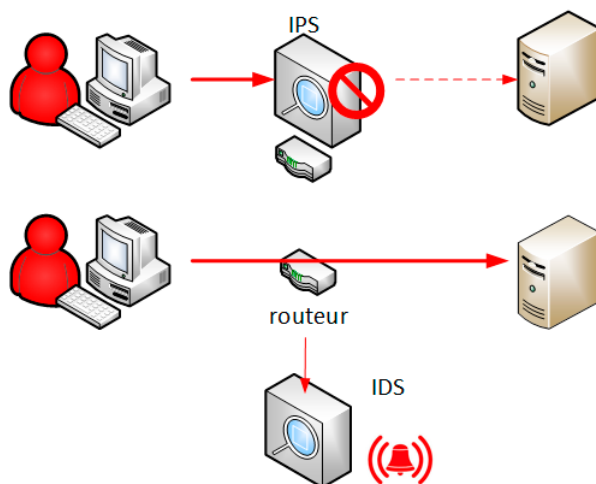
Ce qu'on détecte ce sont les symptômes, appelés aussi **indicateurs de compromission** (IOC). La détection peut se faire à plusieurs niveaux :

- par l'utilisateur lui-même : qui peut constater des symptômes (affichage perturbé, indisponibilité des données, absence de connexion) ;
- par le système de supervision : il permet de contrôler les aspects fonctionnels du réseau, des serveurs, des services. Tout incident de sécurité se traduit par des dysfonctionnements (par ex. une augmentation anormale du trafic, des tentatives de connexion infructueuses) ;
- par des sondes de détection réparties, ce sont des sondes de détection d'intrusion, (IDS *Intrusion Detection System*). Ne pas confondre IDS et IPS (*Intrusion Prevention System*), la figure 2.15 présente la différence. IDS et IPS détectent les tentatives d'intrusion, en analysant le comportement des flux réseau, en se basant sur des signatures d'attaques, mais les IDS alertent alors que les IPS bloquent.

Les alertes ne suffisent pas, pour réduire p_5 , il faut qu'elles soient traitées et fassent l'objet d'un traitement rapide et efficace.

Dans le cas d'une attaque de type DoS, compte tenu de sa rapidité et des trafics mis en jeu, la détection est primordiale pour en repérer les symptômes. Ils sont résumés figure 2.16. Le premier est l'augmentation brutale du trafic. Celle-ci peut déjà être détectée au niveau du fournisseur d'accès à l'internet (FAI).

Concernant les opérateurs de cloud, leur architecture doit prévoir ce type d'attaque et anticiper la détection et le détournement du trafic en cause. Néanmoins ces opérateurs ont des contraintes que n'ont pas les entreprises ordinaires.

FIGURE 2.15 – IDS *vs* IPS

Elles sont tenues à des contrats de service et les débits qu'elle gèrent dans leur infrastructure dépassent le téra-octets/s (To). Les contre-mesures doivent donc éviter de perturber l'internet et éviter de perturber le trafic "normal" des clients.

2.4.8 Impact

L'impact désigne ici le niveau de dommage, soit la phase T14 de la matrice MITRE. Plus les dommages sont élevés plus l'impact est grand. De par la formule du risque, quand il n'y a pas de risque il n'y a pas d'impact. Même si la cible est touchée, si des machines sont compromises, si des données deviennent indisponibles, avoir un système de sauvegarde des données et de restauration des postes de travail et des serveurs permet d'atténuer fortement les dommages. Dans ce cas ils se limitent à des temps d'interruption supportables (ou de fort ralentissement) des processus impactés.

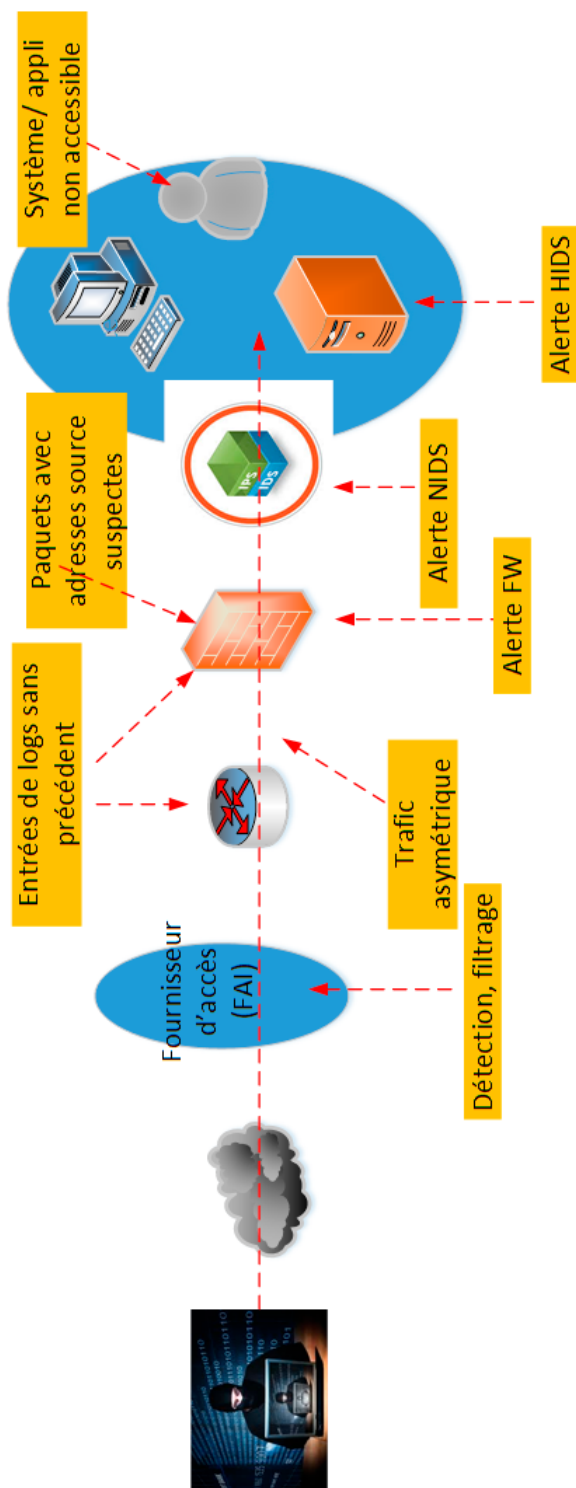


FIGURE 2.16 – Symptômes d'une attaque DoS



2.4.9 Relations entre les concepts

La figure 2.17 est un diagramme entités/rerelations entre tous les termes définis précédemment. L'idéal est de savoir le reconstituer. La figure 2.18 introduit une typologie des différents termes.

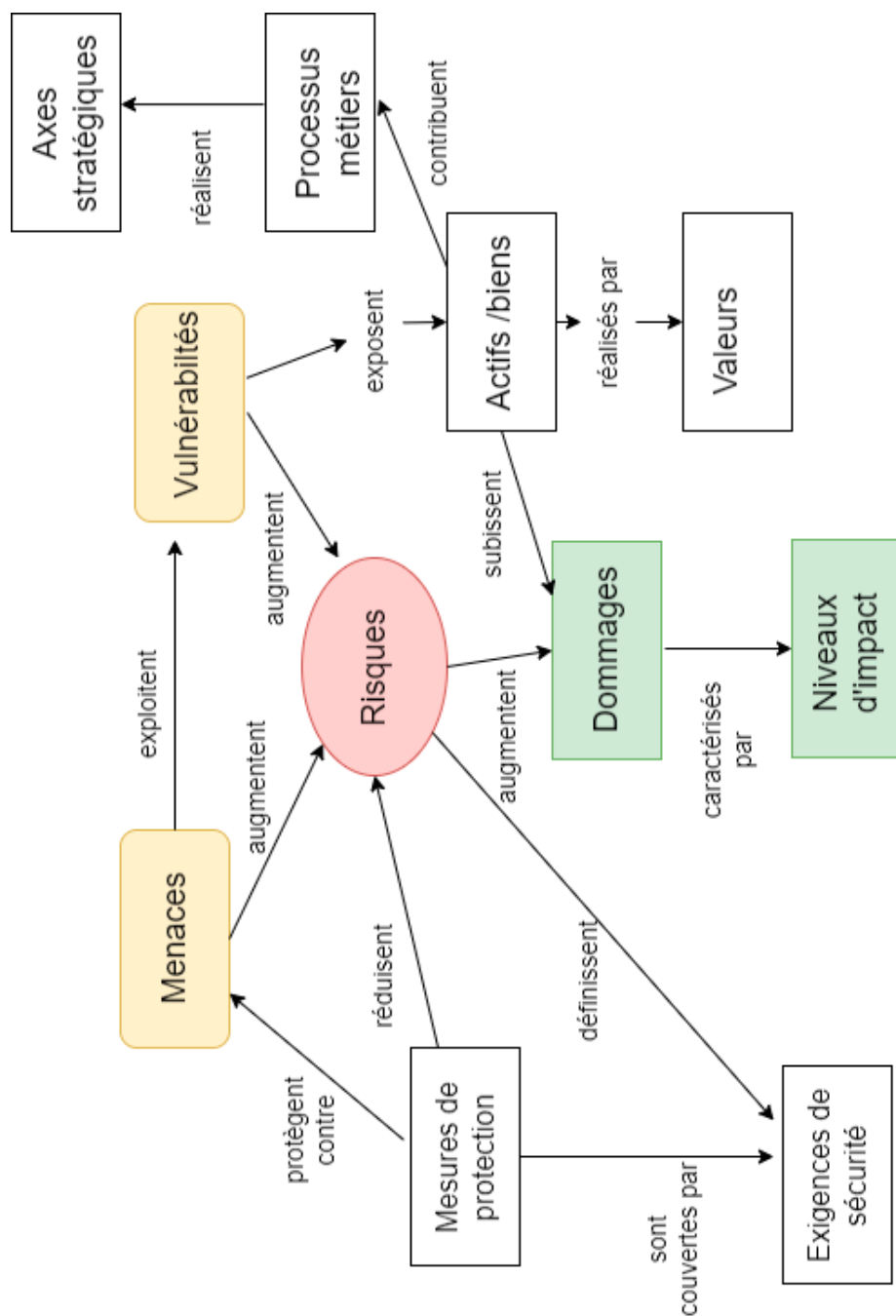


FIGURE 2.17 – Diagramme entités / relations

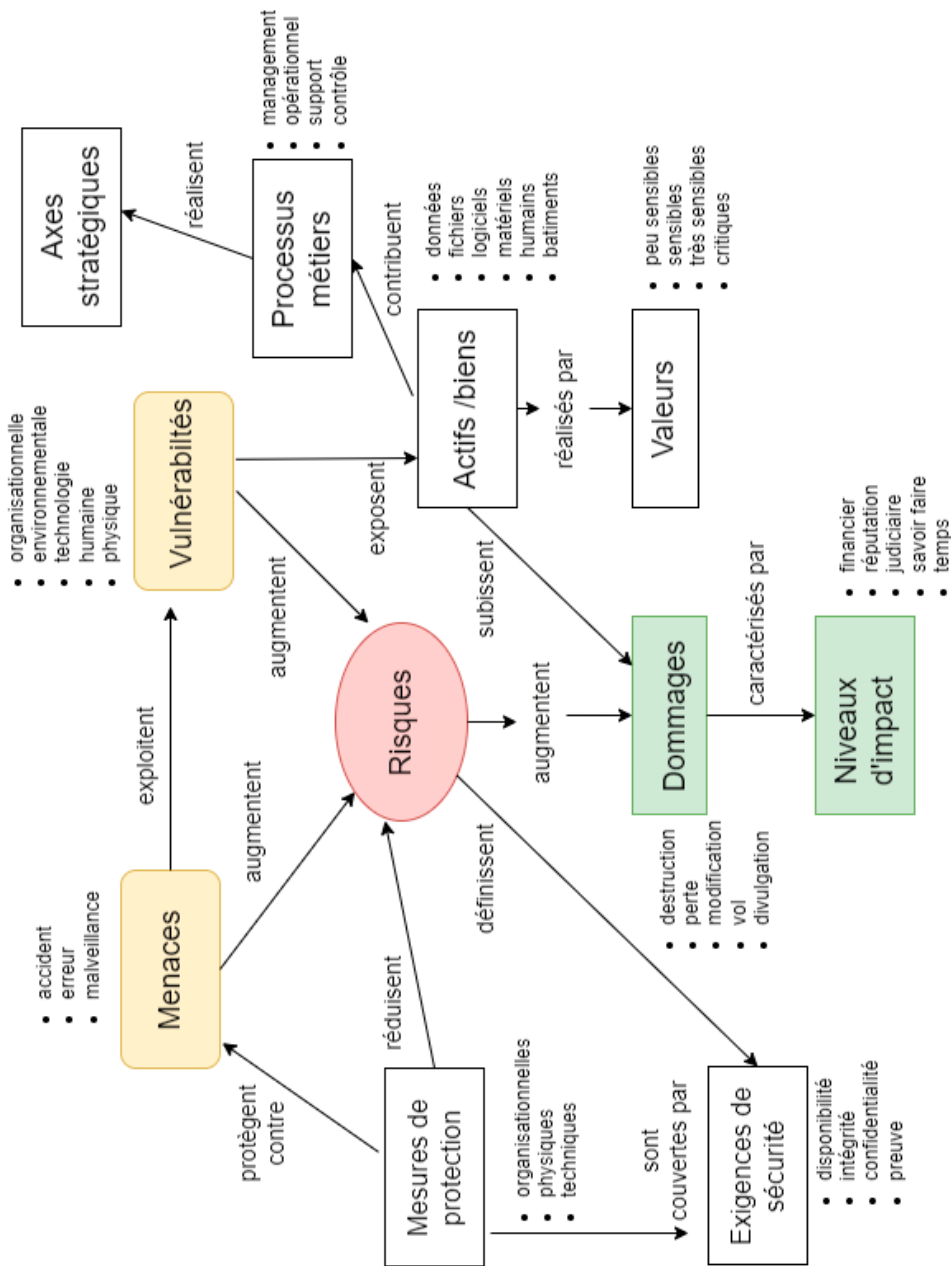


FIGURE 2.18 – Diagramme détaillé

2.5 La gestion des risques

2.5.1 Processus

Le processus de gestion des risques se décompose généralement de la façon suivante :

- P1) Identification : mettre en avant les menaces, les vulnérabilités, l'enchaînement des événements (scénarios) pouvant conduire à l'événement redouté ;
- P2) Estimation : "quantifier" le risque en fonction des actifs concernées (individus, données, processus métiers, etc.) ;
- P3) Évaluation : classer et différencier les risques selon leur acceptabilité mais l'identification d'un seuil qui caractérise un niveau maximum de sécurité souhaité et assumé ;
- P4) Traitement : cela concerne les mesure de protection, mitigation, reprise d'activité après accident.

2.5.2 P1-Identification

Il faut s'appuyer sur une analyse de la menace (qui peut nous en vouloir et pourquoi faire, quels sont ses modes d'action), une analyse de vulnérabilités (via un audit), identifier les événements redoutés, c'est-à-dire identifier les scénarios pouvant impacter les actifs (les connaître).

Pour les PME/TPE, la perception du risque est très souvent réduite au minimum :

- p_1 : je suis trop petit je n'intéresse personne
- p_2 : ça n'arrive qu'aux autres
- p_3 : non concerné (de fait)
- p_4 : non concerné
- p_5 : non concerné

2.5.3 P2-Estimation

La composante p , qui mesure un niveau de vraisemblance (et qui peut se décomposer en 5 facteurs comme nous l'avons vu précédemment) est évaluée de façon qualitative selon une échelle de 1 à 4, de 1 à 5 ou de 1 à 10. Le principe reste le même, il faut seulement savoir interpréter. Sait-on faire la différence entre un niveau 7 et un niveau 8 ? Dans le cas contraire, mieux vaut se contenter d'une échelle simple de 1 à 4. Dans ce cas la figure 2.19 donne une idée de la façon de graduer le niveau de vraisemblance.

La sémantique est la suivante, 4 : très probable, 3 : probable, 2 : assez probable, 1 : peu probable. Les termes p_1 et p_2 sont quasiment proche de 1. Le rôle de la protection (SSI) est de réduire les 3 autres termes.

La composante G est estimée aussi de façon qualitative par un facteur d'impact. Si on prend là encore une échelle de 1 à 4, la sémantique peut être la suivante, 4 : très grave, 3 : grave, 2 : assez grave, 1 : peu grave. Cette estimation résulte de l'expertise et donc de l'expérience.

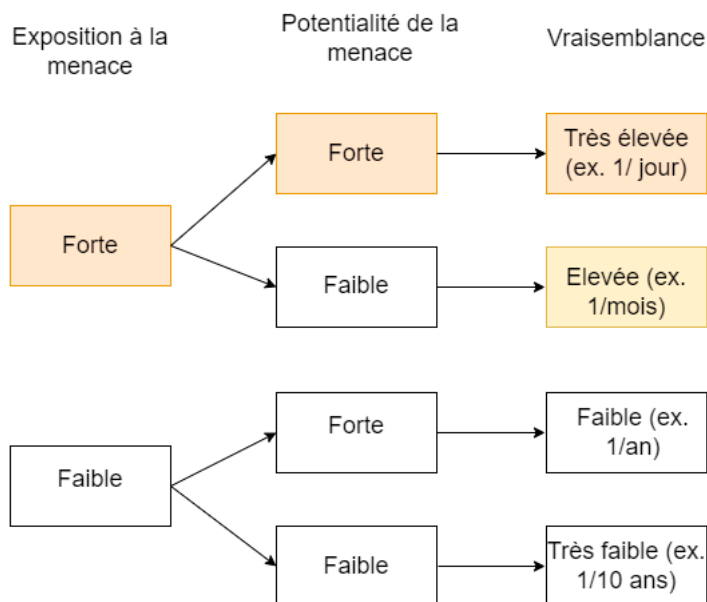


FIGURE 2.19 – Approche qualitative

Le choix du référentiel d'analyse est important, il doit être orienté selon la nature des décisions à prendre.

On peut adopter une typologie :

- par type d'attaques : pour mettre en place des contre-mesures (approche technique) ;
- par type de dommages : pour évaluer les conséquences et évaluer des coûts (approche gestionnaire) ;
- par type de menaces : pour prendre des mesures préventives, définir des actions à plus long terme (approche stratégique).

Chaque scénario redouté peut être associé à une vulnérabilité exploitable. On peut évaluer un niveau de gravité associé. Il existe notamment le système CVSS (*Common Vulnerability Scoring System*), qui fournit un score (entre 1 et 10) pour évaluer l'impact d'une vulnérabilité. Attention néanmoins à ne pas confondre scénario d'attaque et vulnérabilité. Une vulnérabilité peut être exploitée par plusieurs scénarios. Corriger une vulnérabilité permet donc potentiellement de diminuer plusieurs risques associés. La relation vulnérabilité $\leftrightarrow$ scénario (et donc risque) n'est pas bijective.

2.5.4 P3-Évaluation

À partir de la phase P1 on doit dresser une liste des scénarios redoutés. À partir de la phase P2 on estime les termes p (vraisemblance) et G (impact). Le risque peut alors être calculé $R = p * G$, pour chaque scénario. Chacun peut

donc représenter dans un graphe comme celui de la figure 2.20. Pour chaque carré élémentaire on peut adopter un code de couleur, selon le niveau du risque : rouge quand p et G sont élevés, orange quand l'un des 2 est élevé, jaune quand les 2 sont modérés et vert quand les deux termes sont faibles.

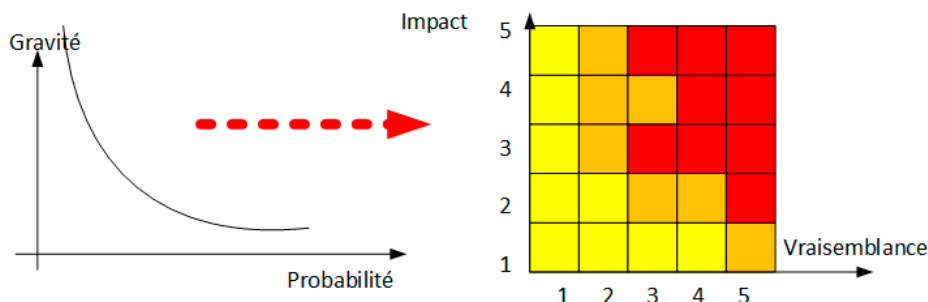


FIGURE 2.20 – Risques : approches quantitative *vs* qualitative

Les risques calculés peuvent ensuite être classés par ordre décroissant. Sur la base de l'évaluation, permettant de hiérarchiser les risques, on fixe alors un seuil d'acceptabilité. Il convient que le niveau de risque du seuil soit faible. En dessous, on parle de risque résiduel (par ex. $p = 1$ et $G = 1$). Cela ne veut pas dire que le risque est négligé, cela veut dire qu'il est identifié et doit être sous contrôle. Comment ce seuil est-il fixé? Le dilemme de la gestion des risques est l'acceptabilité, avec plusieurs points de vue :

- technique : selon le jugement des experts (informatique, cyber-sécurité) ;
- économique : la balance coût / bénéfices doit être équilibrée ;
- sociale (individuelle et organisationnelle) : la sécurité peut être vécue comme une contrainte (limitation d'accès, allongement des procédures, frein aux projets, etc.).

2.5.5 P4-Traitement

Tous les risques situés au-dessus du seuil d'acceptabilité doivent être traités et ramenés à des niveaux acceptables (jaune, vert) comme l'illustre la figure 2.21.

2.5.6 Norme ISO 27005

La norme ISO 27005 fournit un cadre de gestion du risque lié à la sécurité de l'information. Elle fournit aussi des conseils relatifs à l'appréciation, au traitement, à l'acceptation du risque.

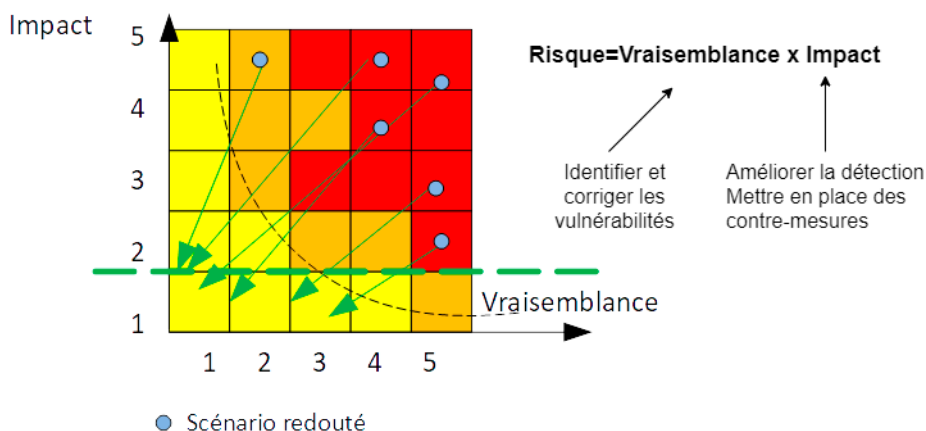


FIGURE 2.21 – Réduction des risques

2.5.7 Méthodes d'analyse de risques

Il existe plusieurs méthodes d'analyse de risques. Elles sont destinées à fournir à la fois un cadre méthodologique et un cadre référentiel. Nous nous contenterons ici de les citer. Nous y reviendrons au chapitre suivant. Comme nous l'avons vu, le sujet n'est pas que technique, il est aussi organisationnel. Quand un auditeur arrive dans une entreprise pour effectuer une analyse de risques du SI, la question est pour lui de savoir comment procéder et quoi contrôler.

Pour le référentiel, on peut se baser sur la norme ISO 27002, révisée en 2017. Elle comporte 14 volets (voir figure 2.22) qu'on peut regrouper en deux grands sous-ensembles :

- organisationnel : la politique de sécurité, l'organisation de la sécurité, la gestion des actifs, la sécurité des RH, la relation avec les fournisseurs, la gestion des incidents ;
- technique : contrôles des accès, utilisation de la cryptographie, sécurité des communications, sécurité physique, sécurité liée à l'exploitation.

Pour chacun des volets, plusieurs points de mesure sont à évaluer.

Pour les aspects méthodologiques, le fil conducteur est le suivant :

- identifier les actifs de l'entreprise ;
- identifier pour chacun des actifs les scénarios redoutés (malveillance, pannes, accidents) ;
- pour chaque scénario, analyser les vulnérabilités exploitables ;
- évaluer la vraisemblance p de chacun des scénarios ;
- évaluer les impacts G ;
- évaluer les risques de chacun des scénarios dans un graphe $p * G$;

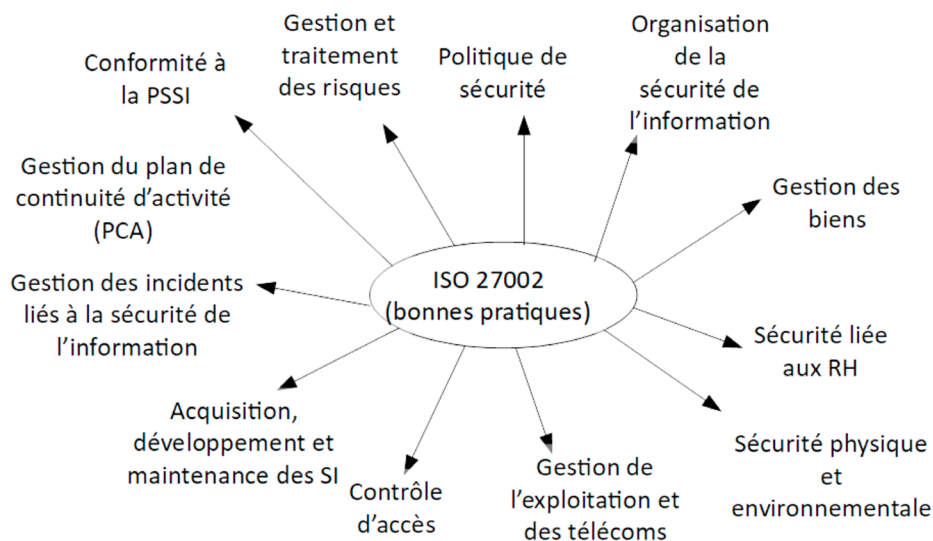


FIGURE 2.22 – ISO 27002 : les 14 volets

- élaborer un plan de réduction des risques situés au-dessus d'un seuil d'acceptabilité.

Rappelons que les relations entre scénarios, vulnérabilités, risques, ne sont pas bijectives, ce qui veut dire que :

- plusieurs scénarios peuvent menacer un même actif ;
- plusieurs vulnérabilités peuvent être exploitées dans un même scénario ;
- une vulnérabilité est potentiellement exploitable par plusieurs scénarios ce qui veut dire que la corriger peut avoir pour effet de diminuer plusieurs risques associés.

Les normes ISO peuvent paraître sur-dimensionnées pour les PME et les TPE. Néanmoins, on peut s'inspirer du cadre exhaustif proposé et essayer de l'adapter (sans le dégrader). Souvent, une mise à niveau élémentaire à partir de ce qu'on appelle les bonnes pratiques de sécurité (protection du poste de travail, du réseau, des accès aux ressources du SI, des données sensibles) permet déjà de corriger de nombreuses vulnérabilités.

En France la méthode MEHARI [10] est une méthode de gestion des risques conçue par le CLUSIF. Elle a été très utilisée pour sa simplicité, la dernière version date de 2010.

La méthode EBIOS [11], développée en 1995, est maintenue par l'ANSSI (Agence Nationale de la Sécurité des Systèmes d'Information). Elle est connue sous le nom de eBIOS-RM (Risk Manager).

2.6 Autres définitions

2.6.1 Cybersécurité

Nous utilisons ici la définition de l'ANSSI qui doit faire référence. La cybersécurité englobe 3 grands domaines, non-disjoints (figure 2.23) :

- la sécurité des systèmes d'information (SSI) ;
- la lutte contre la cyber-criminalité ;
- la cyber-défense.

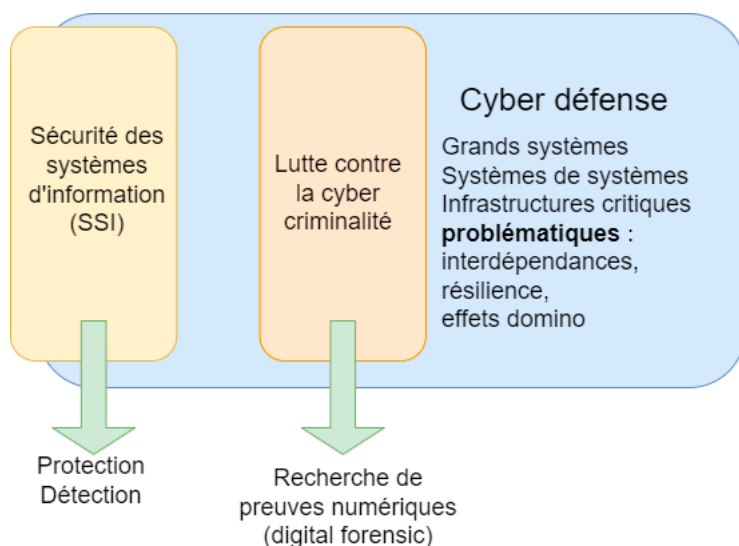


FIGURE 2.23 – Cybersécurité : composantes

2.6.2 Sécurité des systèmes d'information

Cela regroupe toutes les actions pour défendre le système d'information contre les menaces internes et externes. Le mot clé est d'abord : protection. On peut ensuite rajouter : détection. La mise en place d'un système de détection efficace est la clé pour limiter les impacts.

2.6.3 Lutte contre la cyber-criminalité

Cela regroupe les actions pour étudier la malveillance sous toutes ses formes, malveillance établie par rapport au droit. Son rôle est surtout curatif (après incident) mais nécessite des formes d'anticipation, afin d'étudier en amont la menace sous toutes ses formes. Le mot clé est ici : recherche de preuves numériques (ou *digital forensic*). Nous reviendrons sur ce point dans la partie 3.

Cela concerne avant tout les officiers de police judiciaire (police, gendarmerie), qui agissent dans le cadre d'une violation du droit pénal qui définit la cyber-criminalité.

2.6.4 Cyber-défense

La cyber défense peut se définir comme la SSI appliquée aux organismes d'importance vitale. Ce qui les caractérise, outre leur aspect stratégique (pour l'état, les collectivités, les citoyens), c'est surtout qu'il s'agit de grands systèmes, voire des systèmes de systèmes. Par exemple : les réseaux de transport (eau, gaz, électricité), les opérateurs de télécommunications, de production d'énergie, de transport. Pour ces entreprises, les exigences de sécurité sont à la hauteur des missions qu'elles doivent rendre. Les interruptions de service ne sont pas envisageables. Se posent alors des questions :

- de résilience : comment continuer de fonctionner même en mode dégradé suite à une cyber-attaque ;
- de sécurité globale : comment éviter les effets domino entre cyber-attaque et atteinte à la sécurité des biens et des personnes, à la suite d'un accident industriel (explosion, inondation, pollution, incendie, fuite radioactive, collision...).

Autres usages du terme cyber-défense :

- défense contre des attaques dans un cadre de conflit (terme militaire) ;
- traitement des (cyber) incidents (terme employé par les recruteurs).

2.6.5 Cyber-guerre

En matière de droit (de la guerre) le terme cyber-guerre ne veut rien dire. Personne n'a jamais déclaré de cyber-guerre. Toutes les actions visant les SI d'un autre état relève donc du droit pénal. Néanmoins, on peut dater de 2007 et l'attaque massive de l'Estonie (pays qui a massivement numérisé ses procédures publiques) par son puissant voisin, sous forme d'attaque de déni de service sur les serveurs publics, et ce pendant plusieurs jours, l'exemple d'un état qui s'en prend à un autre état, sans déclaration de guerre préalable. De plus l'état agresseur ne le fait jamais directement mais utilise des prestataires de service qui sont souvent des groupes de cyber-criminels nationalistes de façon à masquer toute responsabilité et à rester dans le déni. D'autres actions de ce type ont été vécues par la suite. On peut aussi ajouter que tout conflit militaire sera précédé, amplifié, par des cyber-attaques contre les infrastructures vitales du pays adverse. Les états se dotent d'armes numériques (malwares, bombes logiques) en plus des armes conventionnelles.

2.7 La réponse à incident

2.7.1 Quelques définitions

Événement

Un événement est quelque chose d'observable (réseau, système). On peut citer comme exemple :

- la connexion à un espace partagé ;
- la réception d'une requête par un serveur ;
- l'envoi d'un email ;
- le blocage d'une tentative de connexion par le pare-feu.

Les événements génèrent des traces, en différents points : équipements réseau, serveurs, terminaux, applications. Ces traces sont communément appelées des logs. Elles ont un format, elles renseignent (notamment) sur le type d'événement, le lieu, la date et l'heure. Cela représente au niveau d'un système une très importante quantité de données répartie mais il existe des outils permettant de les centraliser (à des fins de supervision notamment).

Incident

Un incident est un événement (observable) mais contraire, c'est-à-dire avec des effets négatifs, par exemple :

- un crash système ;
- une inondation de serveur par des requêtes ;
- l'utilisation outre droits de privilèges système ;
- l'accès non autorisé à des données sensibles ;
- l'exécution d'un malware.

Définitions officielles

Elles peuvent être formulées de plusieurs façons mais l'idée reste la même. Un ou plusieurs événements intéressant la sécurité de l'information, indésirables ou inattendus, présentant une forte probabilité de compromettre les opérations et de menacer la sécurité de l'information (ISO 27000).
Acte de violation explicite ou implicite d'une politique de sécurité (*National Institute of Standards and Technology (NIST), Special Publication 800-61*).

Incident vs crise ?

Une crise suppose un incident de sécurité hors norme pour plusieurs raisons qui peuvent se cumuler.

- l'attaque est d'un type nouveau (pas de signature connue, pas de modèle MITRE par ex.) ;

- les cibles impactées sont très nombreuses (plusieurs milliers de postes et serveurs) ;
- la propagation n'est pas maîtrisée.

On a pu connaître des exemples en 2017, quand des milliers d'entreprises et grands groupes de par le monde ont subi les attaques WannaCry et NotPetya. Des milliers de machines ont été impactées, des salariés en chômage technique pendant plusieurs semaines, des dégâts chiffrés en plusieurs milliers d'euros. La résolution de la crise a nécessité pour chaque entreprise plusieurs dizaines d'experts pendant plusieurs semaines. Combien de temps dure une situation de crise ? On considère empiriquement que la crise perdure tant que les experts / techniciens ne maîtrisent pas la situation. Dans le cas contraire, cela ne veut pas dire que l'incident est clos mais cela veut dire que le diagnostic a été posé, qu'un mode opératoire a été défini pour circonscrire la propagation et pour remettre le système en état, qu'il s'applique efficacement, que la clôture de l'incident n'est plus qu'une question de temps.

2.7.2 Les incidents de sécurité

Classification

Les incidents sont classés par niveau de sévérité.

Id	Sévérité	Impact sur activité
0	Basse	faible impact
1	Moyenne	dommages mais sans mettre le système en danger
2	Haute	dommages significatifs au système

TABLE 2.1 – Sévérité des incidents (ISO 27035)

Exemples d'incidents de niveau 2 :

- intrusion dans le réseau ;
- compromission physique du SI ;
- perte d'informations ultra confidentielles non chiffrées ;
- infection de plus de 25% de machines ;
- hameçonnage en cours utilisant le nom de domaine et la marque.

Exemples d'incidents de niveau 1 :

- attaque DoS ;
- utilisation d'accès non autorisés ;
- intrusion automatisée ;
- infection par un malware ;
- installation d'un logiciel malveillant ;
- modification suspect d'activité.

Exemples d'incidents de niveau 0 :

- violation de procédure ou de politique détectée à partir des logs ;
- perte ou vol de portable contenant de l'information confidentielle ;
- installation de logiciel non autorisé ;
- malware sur un PC.

Quelques précisions s'imposent. Un incident de niveau 0 ne veut pas dire qu'on ne va pas le traiter. Cela veut dire que l'incident est localisé, ponctuel et qu'il peut être traité rapidement.

Le classement par ordre de sévérité suppose qu'un diagnostic ait été établi sur la base d'indices de compromission, détectés notamment au niveau du système de supervision et /ou de surveillance.

La figure 2.24 donne quelques exemples de signes de compromission.

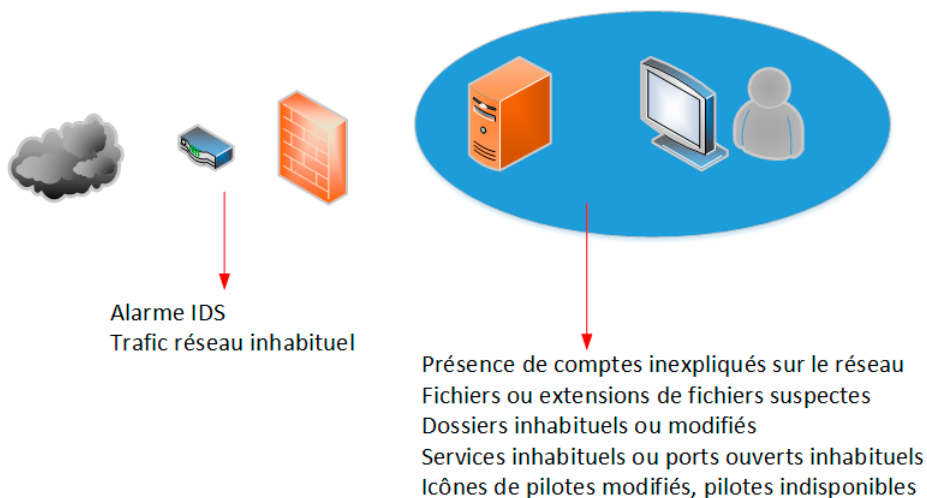


FIGURE 2.24 – Quelques signes de compromission

2.7.3 La procédure de traitement des incidents

Pourquoi élaborer une procédure de réponse à incident ? Deux raisons :

- la nécessité de répondre rapidement et efficacement dès qu'une infraction est détectée ;
- le besoin de définir une méthodologie de réponse et une procédure avec des actions appropriées.

Cette procédure doit permettre :

- d'économiser du temps, d'éviter les pertes d'information, les ruptures de service ;
- de prendre en compte tous les aspects (technique, juridique, organisationnel) ;
- d'améliorer la procédure et le niveau de protection par retour(s) d'expérience.

Pour définir une procédure adaptée, des aspects politiques (de l'entreprise) sont à prendre en compte :

- avoir défini une échelle adaptée de gravité et d'impact des incident de sécurité ;
- avoir défini les rôles, responsabilités, autorités des acteurs ;
- savoir à qui s'applique cette procédure et dans quelle circonstance ;
- avoir défini les buts, les objectifs, le périmètre de la procédure.

2.7.4 Éléments de procédure

Planification

La procédure est exécutée par une équipe de réponse à incident. Il faut définir sa structure, sa taille, ses compétences, mesurer son efficacité (voir figure 2.25).

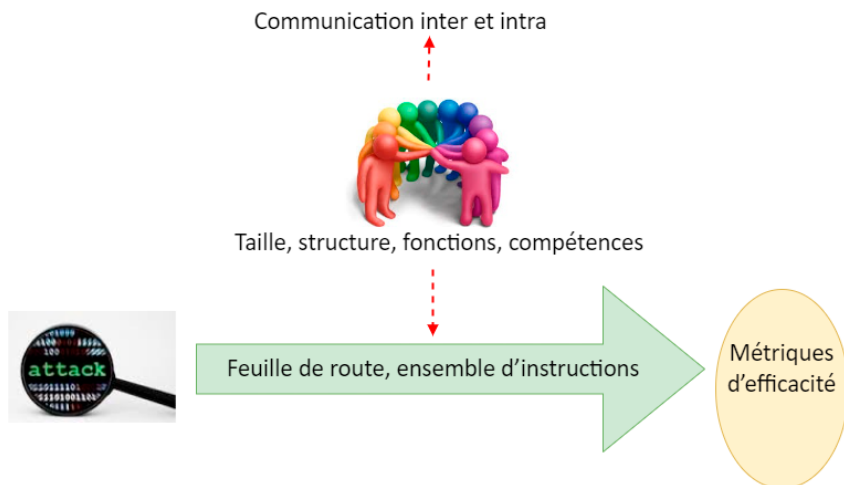


FIGURE 2.25 – Éléments de planification

Communication

L'entreprise peut être amenée à communiquer en interne et avec son environnement, cela dépend de sa surface médiatique, de son écosystème, et aussi de la nature de l'incident de sécurité. Comme le montre la figure 2.26. L'entreprise doit gérer la communication avec :

- ses collaborateurs (surtout en situation de crise) ;
- ses clients (surtout le grand public) ;
- ses partenaires et fournisseurs (pour des raisons de confiance et aussi parce qu'ils peuvent être impactés) ;

- son autorité en matière de sécurité : par ex. l'ANSSI si elle est classée comme OIV ;
- ses prestataires en matière de sécurité, notamment dans le domaine de la surveillance, du traitement des incidents (CERT, voir plus loin) ;
- les services d'investigation (si dépôt de plainte).

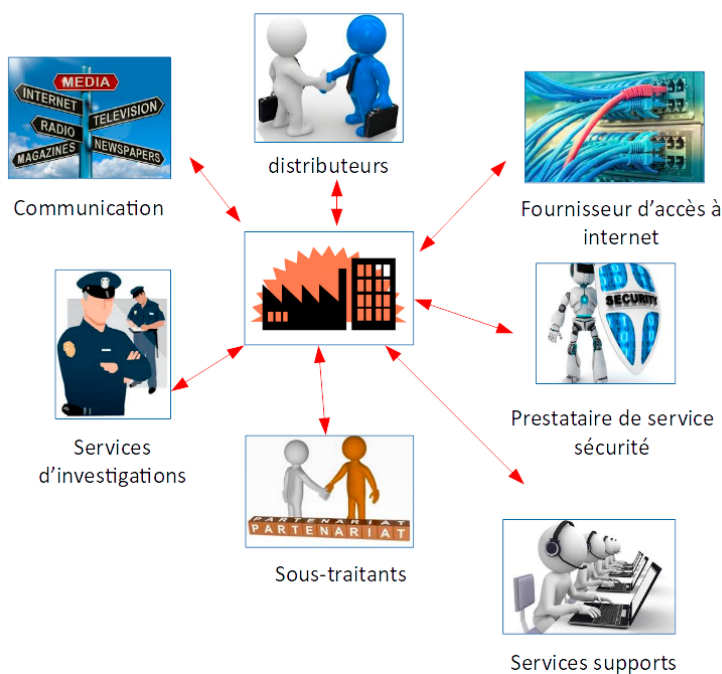


FIGURE 2.26 – Aspects communication

La nature de la communication diffère selon les acteurs. Elle peut être de nature technique (ANSSI, CERT, enquêteurs) ou non. Elle implique la direction, le service communication et les techniciens.

Les aspects à traiter

La figure 2.27 synthétise les différents aspects à traiter lors du déroulement de la procédure de traitement des incidents. Ce sont essentiellement des aspects techniques, qui sont multiples. Nous y reviendrons plus en détail.

Buts à atteindre

Dans sa partie technique, la procédure ne peut se conclure sans avoir atteint des objectifs résumés figure 2.28



FIGURE 2.27 – Aspects à traiter



FIGURE 2.28 – Les buts à atteindre

Moyens nécessaires

Le processus de traitement des incidents peut être long (plusieurs jours à plusieurs semaines en cas de crise), il nécessite des moyens humains mais potentiellement aussi matériels. Ce que présente la figure 2.29.



FIGURE 2.29 – Moyens nécessaires

Documents exploitables en amont

Les documents qui constituent la politique de sécurité peuvent ici être utiles, comme les rappelle la figure 2.30.

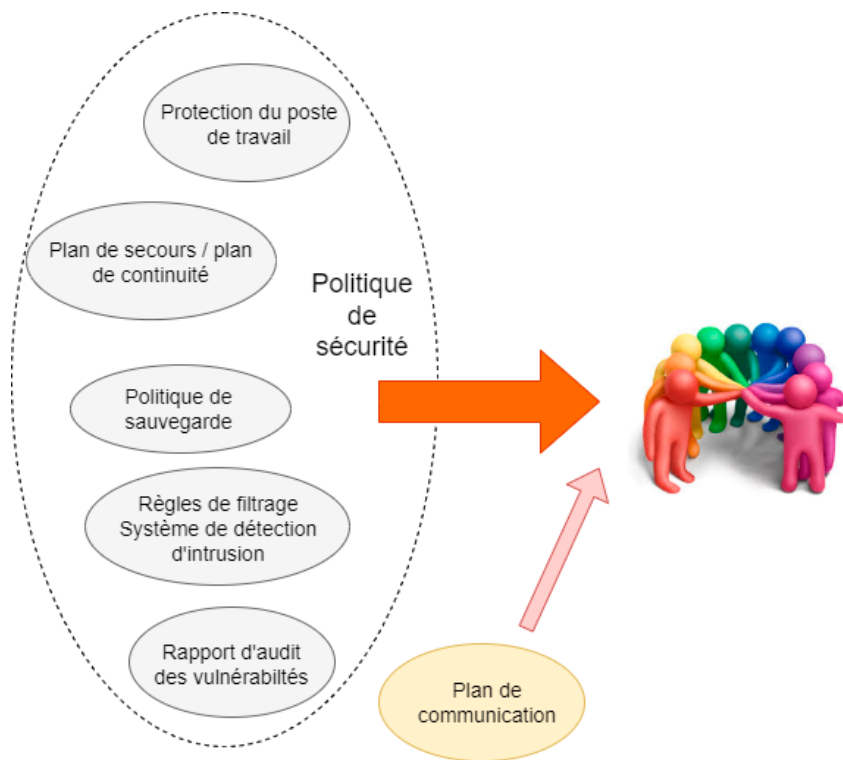


FIGURE 2.30 – Les éléments amont

Certains sont très importants ici comme le plan de continuité des activités (PCA), qui est utilisé dans un cadre de sécurité plus global, incluant la sécurité physique, ou encore le plan de sauvegarde, éléments clé pour diminuer les impacts et pour la restauration du système.

2.7.5 L'équipe de réponse à incident

Organisation

Selon le périmètre géographique de l'entreprise (groupe, PME, mono/multi-sites), son organisation en réseau, plusieurs modèles d'organisation sont possibles pour une équipe de réponse : elle peut être centralisée (figure 2.31), répartie (figure 2.32), répartie mais avec une coordination centralisée (figure 2.33). Elle peut aussi être internalisée (figure 2.34), externalisée (figure 2.35) ou mixte (figure 2.36).

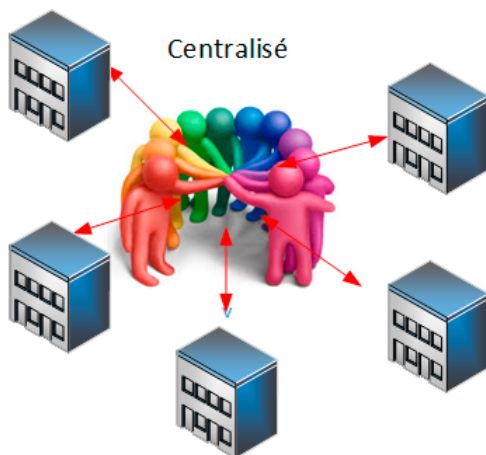


FIGURE 2.31 – Modèle centralisé

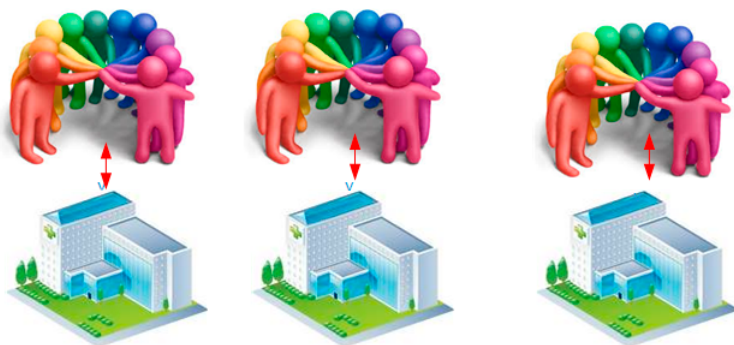


FIGURE 2.32 – Modèle réparti

Une équipe de réponse à incident doit répondre à plusieurs qualités et contraintes :

- la disponibilité : 24h/24, 7j/7 ;
- l'astreinte : sur site ou à domicile ;
- la mentalité et l'esprit de corps ;
- le coût ;
- les compétences et l'expertise sur le sujet.

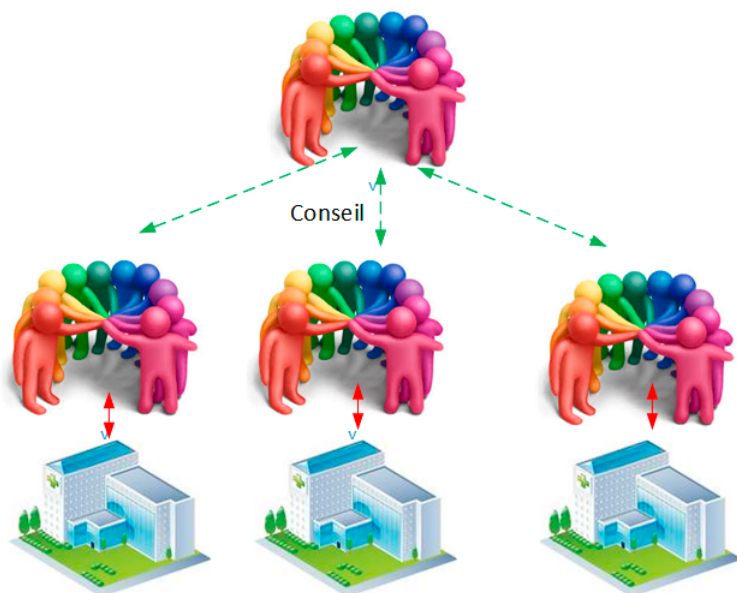


FIGURE 2.33 – Modèle réparti avec contrôle centralisé



FIGURE 2.34 – Modèle interne

Le choix de l'externalisation (oui/non), de son mode (total / partiel), dépend de plusieurs facteurs :

- la qualité du service (au niveau du contrat), comment la définir, quels indicateurs, comment la mesurer et l'évaluer ;

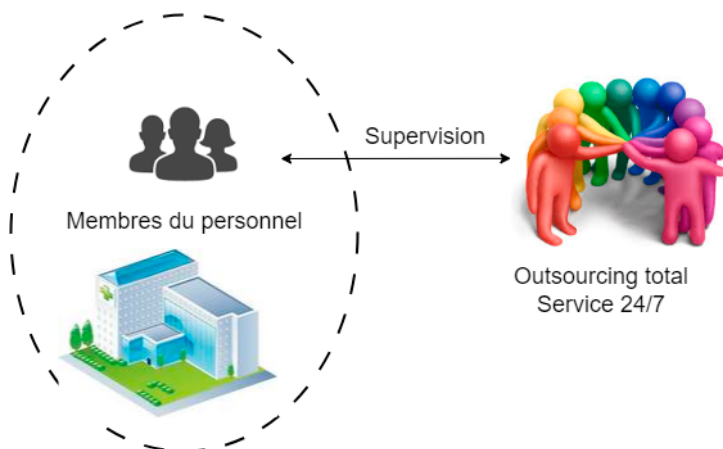


FIGURE 2.35 – Modèle externe

- le partage des responsabilités ;
- l'information sensible (qu'accepte-t-on de partager sur son système?) ;
- la localisation géographique ;
- le choix (ou non) de maintenir un minimum de compétences internes.

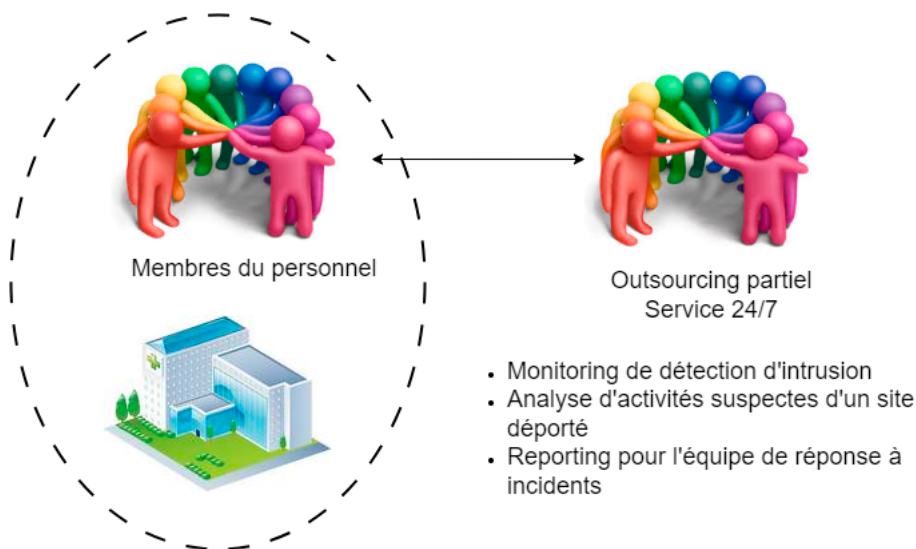


FIGURE 2.36 – Modèle mixte

Les compétences

Les compétences techniques sont nécessaires, concernant notamment :

- la connaissance des systèmes et des applications ;
- la connaissance du réseau et des équipements ;
- l'expertise (connaissance techniques + expérience) des incidents de sécurité.

D'autres compétences doivent être ajoutées (voir figure 2.37) :

- un représentant de la direction, pour assumer les décisions ;
- un juriste : si le risque juridique existe (malveillance interne, atteinte aux données personnelles par ex.)
- les ressources humaines : notamment en cas de malveillance interne ;
- la communication ;

Dans le cas des systèmes industriels, la présence d'un responsable sûreté est nécessaire.

Ces compétences existent en interne ou pas. Les services juridiques des entreprises sont le plus souvent destinés à sécuriser les contrats, pas pour intervenir sur des problèmes de cybercriminalité. Une compétence juridique externe plus appropriée sera sans doute nécessaire.

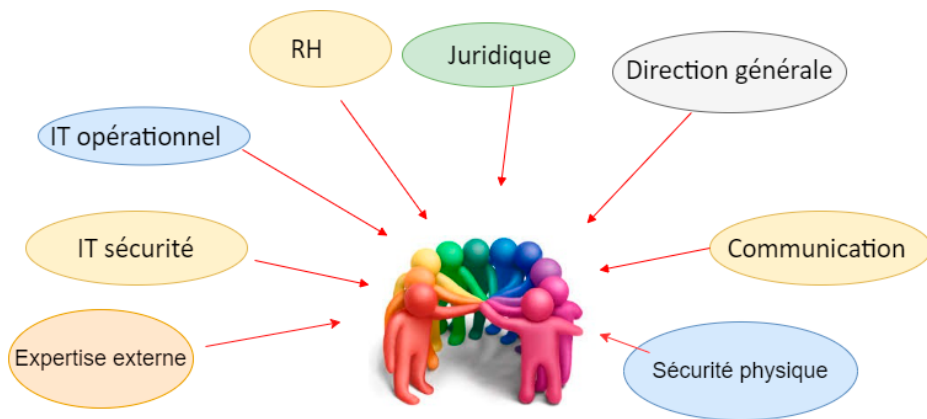


FIGURE 2.37 – Compétences associées

2.7.6 Le processus de traitement

L'enchaînement des activités

Le processus de traitement des incidents comprend plusieurs séquences ou activités, exécutées de façon séquentielle, dont la figure 2.38 donne la forme générique.

Ces activités correspondent à l'enchaînement logique de 3 étapes à franchir avant clôture de l'incident :

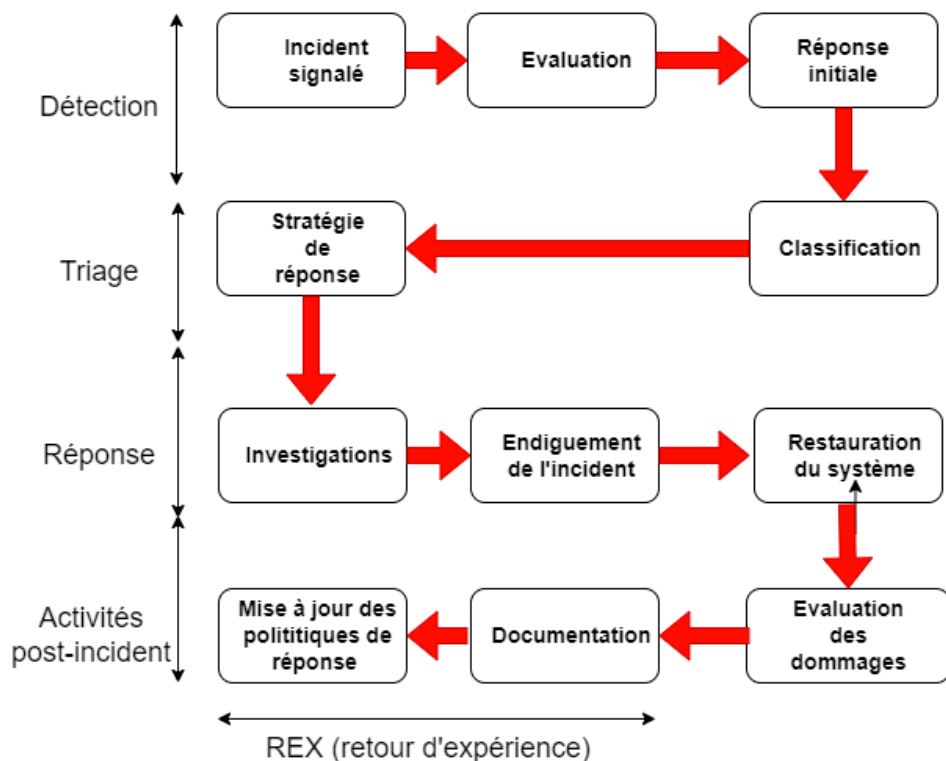


FIGURE 2.38 – Le processus de traitement des incidents

- le signalement et la détection dont le but est d'apporter le plus d'éléments ;
- le triage dont le but est (comme dans un service des urgences hospitalières) d'établir un diagnostic avant de décider du mode de réponse approprié ;
- la réponse proprement dite, jusqu'à la remise en service du système.

Si l'incident est de niveau 2, un retour d'expérience (RETEX) est nécessaire.

Détection / signalement

L'incident peut être détecté au niveau de l'utilisateur et au niveau de la supervision du système et (s'il existe) au niveau du système de surveillance. L'ensemble de ces données formelles (données techniques) ou non (observations) doit permettre d'évaluer la nature de l'incident, ainsi que le résume la figure 2.39.

L'évaluation

L'évaluation consiste à collecter, analyser, documenter l'incident en cours afin d'établir un diagnostic (figure 2.40).



- Alarme IDS/ FW
- Défacement site web
- Tentative infructueuse de login /pw
- Corruption / Destruction de données
- Crashes système suspects
- Tentatives de phishing
- Alertes antivirus
- Activité inhabituelle ou suspecte

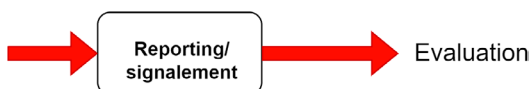


FIGURE 2.39 – Étape 1 : détection

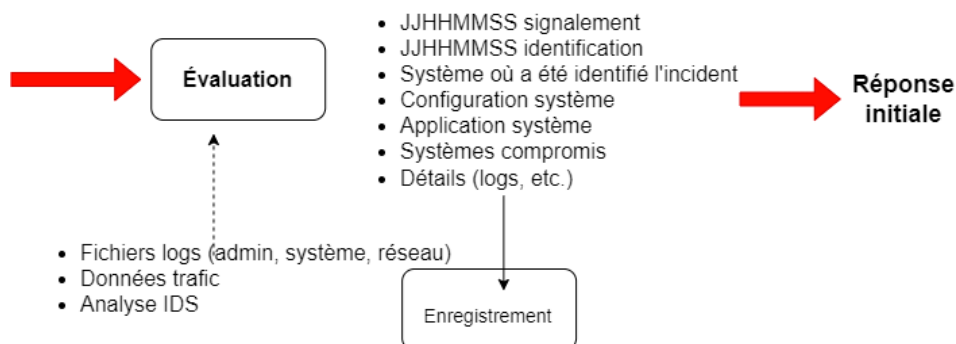


FIGURE 2.40 – Étape 2 : évaluation

Réponse initiale/ classification

Cette étape est cruciale pour décider de la suite à donner. Elle consiste non seulement à qualifier l'incident en cours mais aussi l'état du système, c'est-à-dire identifier les équipements et les services compromis, les données concernées, l'étendue et la propagation de l'incident en cours. Le résultat est un diagnostic fait au niveau technique sur l'incident et son niveau de sévérité (voir figure 2.41).

Il ne faut jamais perdre de vue que de nombreux signalements peuvent arriver en même temps (d'où la comparaison avec un service d'urgence) et qu'il faut définir des priorités, ce qui veut dire mettre en attente. Tous les incidents ne nécessitent pas le déroulement complet de la procédure (heureusement !). Un incident classé 0 n'ira pas plus loin. Un incident classé 1 sera sans doute traité d'un simple point de vue technique.

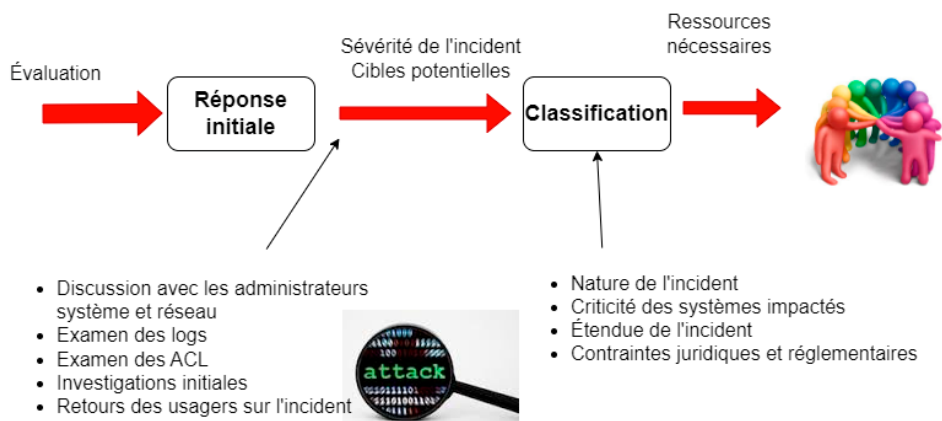


FIGURE 2.41 – Étape 3 : Réponse initiale et étape 4 : Classification

Stratégie de réponse

Pour les incidents les plus graves (classés 2), une stratégie de réponse doit être définie pour décider de la suite à donner, des compétences requises dans l'équipe de réponse à mettre en place. Que faut-il communiquer ? Comment ? Faut-il porter plainte ? Pour cela plusieurs points de vue sont nécessaires : direction générale, juridique, technique (voir figure 2.42).

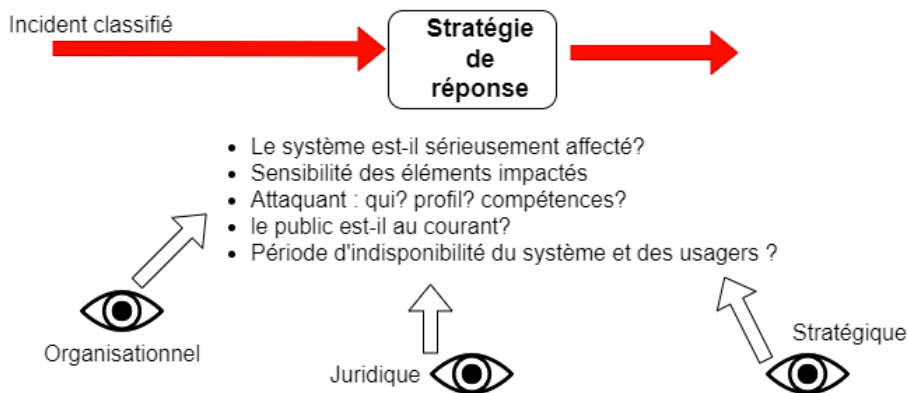


FIGURE 2.42 – Étape 5 : Stratégie de réponse

Investigations

Les investigations constituent une étape à double sortie. Elles consistent à relever des traces de l'incident sur la base des logs réseau, système, système de surveillance (ne pas oublier que les logs comportent des marques temporelles) afin

de reconstituer la chronologie des événements. D'un côté on cherche à reconstituer le scénario d'attaque afin de comprendre quelles vulnérabilités ont été exploitées (point de vue SSI). D'un autre côté on cherche des traces pour confondre des coupables (point de vue de l'enquêteur). De plus en plus souvent les entreprises mènent leur propre enquête (le coupable est peut-être en interne). Elles utilisent parfois les mêmes outils d'investigation (analyse de disque dur) que les enquêteurs officiers de police judiciaire.

Dans tous les cas, l'investigation doit précéder la remise en état du système car celle-ci va effacer les traces. Éteindre un PC revient à effacer les traces en mémoire vive (RAM) et empêche l'analyse de la machine en fonctionnement (*live forensic*). Le remettre en état revient à effacer des fichiers de logs sur le disque dur (*analyse post mortem*). Toute empreinte numérique analysée est en fait une copie. S'il veut que cette empreinte constitue un élément de preuve alors pour satisfaire à la norme ISO 27037 (lignes directrices pour l'identification, la collecte, l'acquisition et la préservation de preuves), l'enquêteur doit garantir qu'il n'y a pas rupture de la chaîne d'intégrité entre le point A (scène de crime) et le point B (puis le point C, etc.) La garantie d'intégrité nécessite l'utilisation d'une technique de hachage pour les fichiers transportés.

L'investigation se décompose en 3 parties (figure 2.43) :

- le recensement des sources : typiquement les logs système, réseau, IDS ;
- la collecte (copies) ;
- l'analyse.

L'entreprise doit fournir des éléments :

- à l'ANSSI si elle est OIV (elle a obligation de signaler l'incident dont elle est victime) ;
- aux enquêteurs (officiers de police judiciaire) s'il elle a décidé de porter plainte ;
- à son prestataire de réponse à incident CSIRT (*Computer Security Incident Response Team*), si elle en a un (voir plus loin).

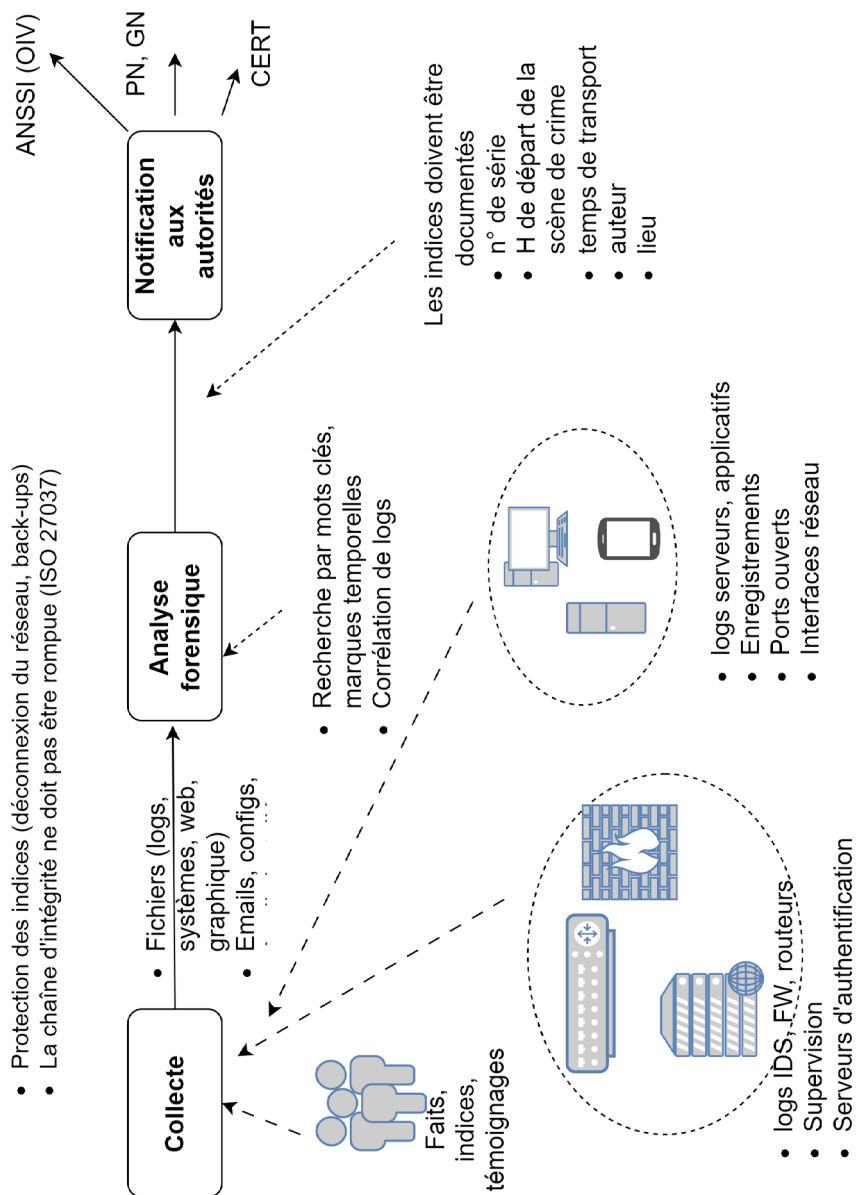


FIGURE 2.43 – Étape 6 : Investigations

Stratégie d'endiguement

L'endiguement correspond aux mesures techniques prises pour arrêter la propagation de l'incident.

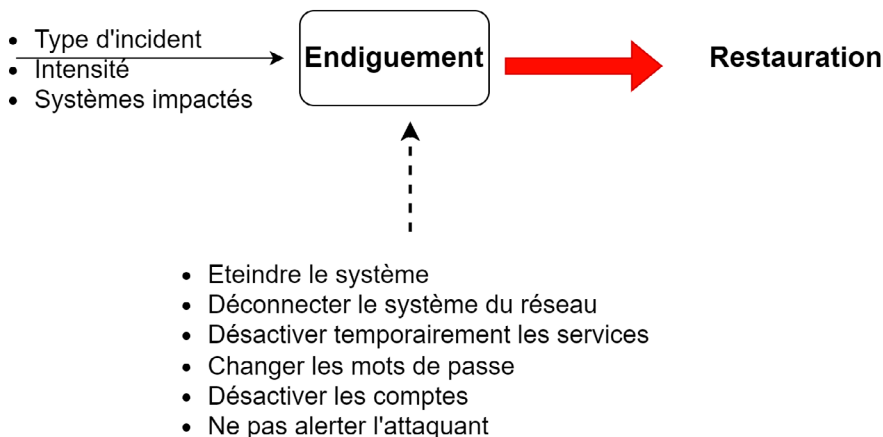


FIGURE 2.44 – Étape 7 : Endiguement

Restauration du système

La remise en état du SI est la finalité première.

Comment garantir de son efficacité ? Des mesures préventives s'imposent. La première est d'avoir une politique de sauvegarde sécurisée, qui permette en cas d'incident de restaurer les données. La seconde est de disposer d'une image "système" des postes de travail (sur ce point le cloud offre une solution qui permet de gagner du temps).

Comment procéder ? Chaque poste remis en état ne peut pas être reconnecté au SI (il risque d'être à nouveau infecté !). La solution est de définir une DMZ dans laquelle seront remises une à une toutes les machines une fois remises en état. La procédure peut-être longue, fonction du nombre de machines, mais elle donne des garanties.

Activités post-incident

Il s'agit ici de tirer les conséquences de ce qui s'est passé (figure 2.46) : évaluer les dommages, corriger les vulnérabilités exploitées, documenter l'incident (le rapport doit être synthétique et compréhensible par le plus grand nombre), évaluer la procédure de réponse telle qu'elle s'est déroulée afin d'améliorer son efficacité.

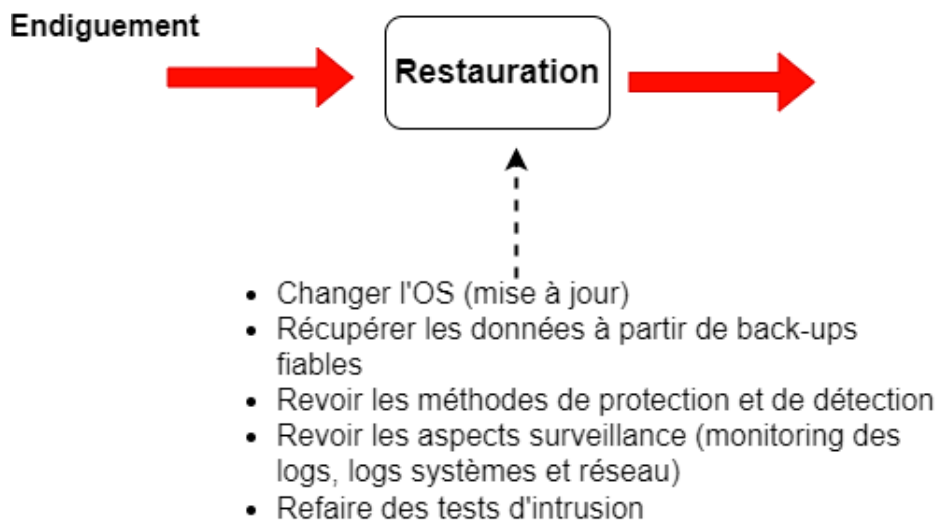


FIGURE 2.45 – Étape 8 : Remise en état du système

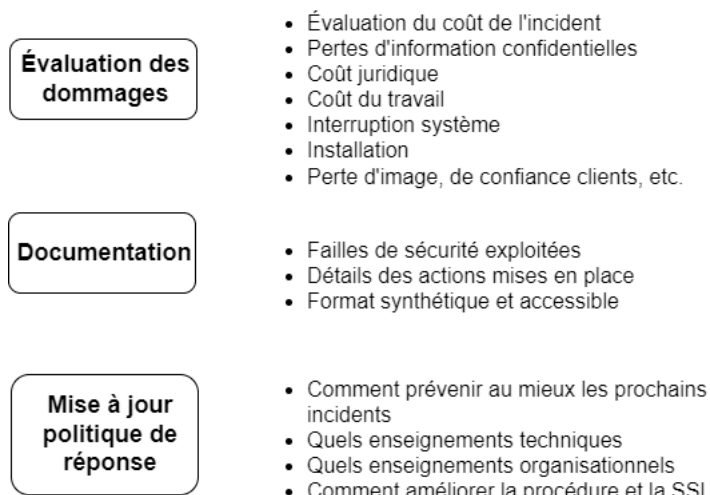


FIGURE 2.46 – Les activités post-incident

Les 4 phases de la réponse à incident

La réponse à incident comporte 4 phases, impliquant différentes compétences (figure 2.47).

— décision : étapes 5 et 11 ;

- communication : étapes 5 et 10 ;
- technique : étapes 1, 2, 3, 4, 6, 7, 8, 9 ;
- RETEX : étapes 10 et 11.

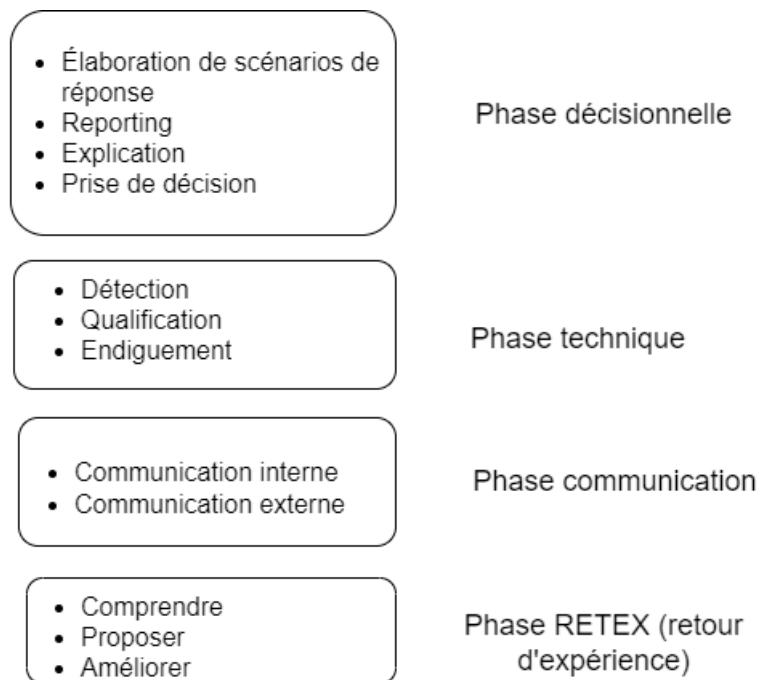


FIGURE 2.47 – Les 4 phases de la réponse à incident

Traitement *vs* gestion des incidents

La procédure de traitement des incidents s'inscrit de façon plus large dans la gestion des incidents, comme le montre la figure 2.48. Elle en constitue la partie réactive activée en cas d'incident grave.

La gestion des incidents peut être définie sous forme d'un cycle, qui intègre aussi des aspects préventifs (avant incident) et post-incident, comme le montre la figure 2.49.

Tout incident grave (et donc toute procédure de traitement) doit faire l'objet d'un retour d'expérience qui peut ensuite être exploité pour améliorer à la fois le niveau de protection mais aussi le déroulement même de la procédure de traitement.

La partie proactive de la gestion des incidents est constituée de tous les services support qui permettent d'améliorer les aspects détection et protection (voir figure 2.50). Cela concerne à la fois les outils de sécurité (conception, déploiement, configurations, tests) mais aussi les menaces (veille, détection).

La partie services de gestion de la sécurité est constituée de l'ensemble des actions

qui participent des missions récurrentes de sécurité. L'état de la menace et l'état du système évoluent en permanence, et obligent à mettre à jour les dispositifs de réponse et à les tester.

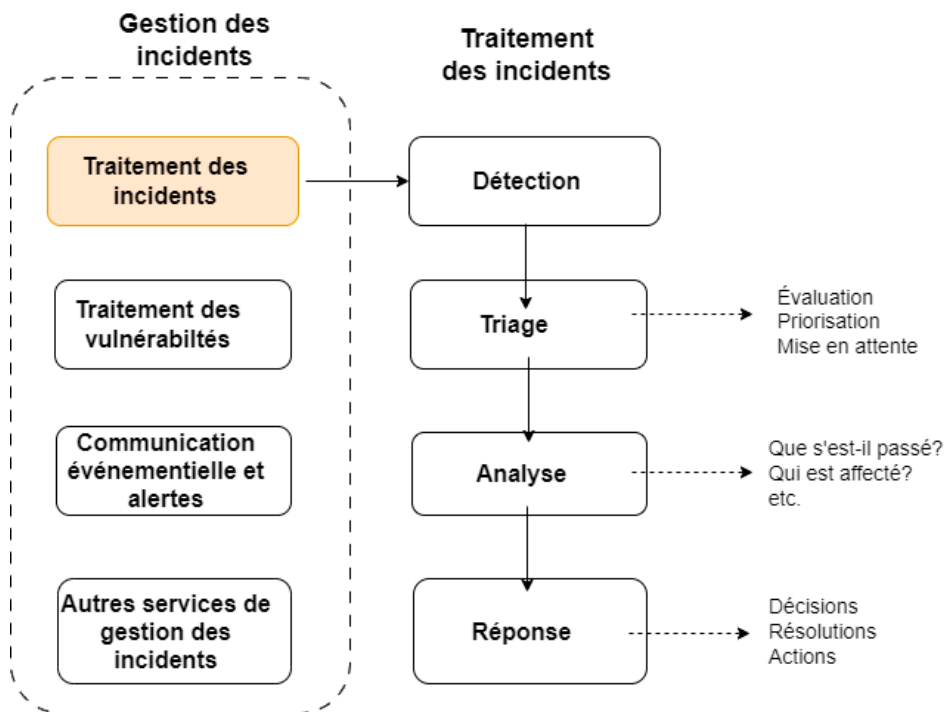


FIGURE 2.48 – Réponse *vs* gestion des incidents

Tout ce qui relève de la veille, que ce soit la veille technologique, la veille sur la menace, les échanges d'informations entre services de traitement des incidents, les bulletins d'alerte, tout cela participe d'une meilleure préparation à affronter des incidents de sécurité. Il faut aussi mentionner les actions et documents annexes déjà cités précédemment et qui font partie des missions de la SSI :

- le plan de secours, plan de continuité (qui doit être testé) ;
- les rapports d'audit des vulnérabilités ;
- les analyses de risques ;
- la sensibilisation des usagers au risque cyber ;
- la formation continue en général pour les personnels dédiés à la cyber-sécurité.

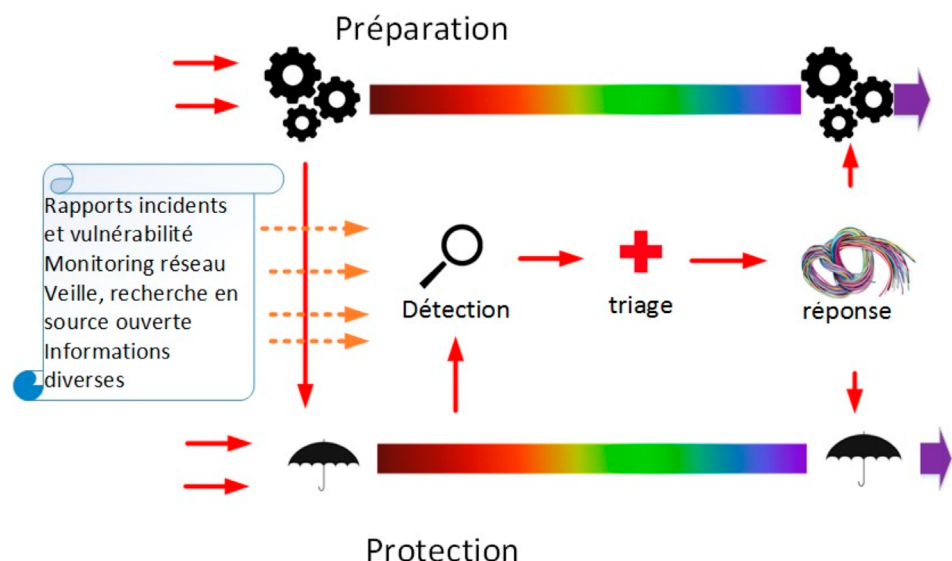


FIGURE 2.49 – Le cycle de gestion des incidents

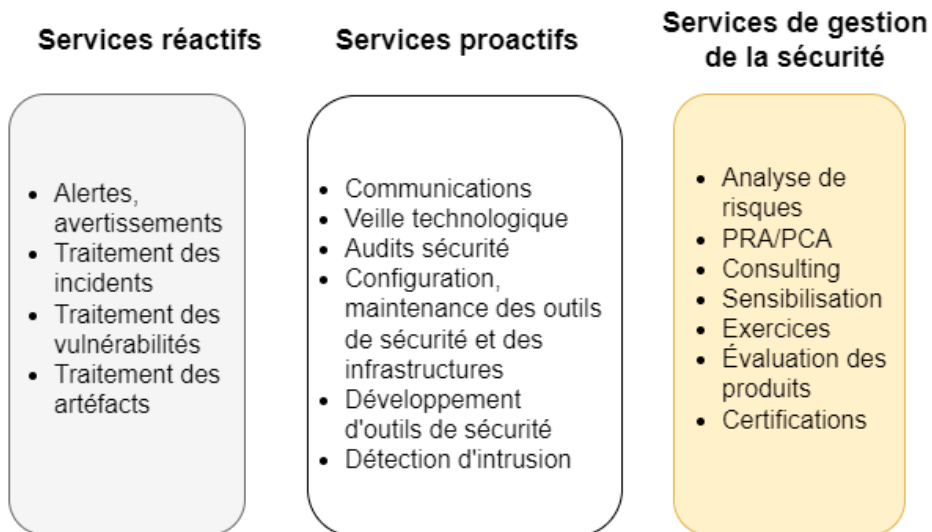


FIGURE 2.50 – Services de gestion des incidents

2.7.7 Le SIEM (*Security Information and Event Management*)

Architecture

Le SIEM est un dispositif plus ou moins réparti (selon la taille du système à surveiller) qui collecte les traces ou logs, les formate, les analyse, génère (ou non) une alerte sur la base de règles. La figure 2.51 en présente l'architecture générale.

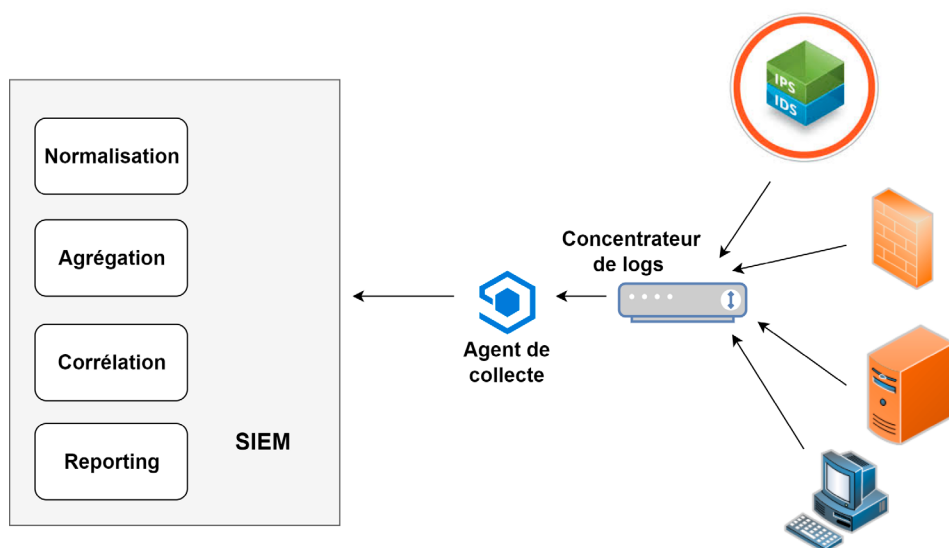


FIGURE 2.51 – SIEM : architecture générale

Un log est l'enregistrement d'un événement (sous forme d'une structure de données et d'un marqueur temporel) spécifique d'une activité système, applicative, réseau. La suite chronologique de logs constitue des journaux de logs, suite d'événements relatifs au système. Rappelons les sources des logs :

- les sondes de détection et de prévention d'intrusion (IDS/IPS) ;
- les équipements réseau (routeurs, pare-feux, commutateurs) ;
- les serveurs d'authentification ;
- les applications (bases de données, serveurs web, informations de comptes, requêtes/ réponses, utilisation des ressources) ;
- les systèmes d'exploitation (clients, serveur) ;
- les systèmes d'accès physiques (badges, caméra, sécurité incendie).

L'information résultante contenue dans ces journaux constitue des données de haute criticité, ce qui oblige à leur appliquer des mesures de sécurité (protection, accès) particulières. La quantité de logs générés par jour est considérable (plusieurs téra-octets), c'est pourquoi les technologies du SIEM vont de plus en plus converger vers les technologies du Big Data, boîte à outils permettant de détecter dans une masse imposante de données des événements suspects voire anormaux :

- incident de sécurité ;
- violation de la politique de sécurité (PSSI) ;
- activité frauduleuse ;
- perte de fonctionnalité (disponibilité) de certaines ressources.

Le processus de gestion des logs est à la base de la supervision de la sécurité (ou surveillance).

Les fonctions

Elle sont présentées à la figure 2.52.

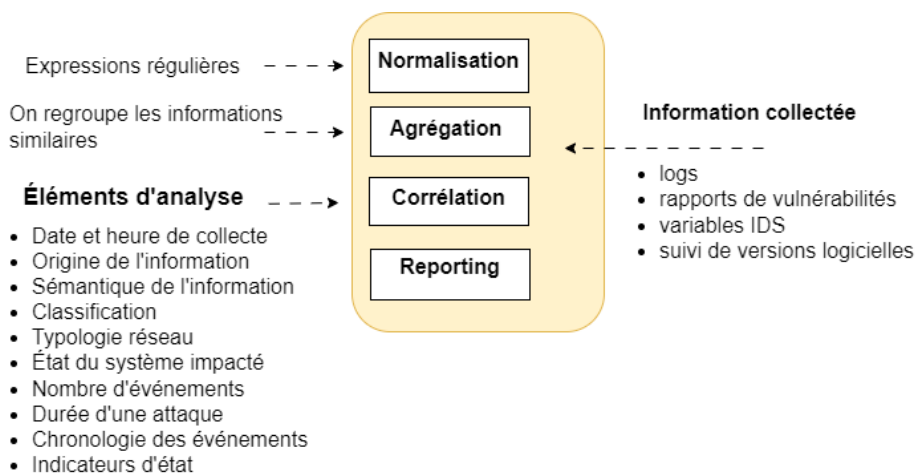


FIGURE 2.52 – SIEM : les fonctions

Les logs sont collectés par un système de centralisation appelé Syslog. Les sources sont diverses, les formats aussi, il convient avant analyse de leur donner un format unique. C'est le rôle des expressions régulières, pour automatiser ce traitement. On désigne sous le terme corrélation le cœur de l'analyse proprement dite. Corréler des événements suppose de chercher des correspondances entre eux, des relations de cause à effet.

L'analyse utilise différentes techniques :

- filtrage des doublons : les multiples signalements d'un même incident ;
- analyse contextuelle : recherche de messages caractéristiques d'une tentative d'intrusion ;
- analyse temporelle : désignée souvent sous le terme de corrélation ;
- analyse fonctionnelle : criticité de l'attaque, vulnérabilité de la cible ;
- analyse comportementale : par rapport à la politique de sécurité.

Le facteur temps est primordial, surtout si on cherche à détecter des attaques furtives, ce qui suppose d'analyser sur le temps long, ce qui par voie de conséquence consomme beaucoup de données, alourdit les traitements et dégrade la réactivité. Sans parler des faux positifs et des faux négatifs possibles.

Évolutions technologiques

Le SIEM correspond à automatiser les étapes 1 à 4 du processus de traitement des incidents. Pour beaucoup le SIEM est destiné à disparaître, remplacé par le Big Data (un big data orienté sécurité) compte tenu de la quantité croissante de données à traiter. On peut supposer que les techniques d'intelligence artificielle apporteront une valeur ajoutée intéressante notamment au niveau de l'analyse contextuelle.

2.8 Les services de réponse à incident

2.8.1 Les CERT (ou CSIRT)

Les CERT (*Computer Emergency Response Team*), acronyme très utilisé bien qu'il s'agisse d'une marque (déposée par l'université Carnegie Mellon), le terme CSIRT (*Computer Security Incident Response Team*) est équivalent, désigne un service d'expertise chargée de réagir en cas d'incident, d'apporter son soutien en terme de diagnostic, de coordination des administrateurs et compétence de sécurité sur place. Les CERTs sont publics ou privés, ils peuvent appartenir à l'État, à des administrations, à des entreprises. En France le CERT-FR est opéré par l'ANSSI et son périmètre est celui des administrations et des OIV. Le CERT-IST est le CERT des entreprises (industrie, services, tertiaire). Le CERT Renater opère sur le réseau du même nom, au service de la communauté Éducation-Recherche. Le rôle d'un CERT est à la fois préventif et curatif :

- centraliser les demandes d'assistance, analyser les symptômes ;
- faire une analyse permettant de définir la réponse à apporter ;
- faire un travail de veille sur les différentes menaces ;
- informer de façon préventive sur ces menaces et les précautions à prendre pour minimiser les risques ;
- partager des informations avec d'autres CERTs de même niveau (entreprise, national, international) et avec des opérateurs de l'internet (par une mise en réseau).

On trouve des CERTs au niveau des grands groupes : opérateurs télécoms, d'énergie, banques, transport. Il existe aussi des CERTs commerciaux qui proposent une prestation de service CERT à ses clients. En France les CERTs XMCO, Lexsi, Devoteam sont des exemples.

2.8.2 Les SOC

Les SOC (*Security Operation Center*) désignent des équipes de réponse à incident qui reçoivent les alertes d'un système de surveillance. Cela regroupe donc de la technologie et une équipe dédiée.

La partie technologique correspond en grande partie au système de détection, (en-core) appelé SIEM (*Security Information and Event Management*).

Procédure SOC

Le rôle du SOC n'est pas d'anticiper, il est d'analyser ce qui se passe. L'équipe SOC est structurée en 3 niveaux d'analyse (L1, L2, L3) selon le besoin. La procédure de traitement est résumée figure 2.53

L1 correspond à un incident qui ne dépasse pas la phase de triage et se contente d'une réponse simple avant clôture si le type d'incident est connu. S'il ne l'est pas, L2 doit trouver une solution à mettre en œuvre. L3 est sollicité pour tester les solutions avec des outils de simulation. On voit donc que L1 travaille à temps contraint et que L3 travaille plus en tâche de fond pendant une procédure de résolution.

Évolutions, rôle de l'IA

L'apport de l'intelligence artificielle est attendu dans deux directions :

- la capacité d'analyse et d'inférence automatisée pour distinguer des comportements anormaux et les bloquer ;
- un périmètre élargi (potentiellement à plusieurs millions) de sources d'informations utilisables en permanence sur la menace : indicateurs de compromission, adresses IP, nom de domaines, URL etc. de manière à élargir le contexte de l'analyse.

2.8.3 Différences entre CERT et SOC

En pratique, les services proposés par les entreprises commerciales présentent un fort recouvrement d'activités entre CERT et SOC. Il existe néanmoins des différences entre services comme le montre le tableau 2.2. Seul le CERT est concerné par les aspects préventifs.

2.9 Exercices

- 1) Selon la définition du risque ($R = p * D$), le terme p caractérise :
 - (a) la cible ;
 - (b) la menace ;
 - (c) l'attaque ;
 - (d) les dommages.
- 2) Les éléments suivants constituent-ils des cyber-menaces ?
 - a) une campagne de phishing en cours ;
 - b) des sauvegardes faites sur des clés usb ;

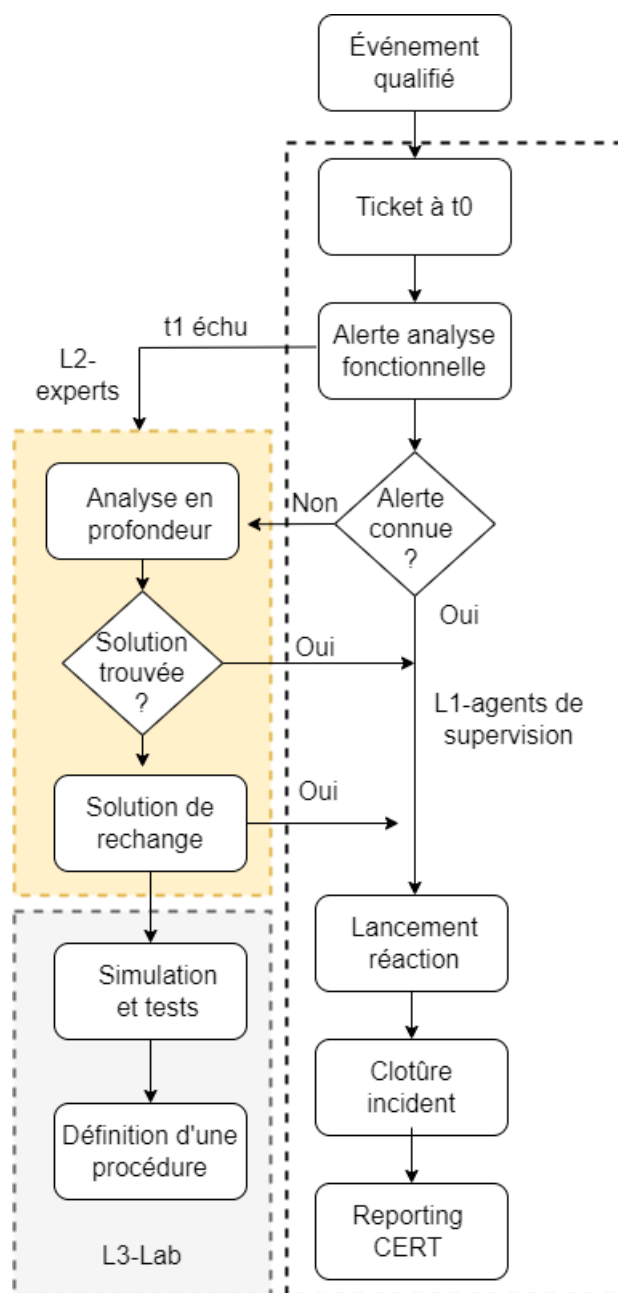


FIGURE 2.53 – Procédure SOC

Tâches	SOC	CERT
Gestion des vulnérabilités	XXX	XX (veille)
Collecte des logs	XXX	-
Gestion des règles de corrélation des logs	XXX	-
Génération d'alertes	XXX	-
Qualification de l'incident	XXX	XXX
Pilotage des contre-mesures	X	XXX
Remédiation technique	XXX	X(X) niveaux L2, L3
Clôture de l'incident	XXX	-
Gestion de cyber-crise	X	XXX
Veille sur la menace	-	XXX
Analyse post-mortem	-	XXX
Communication avec autres CERTs	-	XXX

TABLE 2.2 – SOC *vs* CERT

- c) les chevaux de Troie Trickbot et Emotet responsables de plus de 22 % des attaques de ransomware en France ;
d) l'utilisation massive d'outils de réunion en distanciel pendant le confinement.

3) Les éléments suivants constituent-ils des vecteurs d'attaque ?

- a) pièce jointe ;
- b) usurpation d'identité ;
- c) clé usb ;
- d) disque dur externe ;
- e) mot de passe faible.

4) Quels éléments constituent des cibles ?

- a) données personnelles ;
- b) compte administrateur ;
- c) serveur web ;
- d) pare-feu.

5) Les éléments suivants constituent-ils des vulnérabilités ?

- a) pièce jointe à un mail ;
- b) mot de passe faible ;
- c) faible perception du risque par l'utilisateur ;
- d) port non utilisé non désactivé.

6) Dans une stratégie de cyber-sécurité, les tests d'intrusion permettent d'identifier :

- a) les menaces ;
- b) les vulnérabilités ;
- c) les impacts ;
- d) les dommages.

7) Selon la définition du risque ($R = p * D$) on diminue le terme D :

- a) en diminuant la surface d'attaque ;
- b) en augmentant la capacité de détection ;
- c) en faisant une analyse de la menace ;
- d) par une politique de sauvegarde.

8) Selon la définition du risque ($R = p * D$) on diminue le terme p :

- a) en diminuant la surface d'attaque ;
- b) en augmentant la capacité de détection ;
- c) en faisant une analyse de la menace ;
- d) par une politique de sauvegarde.

9) Le facteur d'impact permet de quantifier :

- a) la menace ;
- b) les dommages potentiels ;
- c) le niveau de vulnérabilité.

10) Les éléments suivants sont-ils des incidents de cyber-sécurité ?

- a) phishing ;
- b) mot de passe faible ;
- c) crash de disque dur ;
- d) attaque DDoS.

11) S'il n'y a pas d'impact il n'y a pas de risque :

- a) vrai ;
- b) faux.

12) La matrice MITRE ATT&CK propose une modélisation :

- a) des cyber-menaces ;
- b) des cyber-attaques ;
- c) des vulnérabilités.

13) Un cheval de Troie permet de :

- a) faire une attaque de déni de service distribué (DDoS) ;
- b) chiffrer des données ;
- c) créer une porte dérobée ;
- d) se propager dans le réseau.

14) Quel(s) critère(s) DICP est (sont) impacté(s) par l'ex-filtration de données ?

- a) D b) I c) C d) P

15) Quel critère DICP est le plus important dans le cas des données médicales ?

16) Le but d'un audit de sécurité est de découvrir :

- a) les menaces ;

- b) les vulnérabilités ;
- c) les failles ;
- d) les impacts.

17) Un usager se connecte tous les jours entre midi et treize heures sur un site de cotation de matière première, ceci peut constituer :

- a) une faille ;
- b) une vulnérabilité ;
- c) une menace ;
- d) un risque.

18) Reconstituez le graphe relationnel entre : actifs, risques, menaces, vulnérabilités, dommages, impact, protection, processus métiers, exigences de sécurité.

19) Les quatre phases de la réponse à incidents sont :

- a) prévention ;
- b) communication ;
- c) restauration ;
- d) décision ;
- e) signalement ;
- f) retour d'expérience ;
- g) analyse ;
- h) technique.

20) Dans le processus de réponse à incident, la fonction de triage doit :

- a) clore l'incident ;
- b) endiguer l'incident ;
- c) évaluer l'incident ;
- d) analyser l'incident.

21) Dans le processus de traitement des incidents, quel est le bon ordre ?

- a) Analyse -> Détection -> Triage -> Réponse ;
- b) Réponse -> Triage -> Détection -> Analyse ;
- c) Détection -> Triage -> Analyse -> Réponse ;
- d) Détection -> Analyse -> Triage -> Réponse.

22) Un laboratoire pharmaceutique (fabrication et production de médicaments sous forme sèche) est victime d'une cyber-attaque. Des documents internes ont été diffusés, des machines et des fichiers ont été chiffrés. Aucune mention n'est faite officiellement sur le site de l'entreprise. Dans une équipe de réponse à incident, quels seraient les rôles les plus pertinents ?

- a) Un administrateur système ;
- b) Un responsable communication ;
- c) Un dirigeant ;
- d) Un DRH ;
- e) Un responsable sécurité ;
- f) Un responsable sûreté.

23) On relève sur plusieurs postes d'une entreprise une activité et des connexions inhabituelles. Il existe un seul accès au réseau public. L'architecture de l'entreprise est sécurisée via un pare-feu et un IDS Snort. Dans un tel cas quels peuvent être les signaux d'alerte ?

- a) Pas de connexion internet ;
- b) Pas de messagerie ;
- c) Activité inhabituelle sur le disque dur ;
- d) Trafic réseau inhabituel ;
- e) Détection d'intrusion.

24) Une PME est victime d'une cyber-attaque. Des documents internes ont été diffusés, des machines et des fichiers ont été chiffrés. Aucune mention n'est faite officiellement sur le site de l'entreprise. Dans un tel cas, quelles doivent être les mesures de première urgence ?

- a) Éteindre sa machine ;
- b) Débrancher sa machine du réseau ;
- c) Arrêter le site web ;
- d) Publier un communiqué.

25) Dans le cas précédent, que doit faire un usager qui constate une anomalie ?

- a) Éteindre sa machine ;
- b) Envoyer un mail à son responsable informatique ;
- c) Ne rien faire.

26) Après avoir collecté des traces numériques, l'enquêteur doit :

- a) en faire une copie ;
- b) les chiffrer ;
- c) en faire un hachage ;
- d) les transférer sur un serveur FTP (transfert de fichiers).

27) Un SIEM est constitué :

- a) d'un système de détection ;
- b) d'un système d'analyse de données ;
- c) d'une équipe de réponse à incidents.

28) Dans un SIEM il n'y a que de la technologie :

- a) vrai ;
- b) faux.

29) Un système Syslog est un système :

- a) de traitement des logs ;
- b) de centralisation des logs ;
- c) de formatage des logs.

30) L'analyse « live forensics » permet d'analyser :

- a) un système éteint ;
- b) les flux réseaux en temps réel ;
- c) le cloud ;
- d) un système en fonctionnement.

31) Étude de cas 1.

La filiale commerciale d'une société nationale de transport est victime d'un *ransomware* qui impacte un serveur de comptes clients. L'entreprise dispose d'un CERT (*Computer Emergency Response Team*). On soupçonne que le malware a pénétré le système via un poste client pour remonter vers le serveur, qu'il a été introduit via une macro dans un fichier word ou bien un mail frauduleux ou encore via une connexion sur un site douteux. L'entreprise soupçonne une société de maintenance avec laquelle elle est en conflit. Elle décide de faire une enquête *Open Source Intelligence* (OSINT) avec l'outil Maltego pour savoir si cette société n'a pas déjà été liée à de la cyber malveillance. Les premiers enquêteurs n'arrivent que 7 jours après les faits. Ils ne disposent que de l'image du serveur et du client. Ils procèdent à une analyse via l'outil Xways mais ne retrouvent pas tous les mails du poste client. Ils retrouvent le *crypto-locker* (key.exe), sa clé publique dans la base de registre ainsi que le texte du message réclamant une rançon de 7 bitcoins mais ils ne retrouvent pas le *crypto-loader*. Ils retrouvent les fichiers du compte client chiffrés ainsi que des dommages collatéraux sur les répertoires où il avait accès ainsi que dans un espace partagé. Ils constatent que l'entreprise a utilisé un certain nombre de logiciels de nettoyage avant leur arrivée. Ses antivirus ne sont pas à jour. Elle décide de ne pas payer la rançon mais n'a pas de sauvegarde pour restaurer ses données.

- a) Comment constitueriez-vous une équipe de réponse à incident (quels types de compétences et de responsabilités) ?
- b) Quels sont les indicateurs de compromission, à quel niveau, et quelles sont les mesures de premier niveau qui doivent être prises immédiatement et par qui ?
- c) Expliquez brièvement le rôle du CERT et à quelle étape il est censé intervenir.
- d) Précisez les actions que l'entreprise ne doit surtout pas faire si une enquête doit être menée.
- e) Qu'est-ce que le renseignement en source ouverte ?
- f) À titre de retour d'expérience utile, quel diagnostic tirez-vous de ce qui s'est passé, et quelles préconisations feriez-vous à l'entreprise en terme de i) protection, ii) gestion des incidents ?
- g) De l'exposé des faits, identifiez la menace, le risque, le vecteur d'attaque (scénario), la cible, l'impact.

32) Étude de cas 2.

Une entreprise spécialisée dans le support informatique est appelée en réponse à un client signalant une erreur sur son serveur de fichiers principal. Le support technique établit qu'il est plus facile de restaurer le serveur que de résoudre le

problème. Le serveur est restauré. L'incident se reproduit deux fois et la même méthodologie est suivie. La société d'assistance informatique commence à soupçonner que le problème n'est pas une faute technique, mais plutôt une attaque malveillante contre le serveur de fichiers. Une décision est prise de rechercher un soutien externe.

Une analyse en temps réel des données de trafic et l'examen des journaux d'activité du serveur de fichiers permettent d'établir un point d'entrée. Les informations pertinentes sont transmises aux forces de l'ordre. Le coupable est identifié comme un ancien employé mécontent de l'entreprise. Sa motivation est la vengeance de voir son contrat résilié.

Une analyse post-mortem de l'attaque révèle que la société n'avait pas de stratégie de sortie d'employé, de stratégie d'accès à distance ou de stratégie de gestion de mot de passe.

- a) De quel soutien (s) externe parle-t-on ?
- b) Qu'est ce qui a déclenché le recours aux forces de l'ordre ? Quelles sont-elles ?
- c) Où récupère t-on les données de trafic dont on parle ainsi que les journaux d'activité ?
- d) De quel point d'entrée parle-t-on ici ?
- e) Concernant le diagnostic établi, explicitez les mesures correctives concernant :
 - la stratégie de sortie d'un employé : organisationnelle, technique ;
 - l'accès à distance : pour qui ? pour quoi ? comment ?
 - la gestion des mots de passe : pour qui ? pour quoi ?

33) Étude de cas 3.

Une association dont le secteur d'activité est basé sur l'assistance médicale, a eu l'intégralité de ses fichiers chiffrés. Le seul fichier de logs dont disposent les enquêteurs (photocopie de mauvaise qualité) provient du routeur. Il a dû être ressaisi à la main pour une meilleure lisibilité par Notepad. L'attaque s'est produite le 16 juillet 2019 à 8 :48 :31. On relève la ligne suivante :

Tue, 2019-07-16, 08 :48 :31 - TCP Packet - Source :88.249.68.254, 2135 Destination : 192.168.2.1, 3389 - [DOS]

- le port 2135 permet d'obtenir des informations sur le serveur, et savoir notamment quelle version du système d'exploitation est installée, et quelles sont les mises à jour effectuées, afin de déterminer les failles potentielles ;
- le port 3389 (MS WBT Server) est le port d'écoute par défaut du protocole RDP, couramment utilisé pour accéder à des bureaux distants, accéder aux dossiers des serveurs, effectuer des impressions sur des imprimantes locales à partir de sessions distantes ;
- la mention [DOS] indique que nous sommes face à une attaque de type déni de service ;
- l'examen de l'adresse IP source 88.249.68.254 nous informe que cette dernière provient de Turquie, mais tout laisse à supposer qu'il s'agisse d'une adresse VPN pour brouiller les pistes.

Cette association disposait d'une architecture assez basique avec un routeur, un pare-feu, des serveurs publics (web, mail, VPN, DNS).

L'infogérance est externalisée auprès d'un prestataire. Pour son serveur d'activités elle utilisait une version Windows server 2008 R2 standard présentant notamment la vulnérabilité MS12-020 (vulnérabilité du protocole RDP), non corrigée malgré les recommandations du prestataire.

L'attaque s'est apparemment faite par intrusion sur ce serveur. On suppose que le réseau a au préalable été écouté (sniffé) par l'attaquant pour repérer si le port 3389 était ouvert.

Entre l'intrusion dans le réseau le 16 juillet 2019 à 08 :48 :31 et le début du chiffrement (modification des extensions des fichiers) des données le 16 juillet 2019 à 09 :44, il s'écoule 56 minutes. Cette durée pourrait correspondre au délai mis par le malware pour, dans un premier temps, procéder à la désactivation du VSS (*Volume Snapshot Service*) et des fonctions de restauration du système.

Les premiers dossiers sont chiffrés le 16 juillet à 9 :44 et le dernier à 11 :38, pour un total de 65 Go environ. Il faut rajouter 56 minutes pour rendre inopérants les points de restauration et sauvegarde.

À la racine de chaque répertoire chiffré se trouve un fichier texte "95f5i6m-readme.txt" et tous les fichiers chiffrés sont renommés avec l'extension complémentaire *.95f5i6m. C'est une des particularités du ransomware Sodinokibi : il chiffre les fichiers avec des extensions différentes totalement aléatoires sur chaque système attaqué, ainsi une victime possédant plusieurs systèmes en réseau, aura des chiffrements différents sur chacun d'eux. Le Groupement NTECH de la gendarmerie a d'abord été consulté avant d'être dessaisi par la section cybercriminalité du parquet de Paris en charge du ransomware Sodinobiki.

- a) Quels sont les indices de compromission de cet incident ? Les impacts ?
- b) Au moment où un écran apparaît réclamant une rançon, que doit faire la victime ?
- c) Les logs "réseau" mentionnent une attaque DOS, explicitez pourquoi ici.
- d) Précisez les actions à éviter si une enquête doit être menée.
- e) Quels sont les éléments d'information pour poser un diagnostic. Où et comment les récupérer ?
- f) Quels sont les risques pour le système au moment où ce diagnostic est posé et quelles sont les mesures de premières urgence à prendre ?
- g) Quels sont les étapes de traitement que vous préconisez ensuite :
 - objectifs ;
 - acteurs impliqués ;
 - mesures techniques.
- h) Au regard des faits, faites des propositions techniques et organisationnelles pour limiter le risque ransomware, en précisant pour chacune leur rôle en termes de détection, protection, limitation d'impact.

Chapitre 3



L'espace de confiance

La confiance repose sur des textes de référence (lois, règlements, normes, procédures), sur des acteurs au sens métier (ingénieurs, experts, enquêteurs, magistrats, auditeurs, développeurs) afin de contribuer à l'ordre et à la confiance dans le cyber-espace, avec différents champs d'action : former, protéger, enquêter, sanctionner. La figure 3.1 en présente un aperçu.

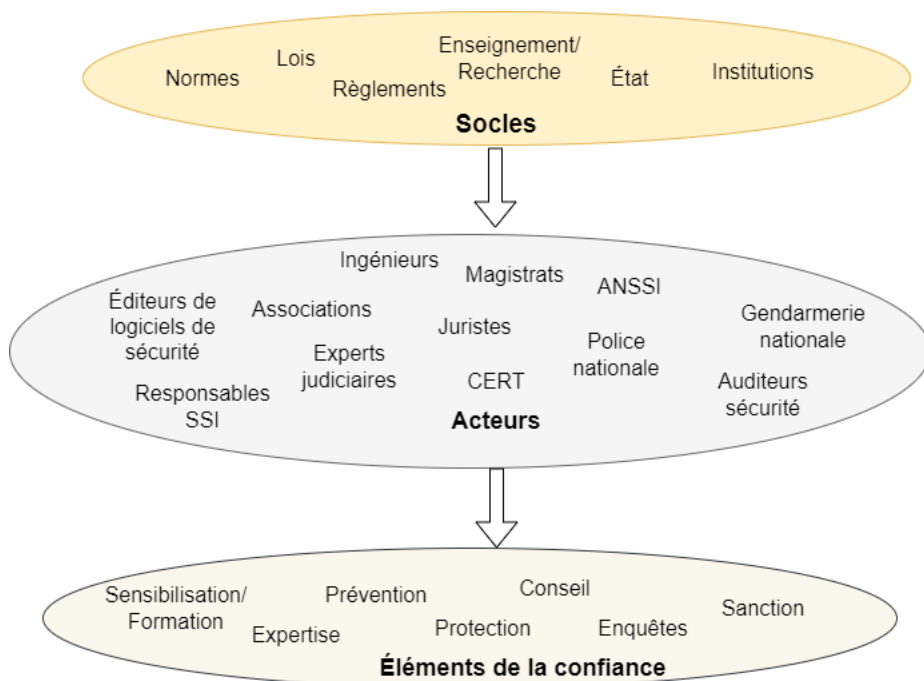


FIGURE 3.1 – Écosystème de la cyber sécurité

Les différents textes ne se situent pas au même niveau en termes d'obligation / sanction, la figure 3.2 situe ces différents niveaux.

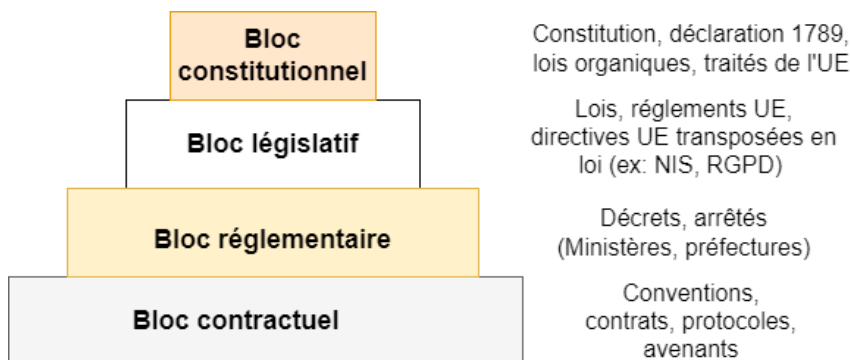


FIGURE 3.2 – Hiérarchie entre lois, obligations, règlements, standards

3.1 Les lois

La loi permet de définir un périmètre d'usages et donc de tracer la ligne rouge des infractions. Celles-ci peuvent donner lieu à plainte, jugement, condamnation. Les aspects juridiques sont une composante de la lutte contre la cybercriminalité.

3.1.1 Évolution des lois

Le périmètre des lois a évolué depuis le milieu des années 70 en fonction de l'évolution des technologies, des besoins, des menaces. Cette évolution s'est structurée en plusieurs phases, chacune correspondant à de nouvelles problématiques. La figure 3.3 résume ces différents jalons. Les listes présentées dans cette figure ne sont pas exhaustives mais permettent de voir les évolutions depuis les années 70. Les jalons apparus sont ainsi :

- la sécurité informatique ;
- la sécurité des SI ;
- la sécurité de l'information ;
- la cyber-sécurité ;
- la gouvernance des risques ;
- la cyberdéfense ;
- la protection des données personnelles.

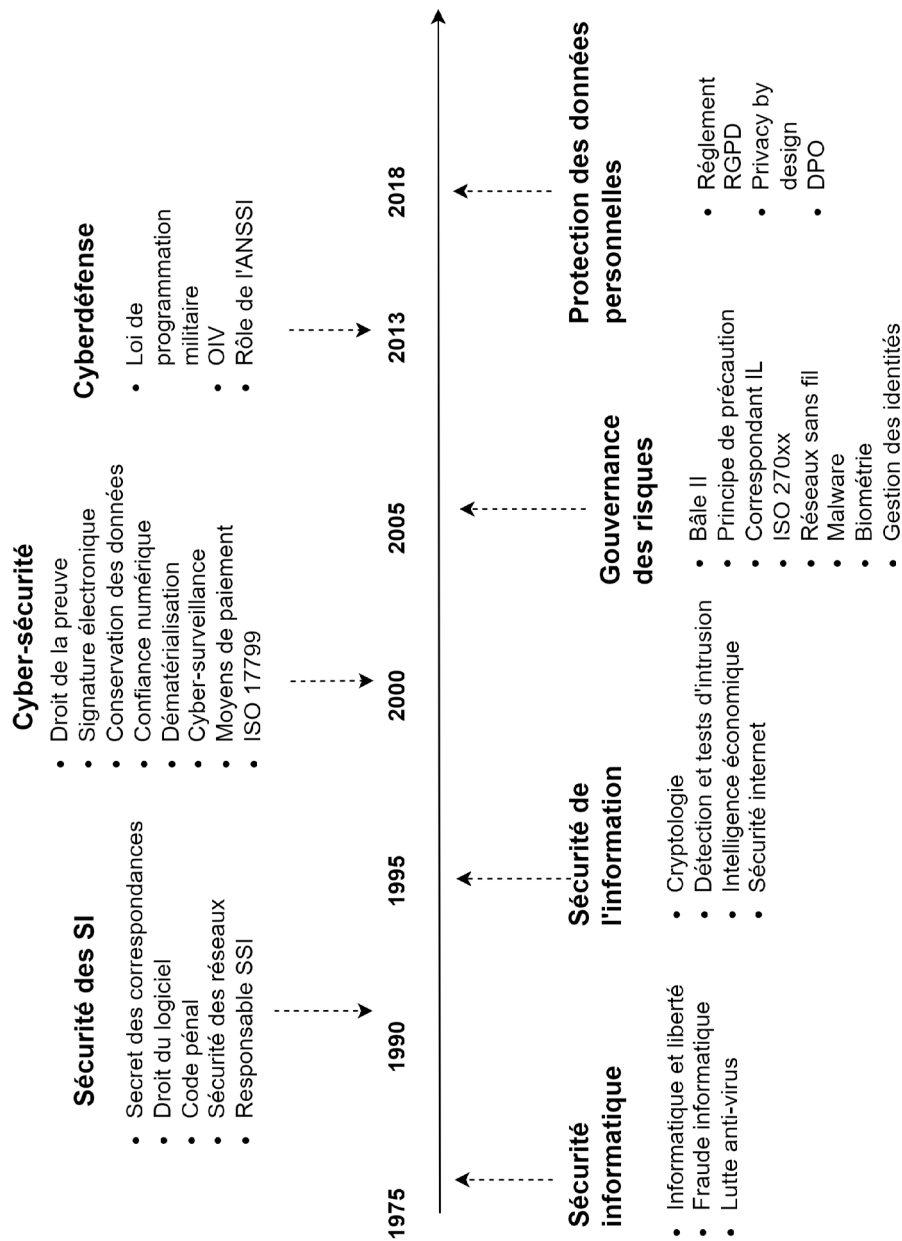


FIGURE 3.3 – Évolutions des lois et règlements

3.1.2 Loi informatique et libertés

C'est en France la loi fondatrice, apparue en janvier 1978, révisée en août 2004. Elle a été conçue pour protéger des risques d'utilisation abusive des données dites nominatives par l'administration. Celle-ci disposait en effet de moyens de stockage et de traitement des données des citoyens, pas le citoyen lui-même. Le risque perçu était celui du fichage centralisé. La notion de données personnelles apparaît en 2004. La loi s'accompagne de la création de la CNIL (Commission nationale informatique et liberté), chargée de surveiller de l'application de la loi en matière de traitement automatisé des données à caractère personnel.

Comme nous l'avons déjà mentionné au chapitre 1, toute information relative à une personne physique identifiée permettant de l'identifier soit directement, soit indirectement, par référence à un identifiant, ou par des éléments qui sont propres à la personne, constitue une donnée à caractère personnel. Pour la CNIL, une donnée personnelle est une donnée se rapportant à une personne physique. La liste n'est pas figée, depuis 1978 elle s'est élargie aux données numériques : adresse IP (même dynamique), numéro de badge individuel, photographie, empreinte digitale, enregistrement vidéo.

Les traitements concernés par les données personnelles incluent : la collecte, l'enregistrement, l'organisation, la conservation, l'adaptation ou la modification, l'extraction, la consultation, l'utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l'interconnexion, ainsi que le verrouillage, l'effacement ou la destruction.

3.1.3 Règlement général de la protection des données

Le RGPD [12] est un texte européen entré en application le 25 mai 2018. Il est destiné à encadrer le traitement des données personnelles sur le territoire européen. Avant 2018, les entreprises devaient déclarer à la CNIL les traitements effectués sur les données personnelles. C'était le rôle du CIL (correspondant informatique et liberté). Ces traitements sont souvent génériques (tout les traitements relatifs aux ressources humaines par ex.) et font l'objet d'une procédure déclarative standardisée.

D'autres traitements plus spécifiques peuvent exister, comme par ex. ce qui relève de la cybersurveillance des activités des personnes au sein de l'entreprise.

En 2018, on passe d'un régime déclaratif à un régime réglementaire. Le RGPD oblige les entreprises et administrations à mettre en place des moyens de protection des données à caractère personnel et de pouvoir justifier qu'ils existent. Elle introduit aussi un pouvoir (consentement ou non) aux personnes concernées. La problématique n'est plus seulement juridique mais devient aussi technique et implique le responsable de la sécurité des systèmes d'information (RSSI). Le CIL est remplacé par le délégué à la protection des données (DPO, *Data Protection Officer*) avec un rôle et des compétences accrues. La présence d'un DPO est obligatoire, qu'il soit salarié de l'entreprise ou prestataire de ce type de service, pour :

- gérer les incidents de sécurité relatifs aux traitements ;
- notifier les violations de données personnelles ;
- veiller à l'actualisation des traitements et des formalités vis-à-vis de la CNIL.

Le sujet peut être complexe. Les traitements n'ont pas forcément un caractère statique et générique. L'entreprise doit se poser diverses questions notamment en phase projet. Le projet implique-t-il un traitement des données personnelles ? Si oui quels traitements sont concernés ? Quel est le responsable ? Quelles sont les données éventuellement sensibles ? Quel est l'interlocuteur pour chaque traitement ?

À partir de là il faut :

- déterminer les finalités de ces traitements ;
- fixer les durées de conservation ;
- identifier les catégories de destinataires ;
- s'assurer des mesures de sécurité de ces données ;
- identifier les éventuels sous-traitants qui interviennent et définir un cadre contractuel sur le sujet ;
- identifier les transferts de données personnelles hors UE ;
- informer les personnes concernées et obtenir leur consentement ;
- remplir les formalités avec la CNIL ;
- gérer les demandes des personnes concernées : accès, rectification, suppression, opposition.

La notion d'anonymisation est ici importante. Il s'agit d'un traitement sur des données personnelles destiné à empêcher d'identifier la personne et ce de façon irréversible. Attention : ne pas confondre avec la pseudonymisation, qui consiste à remplacer un attribut par un autre, ce qui n'empêche pas l'identification de façon indirecte.

La CNIL a mis en ligne un outil PIA (*Personal Impact Analysis*) [13] permettant de faire une analyse d'impact relative à la protection des données personnelles, telle que prévue par le RGPD.

3.1.4 Loi Godfrain

La loi Godfrain de 1988 est la première loi qui s'attaque à la cybercriminalité en France. Cette loi introduit la notion clé de "Système de traitement automatisé des données (STAD)". Tout système disposant d'une capacité de traitement et de mémoire (même élémentaires) rentre dans cette catégorie, aujourd'hui : un serveur, un ordinateur, un smartphone, un auto-commutateur d'entreprise, mais aussi une carte à puce et même un tag RFID peut rentrer dans cette catégorie. Toute atteinte au bon fonctionnement d'un STAD relève de la cybercriminalité et donc du droit pénal.

3.1.5 La cyber-criminalité dans le code pénal

Le code pénal français dispose d'un certain nombre de lois relatives à la cybercriminalité qui peuvent se répartir en 3 types :

- T1) les actions portant atteintes aux systèmes (STAD) ;

- T2) l'utilisation des technologies numériques dans le cadre de la criminalité classique (atteintes aux services) ;
- T3) l'échange de contenus illicites : pédopornographie, trafics, harcèlement, incitation à la haine, au terrorisme.

Le premier volet est celui introduit par la loi Godfrain, tout ce qui porte atteinte aux systèmes d'information. La détection repose sur des moyens de surveillance des systèmes (essentiellement).

Le second volet concerne l'usage des technologies numériques pour réaliser crimes et délits. La détection repose sur la surveillance des procédures et des données associées (par ex. pour la fraude).

Le troisième volet porte sur les contenus. Dans ce cas la détection repose sur la surveillances des flux échangés (par ex. dans le dark web).

La figure 3.4 explicite d'avantage l'ensemble des actions malveillantes potentielles, concernant les systèmes, les services, les contenus. On voit que les cercles ne sont pas disjoints.

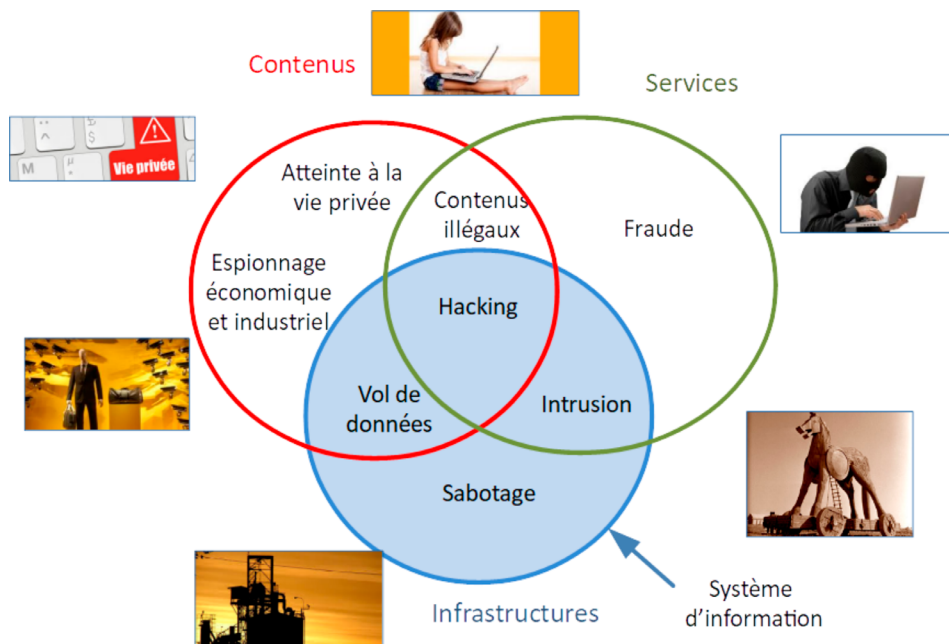


FIGURE 3.4 – Typologie de la cybercriminalité

3.1.6 Loi de confiance sur l'économie numérique - LCEN

L'extension du commerce électronique a conduit à légiférer en 2004 pour encadrer les transactions et ainsi créer un espace de confiance dans cette activité. La LCEN est une transposition d'une directive européenne sur le commerce électronique. La LCEN définit la notion de commerçant électronique, souligne la respon-

sabilité des hébergeurs, encadre la publicité par voie électronique et précise ce qui relève de l'intrusion dans les STAD dédiés à ces procédures.

3.1.7 Loi LOPSSI 2

La loi d'orientation et de programmation pour la performance de la sécurité intérieure de 2011 contient un volet relatif à la lutte contre la cyber-criminalité. Cela concerne :

- l'usurpation d'identité sur internet reconnue comme un délit
- le rôle des FAI pour le blocage des sites pédopornographiques, la constitution de listes noires de sites prohibés, le filtrage des adresses IP
- le rôle des forces de l'ordre : possibilité d'intrusion (via autorisation) dans des réseaux et les ordinateurs de suspects à des fins d'extraction de données dans le cadre d'enquêtes (crimes, trafic, blanchiment)

3.1.8 Loi de programmation militaire - LPM

Dans la loi de programmation militaire (depuis 2013) plusieurs articles concernent la protection des opérateurs d'importance vitale (OIV) contre les cyber-menaces. La LPM donne toute latitude aux services de l'état pour contrer les cyber-menaces. Nous sommes donc dans le cadre de la cyber-défense définie précédemment. La liste des OIV n'est pas publique. La figure 3.5 donne une idée de la répartition des acteurs selon les secteurs d'activité d'importance vitale (SAIV).

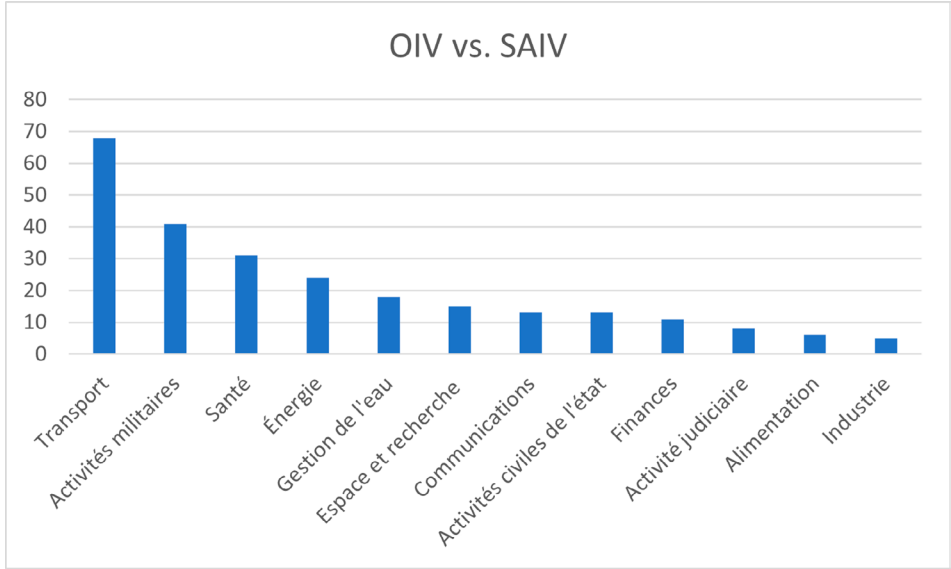


FIGURE 3.5 – OIV *vs* SAIV

La LPM renforce le rôle de l'ANSSI en terme de contrôle des niveaux de sécurité des OIV. Ceci concerne les obligations légales de ces OIV.

3.2 Les obligations légales

Les obligations légales s'appliquent à des secteurs d'activité particuliers (par ex. le secteur bancaire), à certains acteurs (les fournisseurs d'accès à internet (FAI), les hébergeurs (cloud), les OIV), à l'utilisation d'outils de sécurité comme la cryptographie, et enfin à toutes les entreprises pour ce qui concerne la conservation des données de connexion. Les obligations légales ont un rôle important pour renforcer la confiance comme le rappelle la figure 3.6.

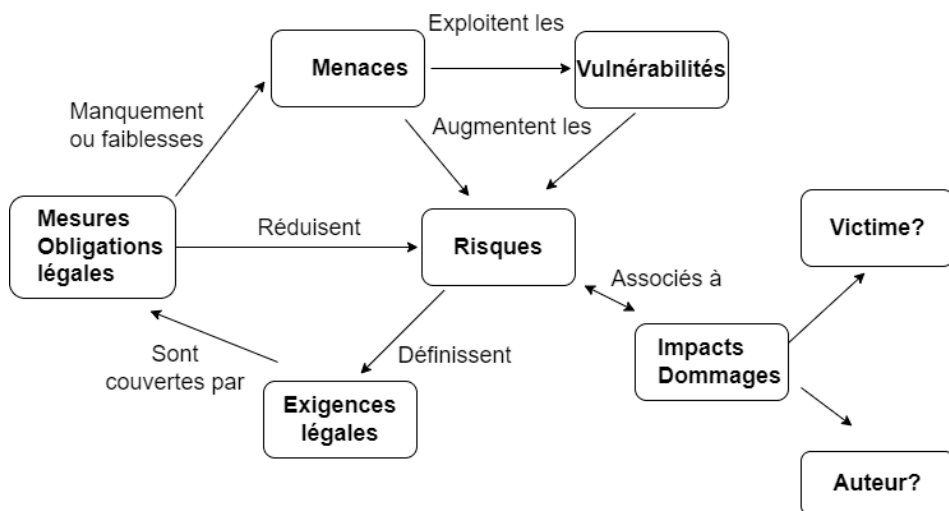


FIGURE 3.6 – Obligations légales

Plusieurs textes de référence définissent le cadre juridique des obligations : code civil, code pénal, loi informatique et liberté, code de la propriété intellectuelle, code du travail, code monétaire et financier, comme le montre la figure 3.7. Ces différentes sources ne constituent pas un cloisonnement du sujet mais pour un délit donné, des articles du code pénal s'appliqueront toujours, renforcés par d'autres plus spécifiques selon les domaines d'activités.

3.2.1 Conservation des données de connexion

Ceci concerne d'abord les opérateurs de télécommunications, les fournisseurs d'accès à internet, les hébergeurs. Pour des besoins de sécurité nationale, afin de lutter contre les menaces (niveau à réévaluer régulièrement), les données de connexion (internet, téléphonie) doivent être conservées pendant 1 an, afin de pouvoir les mettre à disposition en cas d'enquête, sur demande d'un magistrat. Depuis octobre 2021, trois décrets ont redéfini les règles. Cela concerne le type de données [14], les données de personnes ayant créé des contenus en ligne, le contexte de sécurité nationale (lutte contre le terrorisme). Les données concernées sont d'abord les adresses IP (le minimum). On peut y ajouter les données de trafic et de localisation (mais ceci doit être justifié et contrôlé juridiquement).

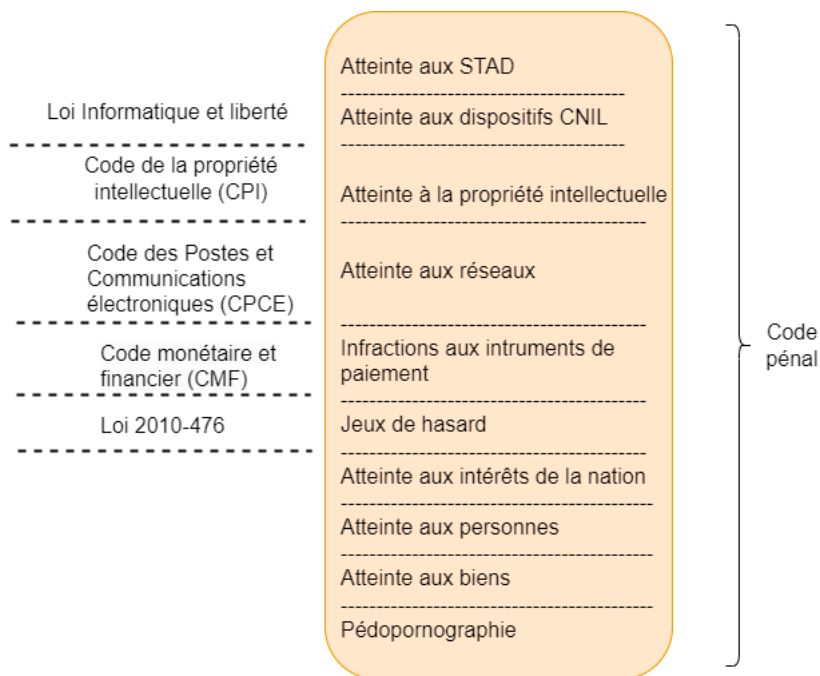


FIGURE 3.7 – Code pénal et autres règlements

S'ajoutent encore des données civiles des utilisateurs mais ceci est très contesté et doit être justifié par un niveau de menaces à évaluer.

Une question revient régulièrement. Les entreprises doivent-elles conserver elles-aussi des données de connexion ? Elles peuvent en effet être vues comme des fournisseurs d'accès pour ses employés et tous les visiteurs à qui elle donne un accès (même temporaire). À vrai dire elles n'y sont pas obligées, mais si elles devaient être victimes d'une cyber-attaque et si une enquête les concernaient, l'absence de données de connexion nuirait au résultat.

3.2.2 Utilisation de la cryptographie

L'article 30 de la LCEN a conduit à libéraliser l'utilisation de moyens de cryptographie (auparavant restreint et encadré). La fourniture, l'importation, l'exportation de moyens de cryptologie reste encadré et soumis à déclaration ou demande d'autorisation.

Il y a obligation pour toute personne ayant connaissance de la convention secrète de déchiffrement de remettre cette information aux autorités à des fins d'enquête (Code pénal art. 434-15-2).

Le juge peut demander à toute personne physique ou morale qualifiée de déchiffrer des données (Code de procédure pénale L230-1).

3.2.3 Cas du *cloud computing*

En matière d'obligations, il ne faut pas voir le Cloud Computing comme un transfert de responsabilité en terme de sécurité concernant notamment le stockage des données. C'est le responsable du traitement, et donc l'entreprise, qui reste responsable de la sécurité des données. Elle doit donc prendre toutes les précautions utiles au regard de la nature des données et des risques impactant les critères disponibilité, intégrité et confidentialité. Le fournisseur de service cloud doit donc donner des garanties via des audits externes et des certifications. Plusieurs questions se posent concernant les données :

- l'accès à des données sensibles qui sont externalisées ;
- la localisation des données (sont-elle en France ?) ;
- la confidentialité des données dans un environnement partagé ;
- la restauration de données après incident au niveau prestataire cloud ;
- l'investigation des services cloud dans un environnement partagé et fluctuant ;
- la visibilité à long terme des politiques de sécurité (qui peuvent changer suite à un rachat d'entreprise) ;
- l'homogénéité de la sécurité dans le cas d'hébergement multi-clouds (avec des niveaux de sécurité différents).

On se retrouve donc dans un problème de partage de responsabilités entre clients et fournisseur de service cloud. Comment le client peut être assuré du niveau de sécurité requis (par lui, pour ses besoins) ? Quels contrôles de sécurité doit-il mettre en place au-delà des contrôles inhérents à la plate-forme cloud ? Comment sa gestion de la sécurité d'entreprise doit intégrer celle du cloud ? Ceci dépend bien sûr du niveau de sensibilité des données concernées.

3.2.4 Les opérateurs d'importance vitale (OIV)

La notion d'OIV est apparue dans la LPM de 2013 [15]. Les OIV représentent plus de 200 opérateurs publics ou privés, qui se répartissent en 12 secteurs d'activité. Les OIV sont soumis à des obligations comme :

- de se soumettre à des audits de vulnérabilité ;
- de disposer d'un système de surveillance ;
- de déclarer à l'ANSSI les attaques dont ils sont victimes.

En retour l'ANSSI accompagne les OIV sur toutes les questions techniques et procédurales de cyber-sécurité.

Il va de soit que les niveaux d'exigence ne sont pas les mêmes selon les secteurs car les niveaux d'impact sont très différents. Par ex. entre le secteur bancaire et le domaine de la production d'énergie, dans le premier cas l'impact porte sur les services, dans le second il porte sur les activités économiques voire sur les atteintes aux biens et aux personnes en cas d'accident majeur. Les OIV sont ainsi classés en 3 niveaux avec des exigences croissantes.

3.2.5 Les établissements financiers

Cela comprend les métiers de la banque, de l'assurance, les sociétés de courtage, les sociétés de crédit bail, les investisseurs institutionnels. Ces métiers sont basés sur la confiance, et de fait très sensibles aux cyber-menaces, qui sont à la fois celles de toute entreprise mais aussi des menaces spécifiques à leurs métiers, dès lors qu'il est questions dans ces processus métiers de flux financiers. La figure 3.8 présente une cartographie des risques qui les concernent. Soit elles peuvent être mises en cause, soit elle sont victimes. Soit les délits relèvent des lois générales, soit d'obligations plus spécifiques (code monétaire et financier notamment).

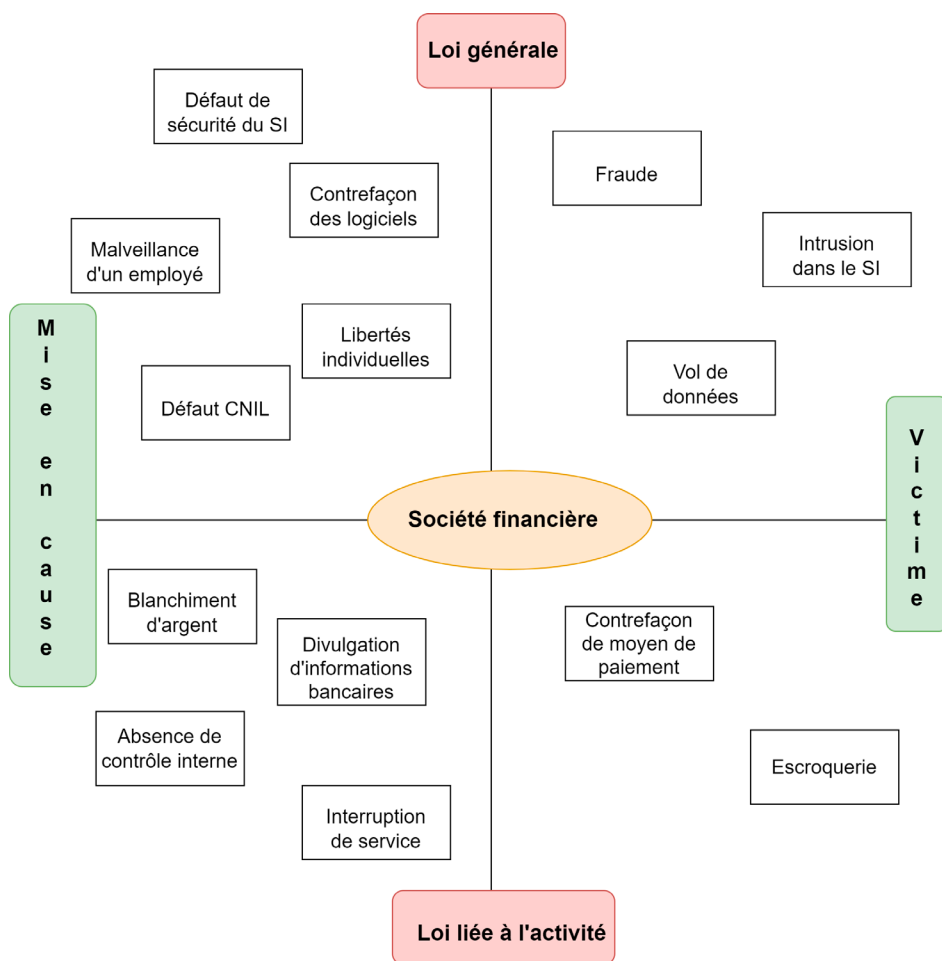


FIGURE 3.8 – Risques des établissements financiers

En plus de la loi, ces établissements sont soumis à des textes plus spécifiques comme le code monétaire et financier. Cela concerne les points suivants :

- le respect du secret bancaire ;

- l'obligation de se prémunir contre le blanchiment ;
- la déclaration d'incidents ;
- la déclaration de mouvements financiers suspects.

3.2.6 La directive européenne NIS

La directive *Network and Information Security* (NIS) constitue un dispositif de sécurité pour tous les opérateurs dits de service essentiel (OSE). Par rapport à la notion d'OIV vue précédemment, le périmètre des OSE est plus large : acteurs dont le service est essentiel au maintien de l'activité économique et sociale (grandes entreprises, établissements publics, importantes PME). Ce qui a été défini pour les OIV depuis la LPM de 2013 peut être réutilisé et transposé aux OSE. Plusieurs critères sont à prendre en compte pour être considéré comme OSE (taille, chiffre d'affaire, secteur prédéfini...) La liste des OSE doit être fournie par chaque état membre à la commission européenne. Les obligations pour les OSE sont [16] :

- avoir un représentant vis-à-vis de l'ANSSI ;
- garantir un socle minimal de cyber sécurité vis-à-vis des attaques aux conséquences graves sur le fonctionnement de l'économie et de la société ;
- être soumis à des contrôles de l'ANSSI ;
- déclarer à l'ANSSI les incidents de sécurité dont elles sont victimes.

Les obligations de sécurité concernent :

- la gouvernance : avoir une politique de sécurité, la mettre en œuvre, la faire homologuer ;
- la protection : sécurisation de l'infrastructure et des accès ;
- la détection : avoir un système de surveillance et une procédure de gestion des incidents ;
- la résilience : en cas de gestion de crise, en cas d'impacts majeurs.

La directive NIS2 a été votée par le parlement européen en novembre 2022. Chaque état membre doit transposer cette directive en droit national, ce qui en France devrait entrer en vigueur automne 2024.

NIS 2 élargit le nombre de secteurs socio-économiques concernés (de 19 à 35), ce qui aura pour effet de multiplier le nombre d'opérateurs de services essentiels (OSE). Par ex. les sous-traitants et les prestataires de service impliqués dans les infrastructures critiques le seront aussi. On se dirige vers une répartition des acteurs socio-économiques en deux entités : essentielles et importantes. La notion d'OIV pourrait se voir concurrencer (au niveau de l'ANSSI) sauf à considérer les OIV comme essentiels.

La directive NIS 2 étend surtout son pouvoir coercitif (obligations, sanctions). Les entreprises, sous-traitants, prestataires devront se soumettre à des audits de sécurité. Les sanctions concernent la non-coopération avec les autorités.

3.2.7 Politique de sécurité du système d'information (PSSI)

Toute entreprise ou organisation en général se doit de définir des enjeux stratégiques en matière de sécurité des systèmes d'information et de gestion des risques. La PSSI est le premier document qui formalise cette base stratégique. En fonction du domaine d'activité de l'organisation, de sa culture, on y explicite les menaces, les risques, les enjeux, les objectifs, les règles, les acteurs. On trouvera dans [17] un guide d'élaboration de PSSI. Cette PSSI globale est le premier document du système de management de la SSI (SMSI). Il peut ensuite se traduire en PSSI technique, voire se décliner en PSSI métier. Ce document qui émane de la direction doit être rédigé de manière compréhensible par tous. Il est rarement modifié (sauf oubli constaté suite à un incident grave de sécurité ou à l'apparition d'une nouvelle menace). La déclinaison technique de la PSSI globale concerne en premier lieu les règles de filtrage des flux, les droits d'accès aux ressources, ce qui plus concrètement concerne les équipements de sécurité réseau comme les pare-feux, ou encore le paramétrage d'un système centralisé d'identification/ authentification (ex. *Active Directory*, très présent en entreprise).

3.2.8 Charte informatique au sein de l'entreprise

Rôle

La Charte informatique permet de définir les conditions générales d'utilisation d'un système d'information au sein d'une organisation professionnelle (entreprise, administration). Elle sert à encadrer les employés au niveau de l'utilisation du matériel informatique mis à leur disposition. Elle permet d'assurer le maintien de plusieurs impératifs :

- garantir le niveau de sécurité du SI ;
- se prémunir du risque judiciaire (civil et pénal) en cas d'usage inapproprié de l'outil informatique de travail ;
- respecter la vie privée des salariés.

Contenu

La Charte informatique doit être intelligible et à la portée de tous. L'objectif est de sensibiliser les utilisateurs aux enjeux et aux risques. Les points à aborder sont les suivants :

- les règles d'utilisation du SI : internet, messagerie, rôle des responsables (directeur des SI, responsable SSI, administrateur réseau) ;
- les moyens de contrôle mis en place, en respectant les règles de loyauté, transparence, proportionnalité vis-à-vis des risques, respect de la vie privée, du secret des correspondances, de la protection des données à caractère personnel ;
- information sur les droits et obligations : en cas de contrevenance, de litige, accusation et défense doivent pouvoir se référer à la charte et à son contenu.

Mise en place

Avant de pouvoir être effective, la charte doit être soumise aux représentants du personnel, à l'inspection du travail. Un avis négatif n'empêche pas la mise en place de la charte, seule l'absence de consultation constitue un délit d'entrave (article L2328-1 du Code du travail). Pour que la charte puisse être validée, elle devra faire l'objet d'un dépôt au secrétariat-greffe du conseil des Prud'hommes. En dernier lieu, elle devra être affichée sur les lieux de travail. Afin d'appliquer d'éventuelles sanctions, elle devra être annexée au règlement intérieur de l'entreprise. Il faudra donc la diffuser auprès des salariés.

Droits et obligations des salariés

En principe, le salarié doit faire un usage personnel raisonnable de son poste de travail et celui-ci conserve le droit au respect de sa vie privée. C'est à l'employeur de fixer les limites du raisonnable. Par exemple prohiber toute consultation de sites pornographiques, de sites de jeux. Tout ce qui relève de la loi est bien sûr prohibé : télé-chargement de contenus illégaux, consultation de sites pédo-pornographiques, diffusion de messages de haines, harcèlement, etc. Il faut rajouter à cela toutes les actions pouvant mettre en cause l'entreprise ou contrevenir à son image : intrusion sur des sites tiers, vol de données... Ce qui reste généralement admis c'est le fait d'utiliser sa messagerie à des fins personnelles, de stocker des fichiers dans un répertoire "personnel" (sans en abuser, ce qui veut dire que les fichiers soient réellement personnels). Ni disque dur, ni clé usb ne peuvent être considérés comme personnels si connecté à un ordinateur professionnel. De la même manière, il est demandé aux salariés de ne pas abuser de l'utilisation du téléphone professionnel dans le cadre privé.

Exemple

Pour illustrer l'importance de la charte informatique prenons le cas suivant : un salarié utilise son ordinateur professionnel pour se connecter sur des sites prohibés par la loi. Il peut être détecté par les services de gendarmerie ou de police (par ex. dans le cadre d'une enquête sur un réseau de pédopornographie), ce qui veut dire que le salarié peut être interpellé sur son lieu de travail (à cause qu'il utilise une adresse IP de l'entreprise). Si l'entreprise n'avait pas mentionné explicitement ce cas dans son règlement intérieur, et plus généralement si l'entreprise ne pouvait justifier qu'elle a anticipé ce cas et fait ce qu'il fallait faire pour alerter les salariés sur le bon usage de son poste de travail, alors cette entreprise pourrait être poursuivie pour complicité par fourniture de moyens.

Mise en place d'un dispositif de surveillance

La surveillance désigne ici (pour les juristes) tout dispositif pour contrôler l'usage des TIC par les salariés. Il ne faut pas confondre avec les outils de filtrage à des fins de sécurité du SI (blocage de connexions sur la base d'adresses IP/numéros de ports).

Cela concerne par exemple :

- la surveillance par des logiciels spécialisés ;
- les écoutes téléphoniques (par ex. l'enregistrement des conversations d'un centre d'appels) ;
- la géolocalisation des personnes ;
- le traçage sur le web ou l'intranet ;
- le filtrage de contenus, la surveillance des courriers.

Tout projet de mise en place d'un dispositif de surveillance ne peut être mis en place sans respecter un parcours juridique en interne. Les principes directeurs pour la mise en place d'un dispositif de contrôle de l'activité des salariés sont ainsi :

- la procédure : information et consultation préalable des institutions représentatives du personnel (IRP), c'est-à-dire depuis 2017 le comité social et économique (CSE) pour les entreprises d'au moins 11 salariés ;
- la finalité (quels sont les enjeux, que veut-on protéger ?) ;
- la transparence : information préalable et individuelle des salariés ;
- la proportionnalité : les moyens mis en œuvre doivent être proportionnés au regard des intérêts à protéger et ne doivent pas permettre une surveillance constante et permanente des salariés ;
- la formalité : inscription au registre des traitements déclarés à la CNIL (si le dispositif est agréé).

Le non-respect de certains points : non-déclaration au registre des traitements, absence de consultation du CSE fera l'objet de sanction par la CNIL.

Du bon usage des réseaux sociaux

Les utilisateurs doivent adopter un comportement loyal vis-à-vis de leur entreprise. Rendre publiques des informations préjudiciables (sur les réseaux sociaux, les blogs, les sites) constitue une forme de déloyauté. Attention, c'est le caractère public qui pose problème, pas le fait par ex. d'injurier son employeur auprès de ses amis.

Cas du BYOD (*Bring Your Own Device*)

Cet acronyme (*Bring Your Own Device*) désigne une pratique très courante et en usage depuis les années 2000, qui consiste à utiliser ses outils personnels (ordinateur, smartphone) à des fins professionnelles. Cela pose plusieurs problèmes :

- de propriété intellectuelle : en cas d'usage par le salarié d'un logiciel non destiné à un usage commercial ;
- de sécurité : des données d'entreprise peuvent se retrouver dans un périmètre privé, pas ou peu protégé, des terminaux privés peuvent se retrouver connectés au SI de l'entreprise soit directement soit via des passerelles ;
- de droit du travail : utiliser son outil personnel (ex. smartphone) à des fins professionnelles ;
- de vie privée : il y a une confusion entre vie professionnelle et vie privée dès lors que les deux types de données se retrouvent sur un même terminal.

La plupart des entreprises n'ont pas anticipé ce phénomène qui peut être vu comme un moyen d'accélérer la productivité des salariés mais aussi pour d'autres comme source de potentielles portes dérobées susceptibles d'accroître la surface de vulnérabilité du SI de l'entreprise. Le phénomène s'est encore aggravé avec l'apparition des objets connectés, certains pouvant être connectés via des applications téléchargées par le salarié lui-même : montre, dispositif e-santé...

3.2.9 Les normes ISO

Ce sont les standards de référence utilisés au niveau ingénierie (RSSI, auditeurs) pour fournir un cadre méthodologique et un référentiel à la SSI sous tous ses aspects : gouvernance (mise en place d'un système de management de la sécurité SMSI), objectifs, mesures. La figure 3.9 situe le périmètre des normes ISO 2700x.

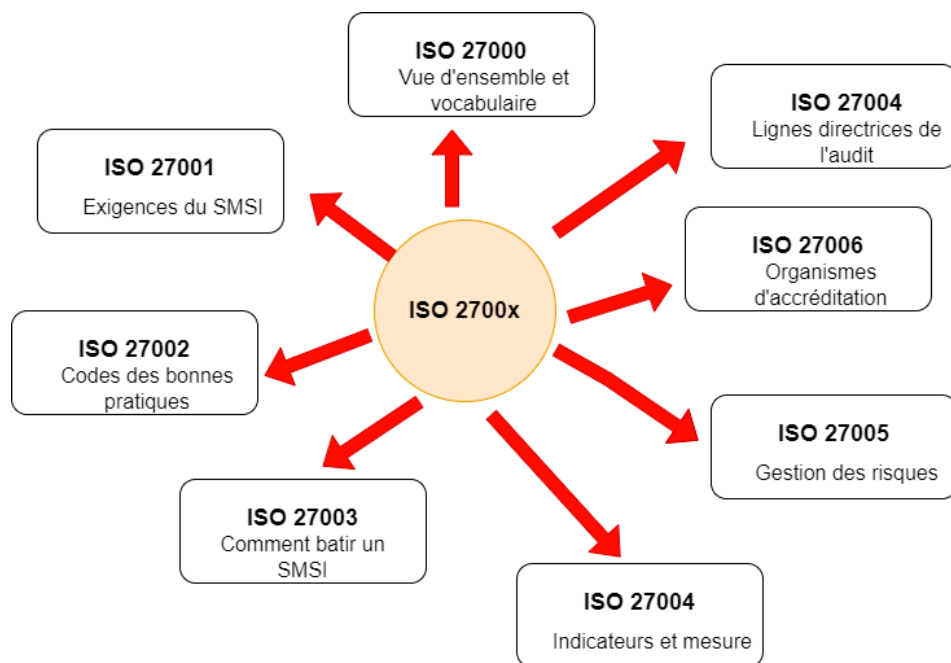


FIGURE 3.9 – Normes ISO 2700x

Les normes ISO donnent lieu à un processus de formation / certification des responsables qui les utilisent. Les plus citées sont dans ce cadre ISO 27001 et ISO 27005.

Comme déjà mentionné précédemment, ces normes ont été conçues pour l'entreprise sans réellement prendre en compte la taille ni les compétences présentes. Pour les petites entreprises elles peuvent apparaître sur-dimensionnées. C'est pourquoi dans la pratique, nombre d'auditeurs et de conseillers en sécurité, tout en s'inspirant des principes, appliquent des versions allégées de ces normes, notamment pour estimer les niveaux de sécurité des PME/TPE.

On peut citer d'autres normes ISO (certaines déjà mentionnées précédemment) :

- ISO 27031 : concepts et principe de préparation des TIC pour la continuation d'activité ;
- ISO 27035 : gestion d'un incident de sécurité ;
- ISO 27037 : identification, collecte, acquisition, préservation de la preuve.

3.3 Les institutions

3.3.1 Agence nationale de la sécurité des systèmes d'information

L'ANSSI a été créée en 2009, dans la continuité du Service Central de la SSI (SCSSI, 1986), de la Direction centrale de la SSI (DCSSI, 2001). Elle est rattachée au SGDSN (Secrétariat Général de la Défense et de la Sécurité Nationale). Son ministère de tutelle est le Premier ministre. C'est un service de plusieurs centaines de personnes (en évolution). Son rôle a été renforcé depuis la loi de programmation militaire (LPM 2013). Elle fait autorité en terme d'expertise, de proposition de règles de sécurité, de validation, de certification (notamment des prestataires de service de sécurité). Elle assure un rôle de veille, de formation, de détection, de lancement d'alertes, de gestion des incidents et des crises pour les réseaux de l'état, les services de l'état, les opérateurs d'importance vitale.

Elle abrite le CERT-FR (Centre gouvernemental de veille, d'alerte et de réponse à incident). Elle diffuse via son site [18] des guides de bonne pratique ainsi qu'un programme technique de formation, SecNumEdu [19]. L'ANSSI est aussi le promoteur de la méthode de gestion des risques EBIOS.

3.3.2 Commission nationale de l'informatique et des libertés

La CNIL[20] a été créée en 1978 dans le cadre de la loi du même nom. C'est une autorité administrative indépendante, c'est-à-dire qu'elle ne dépend d'aucun ministère. Ses missions sont :

- protéger la vie privée et la liberté dans le monde numérique ;
- informer, protéger, conseiller, réglementer, sanctionner, anticiper.

La CNIL a un rôle d'alerte, de conseil, d'information sur tout ce qui menace la vie privée via le développement des technologies numériques. Elle intervient de plus en plus sur la dimension économique des données.

Elle a aussi un pouvoir de contrôle et de sanction (amendes).

3.3.3 Sous-direction de lutte contre la cybercriminalité

La SDLC [21] a été créée en 2014. C'est une organisation issue de l'office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC), créée en 2000, auquel on a rajouté une division de la preuve numérique, une division de l'anticipation et de l'analyse, un bureau de

coordination stratégique. C'est un organisme de la police nationale qui contribue à la lutte contre la cybercriminalité. Les missions sont : enquêter, appuyer, détecter et renseigner.

Ce service gère la plate-forme de signalement PHAROS (Plate-forme d'harmonisation d'analyse, de recoupement, d'orientation des Signalements) [22] créée en 2009, située dans les locaux de l'OCLCTIC à Nanterre. Peuvent être signalés des faits utilisant internet, les réseaux sociaux, les sites web. Les signalements concernent surtout la cybercriminalité relative aux contenus :

- pédophilie et pédopornographie ;
- racisme, antisémitisme, xénophobie ;
- incitation à la haine raciale et religieuse ;
- terrorisme et apologie du terrorisme.

Il est possible de signaler des faits d'escroquerie, arnaques financières via internet, et aussi de cyber-harcèlement.

3.3.4 Brigade de lutte contre la cybercriminalité

La BL2C est le nom donné en 2019 à la brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI), une unité créée en 1994. Elle dépend de la direction régionale de la police judiciaire de Paris. Elle intervient surtout sur des faits de cybercriminalité concernant les atteintes aux STAD comme :

- les intrusions dans les systèmes informatiques ;
- les contrefaçons de logiciels ;
- le piratage de systèmes de téléphonie ;
- le défacement de sites web ;
- les atteintes à l'intégrité et la disponibilité des données.

La BEFTI participe aussi à la sensibilisation aux risques cyber.

3.3.5 La gendarmerie nationale

La gendarmerie nationale participe à la lutte contre la cybercriminalité via divers services spécialisés :

- Le C3N (centre de lutte contre les criminalités numériques), basé à Pontoise ;
- Le centre national d'expertise numérique département "hardware" au sein de l'IRCGN (institut de recherche criminelle de la GN) basé à Pontoise, spécialisé dans la recherche de preuve numérique avancée ;
- Le réseau CyberGend des enquêteurs numériques de la gendarmerie (appelés communément les Ntech), présents dans les Unités de Recherche du territoire.

Le Commandement de la Gendarmerie dans le Cyberspace (ComCyberGend) est l'organisme mis en place en 2021 pour fédérer l'action de ses services spécialisés. La structure du dispositif CyberGend est pyramidale. De la base au sommet on trouve :

- niveau local (brigades autonomes, premier intervenant P-Ntech) : recueil de plaintes pour des infractions de droit commun (usurpation d'identité), préservation et saisie de la preuve ;
- niveau local (brigades autonomes / brigades de recherche, Correspondant C-Ntech) : enquête de niveau local, vérification des données accessibles, saisies, placement sous scellés lors des perquisitions ;
- niveau départemental/ régional (sections de recherche, Enquêteur Ntech) : enquête de premier niveau, exploitation des supports (PC, smartphone, box, console, GPS), enquête judiciaire ;
- niveau central (experts IRCGN, C3N) : enquêtes poussées, investigations hardware, cas de supports ou terminaux endommagés, veille judiciaire sur le darkweb, traque des activités illicites.

3.3.6 Direction générale de la sécurité intérieure

La DGSI (ex DCRI devenue direction générale en 2014, elle-même intégrant les services de la direction de la surveillance du territoire et des renseignements généraux) est le service de renseignement dépendant du ministère de l'intérieur. Sa principale compétence est de lutter contre les menaces susceptibles de porter atteinte aux intérêts fondamentaux de la nation. Ses missions sont [23] :

- la lutte contre le terrorisme ;
- la protection du patrimoine économique et scientifique de la nation ;
- la lutte contre les cyber-menaces.

Du point de vue de la lutte contre la cybercriminalité, la DGSI agit dans deux directions : de façon pro-active par le renseignement vis-à-vis des menaces contre l'état (tout ce qui entre dans le périmètre des OIV) et de façon réactive par l'enquête judiciaire en cas de piratage des SI sensibles (sur ce point les agents de la DGSI peuvent être secondés par les experts de l'ANSSI) et les attaques terroristes (relevé et analyse de traces numériques).

3.3.7 Traitement du renseignement et action contre les circuits financiers clandestins

Le service TRACFIN [24] dépend du ministère de l'économie et des finances. Sa référence est le code monétaire et financier. C'est un service à compétence nationale, d'enquête administrative dont l'action s'inscrit en amont de la phase judiciaire. Son but est de recueillir, analyser, enrichir les déclarations remontées du terrain par les professionnels assujettis : banques, établissements de crédit, compagnies d'assurance, notaires, experts-comptables... Comme son nom l'indique, le but est de lutter contre les circuits financiers clandestin, le blanchiment d'argent et le terrorisme. Cela s'inscrit donc de façon plus générale dans la lutte contre :

- la criminalité économique et financière ;
- la fraude aux finances publiques ;
- tout ce qui menace les intérêts de la nation.

Le service dispose de compétences cyber et d'outils de surveillance des réseaux, d'investigation (bases de données), de renseignement, avec une finalité de détection d'activités financières illégales, activités pouvant être supports d'autres activités (terrorisme notamment).

3.3.8 Cyber-douanes

Ce service des douanes (situé à Paris) intervient dans le cadre de la lutte contre :

- les importations illégales ;
- la contrefaçon ;
- la fraude ;
- le trafic d'objets volés.

On se situe donc (comme pour TRACFIN) dans la recherche d'activités criminelles utilisant l'outil informatique (sites de vente en ligne, réseaux). Là encore, les techniques de renseignement (recherche en source ouverte pour détecter des transactions illicites), de surveillance des réseaux, d'investigation sont requises. Les procédures de surveillance résultent de remontées d'alertes du terrain. Dans le cas des cyber-douanes, cela implique : les entités régionales des douanes, la plateforme Pharos, les administrations spécialisées, les enseignes de e-commerce, les entreprises de fret, les intermédiaires financiers.

3.3.9 Les officiers de police judiciaire

Les OPJ sont des fonctionnaires de la police nationale ou de la gendarmerie nationale qui (après au moins trois ans de service) ont réussi un examen leur permettant de recevoir de l'habilitation OPJ du procureur général. Le titre d'OPJ est aussi accessible à des agents des douanes ou des services fiscaux. Dans le cadre d'une procédure pénale, et notamment relative à la cybercriminalité, ils ont ainsi la capacité de :

- constater crimes, délits, contraventions ;
- recevoir plaintes et dénonciations ;
- garder à vue des personnes ;
- procéder à des perquisitions ;
- faire de l'investigation numérique : identification des sources, collecte, analyse ;
- effectuer des réquisitions de personnes qualifiées (par ex. pour déchiffrer des fichiers).

Les OPJ agissent sous la direction du procureur de la république, sous la surveillance du procureur général et le contrôle de la chambre d'instruction. Les experts de l'ANSSI ou des agents de la CNIL qui participent à des enquêtes n'ont pas (sauf exception) le titre d'OPJ. Dans le cas d'une enquête suite à intrusion dans un système d'importance vitale, les OPJ sont des agents de la DGSI.

3.3.10 La magistrature

Les magistrats sont aujourd'hui confrontés aux technologies numériques dans le cas de procédures judiciaires relatives aux types 1, 2 et 3 du code pénal qui définit la cybercriminalité. Concernant le type 2, toute scène de crime comporte aujourd'hui des traces numériques (PC, smartphone, box, objets connectés), souvent décisives pour confondre les coupables.

Dans tous les cas, les magistrats doivent savoir interpréter les éléments de preuves qui ont servi à constituer des inférences dans le dossier d'accusation, permettant ensuite de constituer une thèse générale. Ceci pose problème au niveau de la formation de ces magistrats car des données techniques sont utilisées dans le dossier, à partir des traces numériques relevées. Le juge peut recourir à l'avis et l'éclairage d'experts judiciaires, c'est-à-dire des spécialistes d'un domaine technologique précis, par ex. les smartphones, le cloud, les malwares, etc. Ces experts sont inscrits sur une liste établie à la cour d'appel et assermentés.

Le problème similaire concerne les avocats mais il existe aujourd'hui des cabinets spécialisés dans le droit relatif aux technologies numériques.

3.4 Les associations

Les associations sont plus ou moins thématiques. Certaines sont généralistes dans le domaine de la sécurité des SI, elles regroupent des experts (des RSSI généralement), constituent des cercles de réflexion autour des évolutions des SI et conséquemment des problématiques de sécurité. Elles proposent à leurs membres des événements (conférences typiquement), des groupes de travail autour de sujet prospectifs, ce qui peut donner lieu à des documents de synthèse, disponibles à ses membres. On peut citer ici les plus connues.

3.4.1 Le Clusif

Le Clusif (Club de la sécurité de l'information français) est l'une des plus anciennes associations en France (1992). Elle regroupe généralement des experts concernés, dans le domaine de la cyber sécurité mais aussi plus généralement à la confiance numérique, que ce soit des offreurs de solutions ou des utilisateurs. Le but est d'échanger les idées, les points de vue, les expériences. Le clusif s'est organisé en entités régionales (Clusir) qui ont leur propre autonomie pour organiser les groupes de travail ; Aquitaine, Champagne Ardennes, Est, Bretagne, Auvergne Rhône-Alpes, Nord, Ouest, PACA, Normandie, Guyane, Occitanie, Caraïbes, Réunion, Nouvelle-Calédonie). La liste peut évoluer. Le Clusif publie périodiquement un panorama de la cyber sécurité, basé sur des enquêtes auprès des entreprises. De façon générale, le Clusif maintient une bibliothèque de ses publications (panoramas de la SSI, états de l'art, méthodologies, recommandations). Le Clusif est à l'origine de la méthode d'analyse de risques MEHARI.

3.4.2 Le CESIN

Le CESIN (Club des experts de la sécurité des systèmes d'information et du numérique) est une association plus récente. Son périmètre est semblable à celui du Clusif. Le but est de partager entre experts, responsable SSI, les expériences et les pratiques. Il fonctionne en collège autour de grandes thématiques : fondamentaux, méthodes et standards, cybersécurité, opérationnelle, facteurs humains, grandes entreprises. Le CESIN organise un congrès annuel et une université d'été.

3.4.3 Le CeCyF

Le CeCyF (Centre expert de lutte contre la cybercriminalité français) a été créé début 2014 à la suite du projet européen 2CENTRE (2011-2013) autour de la lutte contre la cybercriminalité. Ses membres fondateurs sont la Gendarmerie nationale, l'Université de technologie de Troyes (UTT), Thales, Orange pour citer les principaux contributeurs du projet 2CENTRE. Ici on s'intéresse à la menace, à l'enquête, aux aspects technologiques, techniques, mais aussi judiciaires, liés à la réponse à incident en général et à l'investigation numérique en particulier. Ses membres viennent donc du monde des enquêteurs, des universitaires, des juristes. Le CeCyF organise tous les ans la conférence CORIIN (Conférence sur la Réponse à incident et l'investigation numérique) en marge de la conférence annuelle FIC (Forum international de la cybersécurité).

3.4.4 Signal Spam

Son nom désigne explicitement une activité autour du Spam, ce qui se traduit ici par la mise en place d'une plateforme pour signaler tout message reçu et indésirable (spam ou pourriel). En fait ces messages publicitaires qui polluent les boîtes de réception de messages peuvent constituer la première phase d'une tentative d'escroquerie (en incitant à fournir ses coordonnées bancaires), d'hameçonnage (en incitant à ouvrir un fichier ou à se connecter sur un site tiers). Ces courriels suspects peuvent être signalés à Signal Spam (après inscription préalable) qui propose une extension à télécharger pour ensuite signaler en un seul clic les messages suspects.

3.4.5 CyberLex

Cyberlex est une association qui traite des problématiques de droit relatif aux technologies numériques. Les membres sont des experts des deux communautés. L'association organise chaque mois une réunion thématique. Les sujets ne manquent pas, l'avenir du règlement RGPD, l'usage croissant de l'intelligence artificielle. Cyberlex situe sa réflexion au niveau de l'évolution du droit vis-à-vis des technologies et des usages.

3.4.6 Les pôles de compétitivité

Les pôles de compétitivité ont un statut d'association. Concernant la thématique de la cybersécurité, le pôle le plus important (en taille, en nombre d'acteurs,

par sa vocation internationale) est le pôle Systematic, localisé à Paris Saclay, et plus particulièrement le hub "Cyber & Security", qui fédère l'écosystème, des représentants du monde académique, des start-up, des PME, des ETI, des grands groupes industriels, des institutionnels. Le périmètre concerne la cybersécurité, mais aussi la confiance numérique et encore les innovations du numérique pour la sécurité.

Le PEC (Pôle d'excellence cyber) fédère l'écosystème de Bretagne, avec des acteurs académiques importants (Univ. Rennes, INSA Rennes, IMT Atlantique, ENST Bretagne, Univ. Bretagne Sud, Ecoles de Saint-Cyr Coëtquidan, etc.), des industriels, essentiellement des PME/PMI du domaine. Le PEC s'est beaucoup spécialisé sur les aspects cyberdéfense, notamment sa composante régalienne (ministère de la défense, ministère des armées).

De façon générale, tous les pôles de compétitivité, internationaux ou nationaux, ont un rôle à jouer vis-à-vis de leurs membres (surtout les PME, TPE, startup) pour les sensibiliser aux menaces et à la protection de leurs données. Les projets de recherche (ANR, Europe) doivent aujourd'hui être labellisés avant dépôt par leurs pôles de rattachement et en fonction de la thématique.

3.5 Les métiers de la cybersécurité

En 2014, un livrable du projet européen 2Centre avait été consacré à la question [25]. En 2017 l'observatoire des métiers du numériques (OPIIEC) a publié une liste des métiers suite à une étude sur les formations et les compétences en France en cybersécurité. L'ANSSI a établi une synthèse en 2018 réactualisée en 2020 [26]. Malheureusement, ce référentiel ignore les métiers du forensique (enquêteurs spécialisés) et le rôle de la formation. La recherche a été (curieusement) rangée dans la rubrique des services. Nous nous présentons ici une version qui corrige ces erreurs. De façon générale, tous les métiers nécessitent une formation à niveau bac+5 minimum.

3.5.1 La gestion de la sécurité et le pilotage des projets

Responsable SSI

Le métier de RSSI (Responsable de la SSI) ou encore en anglais *Chief Information Security Officer* (CISO) a pour mission principale la protection du SI dans son périmètre, ce qui veut dire notamment :

- identifier les risques et les enjeux ;
- définir les axes et objectifs stratégiques, les mesures à mettre en place ;
- définir un plan d'actions ;
- en mesurer les effets par des indicateurs, des audits réguliers ;
- diffuser la culture des enjeux et des menaces auprès des utilisateurs et décideurs.

Son domaine de compétences est la fois technique, mais aussi organisationnel et de plus en plus juridique (il doit connaître les principales lois et obligations légales).

Directeur de programme de sécurité

Par rapport au RSSI, il peut définir et mettre en œuvre une politique de sécurité mais dans des secteurs métier particuliers, ou bien selon un axe de développement technologique particulier (cloud, transformation numérique).

Responsable de projet de sécurité

Son rôle est de mettre en place des solutions et outils, après en avoir défini les besoins et les objectifs, en tenant compte des besoins et des enjeux métiers (les aspects fonctionnels).

3.5.2 Conception et maintien d'un SI sécurisé

Responsable sécurité de projet

Dans le cadre d'un projet informatique il peut être nécessaire de disposer d'une compétence experte en cybersécurité, distincte du chef de projet. Il s'assure de la bonne prise en compte des aspects de sécurité dans le cadre du projet. Si des aspects liés au traitement des données personnelles sont présents alors il faudra aussi adjoindre le DPO.

Architecte sécurité

Il a un profil avant tout technique, pour valider les choix, définir les modèles, accompagner les développements d'architecture, en cohérence avec la stratégie et la politique de sécurité.

Spécialiste sécurité d'un domaine technique

On peut avoir besoin d'une expertise sécurité dans un domaine technologique particulier : réseau, cloud computing, systèmes industriels, systèmes embarqués, IoT... Il peut donc intervenir sur une partie d'un projet (cahier des charges, déploiement), intervenir comme expert en cas de réponse à incident, assurer formation information, conseil, prévention.

Spécialiste en développement sécurisé

Généralement les développeurs ne sont pas formés sur les aspects sécurité. C'est un aspect souvent absent des cahiers des charges. De nombreux développements nécessitent pourtant de prendre en compte la sécurité, à la fois parce qu'ils participent de la confiance, pour des raisons légales, mais aussi pour éviter de constituer des vulnérabilités exploitables. Un spécialiste en développement sécurisé (compétence rare) peut intervenir en amont au niveau du cahier des charges, au niveau du développement, au niveau des tests de vulnérabilités.

Cryptologue

Il intervient au niveau de l'utilisation et de la mise en œuvre opérationnelle de moyens cryptographiques pour assurer les critères DICP (surtout intégrité, authentification et confidentialité). Les applications sont nombreuses et les compétences requises dans le domaine bancaire (carte à puce), les télécommunications, la téléphonie mobile, la protection des documents... C'est un domaine qui évolue fortement avec l'apparition des calculateurs quantiques et la cryptographie post-quantique.

Administrateur de solutions de sécurité

Il met en place des solutions, qu'elles soient logicielles (gestion des accès, des droits, antivirus), ou d'infrastructure (équipements réseau).

Auditeur de sécurité organisationnelle

Il réalise des audits de vulnérabilités, des contrôles de processus de sécurité, afin de vérifier s'ils sont conformes à la politique de sécurité définie et s'ils sont efficaces. Aux vulnérabilités et non-conformités, il propose des solutions de remédiation.

Auditeur de sécurité technique

Il réalise des évaluations techniques de la sécurité, en effectuant par exemple (et selon ses compétences) des tests d'intrusion, des audits de logiciels, des revues de configuration, etc.

3.5.3 Gestion des incidents et des crises

Il faut distinguer incident et crise. On parle de crise quand la situation n'est pas sous contrôle et ceci pour plusieurs raisons :

- l'incident ne ressemble à rien de connu ce qui ne permet pas d'identifier clairement les compétences et la quantité de ressources humaines requises ;
- il a un fort impact de par le nombre d'actifs touchés, le nombre de poste de travail inopérants, de serveurs, les dysfonctionnements générés, le temps de remise en service, etc.

Responsable SOC

Le responsable du SOC (*Security Operation Center*) assure la gestion, la planification et la supervision des opérations mises en place pour détecter les activités suspectes. Il est en charge du processus permanent d'amélioration du service SOC : rapidité, efficacité.

Opérateur analyste SOC

Il participe au processus de détection des activités suspectes ou malveillantes. Il identifie, catégorise, qualifie les incidents sur la base des connaissances sur la menace. Il intervient en support des équipes de réponse à incidents.

Responsable du CERT (CSIRT)

Le responsable CERT dirige une équipe de réponse à incident. Il doit assurer la coordination des parties prenantes (membres CERT, autres CERTs, experts, responsables entreprise). Il doit anticiper sur les questions d'organisation de manière à rendre le processus de traitement efficace, et faire un retour d'expérience.

Analyste réponse aux incidents de sécurité

Dans le cadre d'un CERT (généralement), il analyse les symptômes, réalise des analyses techniques sur le SI afin d'identifier le profil de l'attaque (scénario, étendue de la compromission). Il fait des recommandations pour la phase de remédiation et le durcissement des conditions de sécurité.

Gestionnaire de crises cybersécurité

Dans le cadre d'un CERT ou d'une équipe associée de gestion de crises il analyse l'ampleur de la situation pour proposer un chemin de sortie de crise, sous la forme d'actions coordonnées et de recommandations à suivre. Il organise la capacité de l'organisation à affronter de nouvelles menaces.

Analyste de la menace cybersécurité

Il s'intéresse à la menace en identifiant les attaquants potentiels, leurs motivations, leurs modes de passage à l'acte, c'est-à-dire leur profil afin d'optimiser la stratégie de défense et de fournir au CERT ou SOC associé des renseignements fiables et contextualisés.

Le digital forensique

Le mot clé est ici la recherche de preuves numériques. Deux types de populations sont concernées : les enquêteurs spécialisés (officiers de police judiciaire le plus souvent, des services de police ou de gendarmerie) et les enquêteurs pouvant intervenir au sein des entreprises (soit ils en font partie, soit ils viennent d'une société tierce). Celles-ci ont en effet tendance à traiter les incidents par leur propre enquête. L'enquêteur utilise souvent des équipements spécifiques, assez coûteux, qui nécessitent une formation préalable. Il intervient au niveau des terminaux le plus souvent : PC, supports de stockage, smartphones, voire des équipements réseaux et des serveurs. L'objectif du processus forensique est pour l'officier de police judiciaire de constituer un dossier avec des preuves vis-à-vis de la loi, pour l'entreprise, c'est souvent de comprendre et de reconstituer un chemin d'attaque, voire de confondre en interne un salarié malveillant.

3.5.4 Le conseil

Consultant en cybersécurité

L'intérêt du consultant est d'appartenir à une société de conseil et donc de faire un diagnostic sur le niveau de sécurité d'un SI avec un regard extérieur. Le

second avantage est d'apporter son expérience de précédentes interventions auprès d'entreprises très différentes. À partir de là il peut proposer des solutions, des méthodes à mettre en place, des outils, selon le niveau de conseil : technique, organisationnel, voire les deux.

Formateur en cybersécurité

La formation, la sensibilisation font partie des prestations de service. La sensibilisation concerne tout le monde. La formation peut être spécialisée selon le public, son métier, sa maturité sur le sujet, sa perception du risque. Elles peuvent être thématiques. Ces formations sont bien sûr non diplômantes mais elles peuvent donner lieu à une évaluation finale. Les formations pratiques sont sans doute les plus efficaces.

Évaluateur de technologies

Certaines entreprises sont agréées et spécialisées dans l'évaluation de technologies (systèmes, logiciels, composants). Elles vérifient la conformité d'un produit, d'un système, par rapport à sa spécification de sécurité, selon une méthode et des critères normalisés, réglementaires, appelés critères communs (ISO 15408). Le but est d'évaluer le niveau de confiance qu'on peut avoir dans ces technologies, en matière de non-divulgaration des données, de ruptures d'intégrité, de défaillances, dans un contexte d'activités humaines ou non, malveillantes ou non.

Développeur de solutions de sécurité

Il intervient au sein de sociétés qui développent des logiciels de sécurité, pour définir les spécifications, concevoir les solutions, les tester au regard des menaces concernées par ces produits.

Intégrateur de solutions de sécurité

Tout comme un intégrateur de solution IT, il s'agit ici de solutions de sécurité, ce qui concerne les aspects architecture, assemblage de composants, intégration et déploiement dans un environnement de production. Cette prestation peut s'accompagner d'un service dans la durée, de maintien en conditions opérationnelles.

3.5.5 L'enseignement et la recherche

Formations diplômantes

Comme il a déjà été mentionné, les métiers du domaine supposent une formation de type bac+5 minimum. Cela concerne les formations d'ingénieurs (informatique, réseaux/télécoms) avec généralement une spécialisation en sécurité en dernière année (ou en filière). Le principe est qu'on n'aborde pas les questions de sécurité quand on ne maîtrise pas d'abord les aspects fonctionnels. Cela concerne aussi les masters. Malheureusement, la réforme des masters a imposé l'intitulé du diplôme dans une liste prédéfinie qui ignore complètement le mot sécurité. Alors

que le discours public dans le domaine régalien (armées, intérieur et même Premier ministre) est de rappeler le besoin croissant (et non couvert) de spécialistes en cybersécurité, le ministère de l'Enseignement supérieur et de la Recherche a effacé la possibilité d'intituler des masters en cybersécurité. Le sujet ne peut être que proposé en option de deuxième année (bac+5) à partir d'un intitulé général imposé qui ne peut être que : "Informatique" voire "Ingénierie des systèmes complexes".

Il existe aussi des diplômes de masteres (bac+6), certifiés non par le ministère mais par la conférence des grandes écoles, accessibles à partir d'un diplôme d'ingénieur ou de master, sur des thématiques diverses : Cybersécurité et cyber-défense, Cybersécurité du numérique, Forensic et cybersécurité, pour citer les plus connus.

La problématique est d'identifier la bonne formation en fonction du métier visé, parmi ceux que nous avons cités. Si on vise les métiers de la gouvernance, il faut plutôt choisir une formation de type master assez généraliste sur le sujet, voire le master de l'INSA Lyon. Si on vise les métiers dans le domaine de la réponse à incident, alors l'université de Bretagne Sud (Vannes) peut être conseillée. Le digital forensic n'est enseigné qu'à l'UTT, (qui forme les cyber-gendarmes au niveau licence et qui propose aussi un master spécialisé dans le domaine). Les universités de Limoges, Grenoble sont des références dans le domaine de la cryptographie.

Les métiers de la recherche

Par la recherche, on peut acquérir un diplôme bac+8. Cela conduit à pouvoir être enseignant-chercheur et à faire une carrière universitaire mais les plus nombreux iront travailler dans les entreprises spécialisées (qui peuvent financer des thèses). Par rapport à un ingénieur du domaine, le jeune docteur a souvent un profil plus pointu sur une technologie particulière : télécoms, cryptographie, malwares, IoT, etc. Il peut donc intervenir comme expert d'un domaine quand celui-ci est concerné par une enquête par ex. ou par le développement d'un nouveau produit de sécurité. Il faut rappeler que l'enseignant chercheur est aussi enseignant et que donc il participe activement à des formations diplômantes, qu'il participe donc à l'évolution des enseignements, fonction des technologies, des menaces et des métiers.

3.6 Exercices

1) Quelle loi a introduit le concept de STAD (Système de traitement automatique de données) ?

- a) la loi Informatique et Liberté ;
- b) la loi de programmation militaire ;
- c) la loi Godfrain.

2) Les équipements suivants sont-ils des STAD ?

- a) clé usb ;
- b) carte à puce ;
- c) objet connecté ;

- d) autocommutateur d'entreprise ;
- e) chargeur de smartphone.

3) Quels sont les facteurs aggravants en matière d'atteinte aux STAD ?

- a) mise en œuvre par l'état ;
- b) appartenance à un OIV (Organisme d'Importance Vitale) ;
- c) qualité de l'auteur ;
- d) action en bande organisée.

4) Auprès de quelles autorités doit-on rapporter les incidents de type : Perte de données à caractère personnel au sein de son entreprise ?

- a) plateforme PHAROS ;
- b) agence régionale de santé (ARS) ;
- c) ANSSI ;
- d) CNIL.

5) Auprès de quelles autorités doit-on rapporter les incidents de type : cyber-harcèlement ?

- a) plateforme PHAROS ;
- b) agence régionale de santé (ARS) ;
- c) ANSSI ;
- d) CNIL.

6) Vis-à-vis du code pénal, ce qui compte c'est :

- a) l'action ;
- b) la technique utilisée ;
- c) l'effet de l'action.

7) Les organismes d'importance vitales (OIV) doivent signaler les incidents dont ils sont victimes :

- (a) à l'ANSSI ;
- (b) à la gendarmerie nationale ;
- (c) aux services fiscaux ;
- (d) à la CNIL.

8) Les services suivants ont-ils un pouvoir de police judiciaire ?

- (a) gendarmerie (NTECH) ;
- (b) enquêteur assurance ;
- (c) agent CNIL ;
- (d) cyber-douanes ;
- (e) expert ANSSI.

9) Un expert judiciaire est :

- a) un magistrat ;
- b) un officier de police judiciaire ;
- c) un expert indépendant assermenté.

10) L'agence ANSSI dépend :

- a) du ministère de l'Intérieur ;
- b) du ministère des Armées ;
- c) du Premier ministre.

11) Quels éléments d'information constituent une donnée personnelle ?

- a) numéro de sécurité sociale ;
- b) mot de passe ;
- c) adresse IP statique ;
- d) adresse IP dynamique ;
- e) bilan personnel d'activité ;
- f) note de frais ;

12) L'outil open source PIA proposé par la CNIL permet :

- a) d'identifier les données personnelles ;
- b) d'identifier les processus de traitement des données personnelles ;
- c) de faire une analyse d'impact relativement au RGPD.

13) La directive 2016/1148 du parlement européen et du conseil de l'UE (appelée *NIS Network Information Security*) prévoit de :

- a) combler les failles de sécurité de leurs systèmes ;
- b) signaler les auteurs d'infraction au sein de l'entreprise à la justice ;
- c) divulguer aux autorités compétentes les incidents les plus graves ;
- d) normaliser les exigences de sécurité au niveau européen ;
- e) désigner un point de contact national unique.

14) Un CERT peut offrir un service :

- a) de réponse à incident ;
- b) de détection de cyber-attaque ;
- c) de veille ;
- d) d'analyse forensique.

15) Un dispositif de surveillance est un dispositif destiné à :

- a) surveiller et prévenir les intrusions dans le système d'information ;
- b) surveiller et prévenir les incidents réseau en général ;
- c) surveiller l'usage des TIC (Technologies de l'information et de communication) par les salariés.

16) Les sujets suivants peuvent-ils justifier a priori un dispositif de surveillance ?

- a) protéger les données personnelles ;
- b) contrôler le temps de travail ;
- c) contrôler la présence sur le lieu de travail ;
- d) lutter contre la fuite de données ;
- e) lutter contre le téléchargement illicite.

- 17) Quelle est la durée de conservation des logs de connexion ?
a) 3 mois b) 6 mois c) 9 mois d) 12 mois

18) Pour économiser sa facture télécoms une entreprise souhaite mettre en place un système de traçabilité des appels de ses postes fixes vers des numéros mobiles, quelles sont les étapes du processus juridique à respecter ?

- a) informer et consulter le personnel ;
- b) informer et consulter les instances représentatives du personnel (IRP) ;
- c) déclarer le système à la CNIL ;
- d) inscrire le traitement au registre des traitements (RT).

19) Une entreprise de conception de systèmes embarqués (aéronautique) veut mettre en place un dispositif de filtrage des mails sortants : filtrage par mots clés, filtrage des pièces jointes. Quelles pourraient être les justifications à un tel dispositif ?

20) Étude de cas.

Vous êtes RSSI chez un constructeur d'équipements automobiles et vous disposez d'une délégation de pouvoirs pour tout ce qui touche à la SSI. Le 10 mai 2019, vous avez connaissance des faits suivants : un employé de l'entreprise est suspecté d'avoir mené une campagne de hameçonnage contre certains collaborateurs d'une entreprise sous-traitante, dans le but de diffuser un rançongiciel. L'analyse de son ordinateur, les traces archivées au niveau des équipements réseaux, l'étude de son dossier RH ont mis à jour :

- qu'il avait travaillé au sein de l'entreprise cible et qu'il l'avait quittée suite au refus de sa demande de promotion ;
- qu'il possédait une liste des adresses mail des employés de cette entreprise ;
- qu'il a effectué plusieurs connexions vers le darkweb.

À partir de ces éléments vous devez répondre aux questions suivantes.

- a) Qu'est-ce que la délégation de pouvoir doit prévoir pour être valide ?
- b) La responsabilité de la société pourrait-elle être engagée ? Si oui pourquoi ? À quoi s'expose la société si les faits sont parallèlement découverts par un service de police ?
- c) Quelles mesures organisationnelles un RSSI doit prendre pour éviter ce type de comportement déviant ?
- d) Quelle action au niveau juridique le RSSI peut-il engager contre ce collaborateur (outre une procédure au tribunal des Prud'hommes) ?

Conclusion



Cet ouvrage a présenté la cybersécurité en trois volets et selon le schéma suivant :

- qu'est ce qu'on protège ?
- quel est le danger ?
- comment se protéger ?

Le sujet n'est pas que technique. Il comporte aussi des aspects organisationnels, méthodologiques, juridiques et humains. La cybersécurité n'est pas qu'une affaire de spécialistes. Elle implique une prise de conscience de tous les utilisateurs au quotidien mais aussi des décideurs, des dirigeants d'entreprises, des autorités de l'État.

Correction des exercices



3.7 Partie 1

1) Le réseau internet n'a pas de propriétaire mais il a un système de gouvernance. Il convient notamment d'assurer l'unicité du système d'adressage, que ce soit les adresses (numériques) IP et les adresses (symboliques) des ressources gérées par le système DNS. Cette gestion est aujourd'hui décentralisée aux registres internet régionaux (RIR). Pour l'Europe (+ Moyen Orient + Asie centrale) il s'agit du RIPE NCC (Réseaux IP européens - *Network Coordination Center*).

2) Le terme intranet désigne la sphère privée où se trouvent des ressources accessibles aux salariés d'une organisation, en fonction de leurs droits. Un serveur intranet n'a pas à être vu de l'extérieur et donc ne doit pas être référencé dans le système DNS.

3) On suppose une machine configurée correctement, c'est-à-dire qu'elle connaît l'adresse et le masque de son sous-réseau de rattachement, alors elle peut effectuer l'opération élémentaire (en binaire) $191.76.13.25 \text{ AND } 255.255.255.0 = 191.76.13.0$ pour vérifier que le destinataire n'est pas sur son réseau 192.25.10.0. Dans ce cas elle effectue une remise indirecte via sa passerelle de rattachement (autre paramètre de configuration), c'est-à-dire qu'elle envoie le paquet IP vers l'interface de son routeur. Attention : on ne remplace pas l'adresse IP du destinataire final par l'adresse IP du routeur. L'acheminement se passe au niveau trame (niveau 2) et utilise comme destinataire l'adresse de niveau 2 (par ex. Ethernet) du port du routeur.

4) L'acheminement est la notion clé des réseaux de données où circulent des paquets. Il désigne à la fois quelle information de leur entête on utilise et comment on l'utilise pour aiguiller le paquet vers le bon interface de sortie. Dans internet l'acheminement utilise l'adresse IP. La notion de transport ne concerne pas les équipements du réseau, mais uniquement la source et le destinataire final. La problématique d'un protocole de transport (comme TCP) est de s'assurer que tous les paquets transmis sont bien arrivés.

5) Pour router un paquet, seule l'adresse du destinataire est utile. L'adresse de la source n'est utilisée qu'en cas d'erreur de routage pour permettre à une passerelle de signaler à la source qu'il y a eu un problème.

6) En cas d'acheminement direct, le routeur ne sert pas puisque source et destinataire final sont sur le même réseau.

7) La partie utilisée pour interroger le système DNS est : `www.yvert.com` ; On voit que $3 + 1$ niveaux apparaissent : le niveau -3 : `www.yvert.com` (un serveur web), le niveau -2 : `yvert.com`, le niveau -1 (ou TRL) : `.com`, et le niveau racine (de l'arbre) : niveau 0, implicite car jamais mentionné. À chaque niveau correspond un serveur DNS. Le serveur web `www.yvert.com` est connu du domaine `yvert.com`. Le serveur `yvert.com` est connu du niveau TRL `.com` (il a été enregistré auprès du service qui gère les noms de domaines français, à savoir l'association AFNIC). Si l'interrogation part du domaine français alors la requête du serveur DNS source vers vers le niveau `.com` pour ensuite redescendre vers le serveur DNS du domaine `yvert.com` qui pourra renvoyer en retour l'adresse IP du serveur web de son domaine.

8) Une box internet assure plusieurs niveaux de fonctionnalités : un modem ADSL pour la partie transmission, un routeur pour la partie acheminement, un serveur DHCP pour fournir dynamiquement une adresse IP aux machines du réseau local de rattachement, typiquement : PC, smartphones, imprimantes, objets connectés (TV, chaudière, portail, etc.)

9) Un industriel a besoin d'échanger des informations avec ses fournisseurs dans le cadre de ses processus métiers (notamment logistique). Le besoin est connu mais ceci doit être particulièrement encadré. Quelles applications ont le droit d'échanger ? Gestion des stocks, facturation généralement. Il convient de contrôler les accès et surtout que les politiques de sécurité soient du même niveau d'exigence de part et d'autre. Le risque pour l'industriel est en effet que le fournisseur soit victime d'une intrusion qui le vise de façon indirecte en utilisant ce canal relationnel.

10) Un projet peut durer deux ans, où divers acteurs et services vont intervenir et échanger des données à différentes phases : fournisseurs, équipementiers, marketing, gestion des stocks, design, production, logistique, distributeurs... Un constructeur automobile est aujourd'hui essentiellement un intégrateur de pièces et de composants (numériques, électroniques, mécaniques) fournis par d'autres entreprises. Les données échangées sont à protéger dans un environnement concurrentiel. Les droits des différents acteurs sont à définir aux différentes phases du projet. Ils vont utiliser des outils de bureautique classique (éditeurs, tableurs) mais aussi des outils de communication (téléphonie, réunions en présentiel ou distanciel), des outils d'accès à distance aux bases de données métiers (données techniques, données commerciales), des outils de partage de documents. Une organisation dynamique se met donc en place, hétérogène, avec des outils de partage de données.

11) Les outils de partage de ressources sont souvent utilisés par les acteurs d'une même entreprise (imprimante, photocopieuse, stockage, conférence...), d'un même

service, voire même d'acteurs d'un même projet mais d'entreprises différentes. Cela pose donc plusieurs questions :

- n'importe qui peut-il y accéder ? Les droits d'accès sont-ils définis pour chacun et limités dans le temps ?
- quelles données sont partagées ? Leur niveau de criticité ? On suppose que c'est le cas pendant une phase de projet de conception ;
- les outils applicatifs utilisés sont-ils sécurisés ?

12) Le BYOD (*Bring Your Own Device*) désigne le fait que les salariés peuvent utiliser leurs terminaux personnels dans l'espace professionnel et réciproquement. C'est une pratique qui s'est imposée à l'usage et les entreprises ont mis du temps à réagir avant d'essayer de contrôler le phénomène. Les exemples sont très répandus : utilisation d'un ordinateur portable qui se connecte à plusieurs endroits, sur plusieurs réseaux (domicile, bureau, hôtels), avec des niveaux de sécurité hétérogènes. Des comptes de la sphère privée et professionnelles communiquent entre eux, se synchronisent (agenda, messagerie). Les aspects productivité y trouvent leur compte, moins de temps perdu, convergence des applications, continuum dans les habitudes, partage de données entre les sphères privées et professionnelles. Les aspects sécurité ont tout à craindre. Il n'y a plus de séparation entre les deux sphères. Des données privées peuvent utiliser les ressources du SI de l'entreprise (par ex. son système de messagerie). Des données de l'entreprise peuvent se retrouver plus facilement à portée de malveillance dans la sphère privée.

13) Les méta-données de type "général" sont renseignées automatiquement. Les données relatives aux origines du fichier sont renseignées a priori. C'est à ce niveau qu'on peut trouver : le nom de l'auteur (qui a créé le fichier), le nom de celui qui a fait le dernier enregistrement. Par contre l'auteur peut renseigner lui-même des méta-données de description comme Origine = son nom, Ordinateur = le nom de l'ordinateur (souvent dérivé du nom de l'utilisateur).

14) On peut éditer certaines méta-données d'un fichier PDF à partir de l'éditeur PDF lui-même. Des outils plus exhaustifs existent comme PDF Parser. Pour les images on peut mentionner Exiftool, Jexifviewer, Exifread, PyExif. Les outils de gestion des fichiers permettent aussi d'éditer les méta-données. Pour les fichiers PDF on peut citer Xpdf et Origami. Pour les fichiers image on peut citer XnView.

15) La plupart des objets connectés n'ont pas besoin d'une adresse IP, n'ayant pas la capacité (traitement, énergie, bande passante) de gérer un protocole de communication comme IP. IPv6 est de toute façon le seul protocole pouvant assurer un adressage aux objets sans limitation. Si on a besoin de gérer ces objets à distance (capteurs / actionneurs) alors une passerelle (ou concentrateur ou hub) aura besoin d'une adresse IP pour son interface de communication avec le réseau public mais il n'en a pas besoin pour son interface vers le réseau de distribution vers les capteurs / actionneurs du processus physique sous contrôle. Les caméras de surveillance sont un exemple d'objets connectés (la caméra est un capteur) ayant besoin d'une adresse IP.

16) Le capteur est un capteur de CO. L'actionneur est un générateur de son. Cet équipement a besoin d'une connexion dans deux cas :

- quand on a besoin de localiser l'origine de l'alerte (parmi de multiples sources possibles) ;
- en cas d'absence, le signal sonore ne sert à rien, il est plus utilisé d'envoyer un message d'alerte à distance (vers le smartphone de l'utilisateur).

17) Cadre applicatif des objets :

- a) relevé de température : Service ;
- b) régulation par thermostat : Service ;
- c) détection de présence : Service ;
- d) gestion de l'énergie : Application (qui peut utiliser les services a, b, c) ;
- e) gestion de l'ouverture des portes : Service.

18) Le smartphone : c'est l'équivalent d'un PC aujourd'hui, donc pas un objet, par contre il joue souvent le rôle de passerelle.

La voiture contient des milliers de capteurs, c'est un système connecté. Par contre si on envisage une application antivol alors la voiture devient un simple objet.

La caméra de vidéo-surveillance est un objet connecté.

Le drone est un objet connecté sauf s'il embarque plusieurs applications.

La chaudière est un objet connecté.

Le vélo d'appartement est un objet connectable (via une application).

L'être humain peut être traité comme "objet connecté" dans certains cas d'application de sécurité : suivi (via capteur associé) de personnes vulnérables (enfants, personnes âgées, personnes atteintes de la maladie d'Alzheimer par ex.).

19) Dans l'entreprise on ne trouve pas de gestion des parkings, des feux de circulation, du ramassage des ordures ménagères, de l'éclairage public.

20) La GTB désigne la gestion technique des bâtiments réalisée par des prestataires extérieurs, qui utilisent des capteurs et des actionneurs répartis. Dans le cadre d'un immeuble d'entreprise, les fonctions de gestion sont notamment :

- la gestion des fluides (air, eau) ;
- la gestion des déchets ;
- la gestion de l'énergie ;
- la gestion de l'éclairage ;
- la gestion des accès ;
- la gestion des ascenseurs ;
- la prévention des incendies.

3.8 Partie 2

1) Le terme p caractérise :

- (b) la menace ;
- (c) l'attaque.

- 2) Les éléments qui constituent des cyber-menaces :
- a) une campagne de phishing en cours ;
 - c) les chevaux de Troie Trickbot et Emotet responsables de plus de 22% des attaques de ransomware en France.
- 3) Vecteurs d'attaque :
- a) pièce jointe ;
 - b) usurpation d'identité ;
 - c) clé usb.
- 4) Cibles finales possibles :
- a) données personnelles ;
 - c) serveur web.
- 5) Vulnérabilités :
- b) mot de passe faible ;
 - c) faible perception du risque par l'utilisateur ;
 - d) port non utilisé non désactivé.
- 6) Les tests d'intrusion permettent d'identifier :
- b) les vulnérabilités.
- 7) Selon la définition du risque ($R = p * D$) on diminue le terme D :
- b) en augmentant la capacité de détection ;
 - d) par une politique de sauvegarde.
- 8) Selon la définition du risque ($R = p * D$) on diminue le terme p :
- a) en diminuant la surface d'attaque ;
 - c) en faisant une analyse de la menace.
- 9) Le facteur d'impact permet de quantifier :
- b) les dommages potentiels.
- 10) Les éléments suivants sont-ils des incidents de cyber-sécurité ?
- a) phishing ;
 - c) crash de disque dur, ceci n'est pas lié à la malveillance mais les dommages peuvent être comparables ;
 - d) attaque DDoS.
- 11) S'il n'y a pas d'impact il n'y a pas de risque :
- a) vrai.
- 12) La matrice MITRE ATT&CK propose une modélisation :
- b) des cyber-attaques.

13) Un cheval de Troie permet de :
c) créer une porte dérobée.

14) Critère(s) DICP impacté(s) par l'exfiltration de données :
c) confidentialité.

15) Critère DICP le plus important dans le cas des données médicales :
l'intégrité.

16) Le but d'un audit de sécurité est de découvrir :
b) les vulnérabilités ;
c) les failles.

17) Un usager se connecte tous les jours entre midi et treize heures sur un site de cotation de matière première, ceci peut constituer :
b) une vulnérabilité.

18) La réponse est contenue dans la figure 2.16.

19) Les quatre phases de la réponse à incidents sont :
b) communication ;
d) décision ;
f) retour d'expérience ;
h) technique.

20) Dans le processus de réponse à incident, la fonction de triage doit :
c) évaluer l'incident.

21) Dans le processus de traitement des incidents, le bon ordre est :
c) Détection -> Triage -> Analyse -> Réponse

22) Dans une équipe de réponse à incident on peut mettre :
a) un administrateur système ;
b) un responsable communication ;
c) un dirigeant ;
e) un responsable sécurité.

23) Dans un tel cas quels les signaux d'alerte peuvent être :
c) activité inhabituelle sur le disque dur.

24) La première mesure est :
b) débrancher sa machine du réseau.

25) L'utilisateur peut :
a) éteindre sa machine.

Remarque : il est déconseillé de contacter par mail son responsable informatique mais de le contacter de vive voix.

26) Après avoir collecté des traces numériques, l'enquêteur doit :

- a) en faire une copie ;
- c) en faire un hachage.

27) Un SIEM est constitué :

- a) d'un système de détection ;
- b) d'un système d'analyse de données.

28) Dans un SIEM il n'y a que de la technologie :

- a) vrai.

29) Un système Syslog est un système :

- b) de centralisation des logs.

30) L'analyse « live forensics » permet :

- d) d'analyser un système en fonctionnement.

31) Étude de cas 1.

- a) Administrateur système, responsable commercial + CERT.
- b) Problème de disponibilité des fichiers clients, alerte de niveau utilisateur qui doit avertir (de vive voix son responsable informatique) qui doit déconnecter le poste du réseau.
- c) Le CERT doit aider à analyser les données visibles pour identifier qu'il s'agit d'un ransomware qui se trouve sur le serveur (et non pas sur un poste client) mais on ne sait sans doute pas comment il a pu rentrer là.
- d) L'entreprise ne doit surtout pas "piétiner" la scène c'est-à-dire effacer les traces.
- e) OSINT concerne la recherche de renseignement en source ouverte c'est-à-dire dans tous les serveurs publics. Maltego est un outil très connu, développé par Paterva (Afrique du Sud), présentation sous forme de graphes qui relient les entités.
- f) Anomalies constatées : pas d'antivirus à jour, pas d'antivirus en coupure pour analyser les pièces jointes, pas de processus clair de réponse à incidents, piétinement des traces, délai excessif avant l'arrivée des enquêteurs, pas de politique de sauvegarde.
- g) Phase RETEX. Compte tenu des anomalies constatées, l'entreprise doit mettre en place un antivirus au niveau des postes de travail, un antivirus au niveau du serveur de messagerie pour analyser les pièces jointes. Elle doit définir et mettre en place une procédure de réponse à incident ainsi qu'une politique de sauvegarde.
 - Menace : ransomware + prestataire de maintenance ;
 - Risque : perte de données commerciales ;
 - Vecteur d'attaque : pièce jointe ;
 - Cible : serveur de fichiers ;
 - Impact : commercial, juridique (données personnelles).

32) Étude de cas 2.

- a) On parle d'un soutien via un prestataire de service de type CERT par ex. On peut aussi requérir le soutien de son FAI (si pertinent).
- b) Le recours aux forces de l'ordre peut être motivé par l'intention de porter plainte (police ou gendarmerie). Ceci peut se justifier si on a des chances de trouver le coupable et de le condamner. Or dans le cas où la menace est interne ceci peut se justifier.
- c) Les données de trafic peuvent être récupérées au niveau des logs des équipements réseau : FW, routeur et aussi au niveau système : accès serveurs.
- d) Le point d'entrée peut être ici un accès autorisé ou usurpé à un serveur de fichiers de la part d'un employé. La question sera de savoir s'il y a un contrôle d'accès et si l'employé a des droits légitimes sur ce serveur.

Mesures correctives :

- avoir une procédure de gestion des droits incluant la phase de départ (préavis) des employés et leur départ effectif. Cela veut dire associer une politique RH de sortie à une politique de droits d'accès aux ressources via un outil, de gestion.
- l'accès à distance fait partie des droits d'accès et doit pouvoir être intégré à l'outil de gestion. De plus tout accès distant doit passer par un tunnel sécurisé (VPN) qui permette d'abord d'identifier le distant, puis s'il est autorisé à accéder au SI, de filtrer les ressources auxquelles il peut accéder.
- gestion des mots de passe : pour authentifier les personnes et ensuite associer à chaque accès autorisé l'ensemble des droits mis à jour.

33) Étude de cas 3.

- a) Symptômes : fichiers chiffrés, extensions modifiées.

Impacts : impact business (indisponibilité des données), impact juridique lié au non-respect du RGPD, impact réputation.

- b) L'utilisateur doit isoler son poste en déconnectant le réseau et signaler de vive voix ou par téléphone au responsable informatique (ici).

- c) Il y a plusieurs hypothèses :

- la phase de reconnaissance par l'attaquant a généré une activité suspecte qui génère ce type de log ;
- une attaque DOS sur le serveur a servi de leurre et pendant ce temps le chiffrement a pu avoir lieu ;
- les logs ont été falsifiés.

La première hypothèse est la plus vraisemblable.

- d) Ne pas effacer de fichiers, éviter d'éteindre la machine et le serveur, ne pas lancer d'antivirus.

- e) On a besoin de reconstituer un chemin d'attaque, il faut récupérer les logs qui sont disponibles (FW, routeur, mail, serveur de fichiers) pour savoir ce qui se passe avant 9 :44 le 16/07 ; les logs systèmes pour récupérer les dates de chiffrement de chaque poste.

- f) Le risque le plus immédiat quand il s'agit d'un malware est la propagation. C'est pourquoi la mesure d'urgence est de circonscrire l'attaque par déconnexion des machines du réseau.

g) Équipe de réponse : direction, administrateur, ingénieur réseau, représentant de l'infogérance, responsable communication, juriste. On sait à la base que c'est un ransomware, donc le diagnostic est déjà posé avec un niveau d'alerte maximum (toutes les données sont perdues). Reste à traiter les étapes de mitigation, de restauration du système. La phase décisionnelle doit s'occuper du problème de paiement ou non de la rançon. La phase communication doit traiter de la communication avec les clients. La phase RETEX doit traiter du bilan et des actions d'amélioration.

h) Ceci concerne la phase RETEX. Au niveau des vulnérabilités révélées par cette attaque ($R = p * D$ est ici élevé) on peut dire, concernant le terme p que :

- les versions Windows Serveur ne sont pas à jour ;
- le ransomware est très connu (il y a même des services spécialisés sur son cas) or aucun antivirus ne l'a signalé dans le système ;
- le serveur contient des données personnelles et il n'est pas protégé.

Concernant le facteur D on peut dire que :

- il n'y a pas de sauvegardes ;
- un malware a pu chiffrer des fichiers pendant 56 minutes sans qu'aucune alerte ne soit levée au niveau du serveur ;
- il n'y a pas de plan de secours ;
- il n'y a pas d'équipe de réponse à incident, la preuve est qu'on a appelé au secours les gendarmes ;
- les logs disponibles sont maigres, insuffisants pour un système de surveillance digne de ce nom.

En conséquence il faut donc avoir une politique de mise à jour et disposer d'un antivirus performant dès l'entrée du réseau.

Il faut mettre en place une politique de sauvegarde des données, un plan de secours, passer un contrat avec un CERT voire un SOC, avoir une politique de protection des données personnelles relative aux dossiers médicaux.

Des mesures liées aux filtrages des flux dans le réseau et une politique de gestion des droits ne seront pas de trop.

Un dispositif de surveillance (un H-IDS) au moins au niveau du serveur paraît pour le moins nécessaire.

3.9 Partie 3

1) Concept de STAD.

c) Il a été introduit par la loi Godfrain.

2) Les équipements qui sont des STAD :

- a) clé usb ;
- b) carte à puce ;
- c) objet connecté ;

d) autocommutateur d'entreprise.

Tous ces équipements disposent d'un minimum de ressources de traitement et de mémoire, le minimum étant le tag RFID.

3) Facteur aggravant :

d) Action en bande organisée.

4) À qui signaler la perte de données à caractère personnel :

d) la CNIL.

5) À qui signaler le cyber-harcèlement :

a) la plateforme de signalement PHAROS.

6) Vis-à-vis du code pénal ce qui compte c'est :

a) L'action.

7) Les OIV doivent signaler les incidents de sécurité à :

a) L'ANSSI.

8) Services qui ont un pouvoir de police judiciaire :

a) Gendarmerie NTECH.

Remarque : la police, la DGSI ont aussi ce pouvoir. Officiellement les cyber-douanes ne l'ont pas mais certains de ses agents peuvent à titre personnel avoir le titre d'OPJ.

9) Un expert judiciaire est :

c) un expert enregistré et assermenté qui intervient dans le cadre d'une enquête avec des compétences propres.

10) L'ANSSI dépend :

c) du Premier ministre (et non du ministère de la Défense comme on l'entend souvent)

11) Données personnelles :

Dans cette liste seul le mot de passe n'est pas une donnée personnelle.

12) L'outil PIA est proposé par la CNIL pour :

c) faire une analyse d'impact relativement au RGPD.

13) La directive NIS prévoit :

tout sauf de signaler les auteurs d'infraction.

14) Un CERT offre un service de :

a) réponse à incident ;

c) veille.

15) Un dispositif de surveillance (au sens juridique bien sûr) est destiné à :
c) surveiller l'usage des TIC par les salariés.

16) Arguments a priori recevables pour déclarer un dispositif de surveillance :
a) protéger les données personnelles : le but est louable mais il convient de vérifier que les moyens soient proportionnés ;
d) lutter contre les fuites de données : dans certaines entreprises, cela a du sens d'éviter que dans les communications vers l'extérieur, les salariés révèlent (même à leur insu) des informations confidentielles à l'entreprise : nom de personnes, rôles, projets et contenus, etc.
e) lutter contre le télé-chargement illicite : cela révèle un usage abusif de son outil de travail.

17) Durée de conservation des logs :
d) 12 mois Cela fait partie des obligations légales des FAI. Pour une entreprise quelconque, on ne peut que conseiller de conserver les logs de connexion en perspective d'une enquête où cette entreprise serait victime.

18) Pour mettre en place un système de surveillance :
Un parcours juridique est obligatoire : soit les réponses b, c et d.

19) Une entreprise qui conçoit des systèmes embarqués (aéronautique) veut mettre en place un dispositif de filtrage des mails sortants :
Le justificatif peut être de protéger des données sensibles de l'entreprise (contre l'exfiltration notamment) : données techniques, données personnelles (salariés, clients, fournisseurs).

20) Cas d'étude.
a) Pour être valide une délégation de pouvoir doit être confiée à une personne qui a la compétence nécessaire, qui a l'autorité pour la mener, elle doit être unique.
b) La responsabilité de l'entreprise pourrait être engagée pour complicité par fourniture de moyen (le poste de travail), puisqu'une partie des faits n'a pas été détecté au niveau des infrastructures de sécurité. Si les faits étaient détecté au niveau d'un service de police, l'entreprise pourrait faire l'objet d'une réquisition judiciaire pour tracer en interne le poste du contrevenant, ou simplement faire l'objet d'une perquisition.
c) L'entreprise doit édicter un règlement intérieur avec une charte d'usage des SI, mentionnant un certain nombre d'interdictions tel que la consultation de contenus illicites et rappelant que tous les collaborateurs doivent respecter la législation en vigueur. Elle devra s'assurer de réaliser des rappels réguliers (via des affiches ou des mails) sur le respect des règles d'utilisation du SI.
d) Pour dégager la responsabilité du RSSI et la responsabilité morale de l'entreprise, le RSSI devra mettre en exergue toutes les actions qu'il a entrepris pour empêcher les faits (blocage de sites, charte, affiches ou rappels par mails sur l'utilisation du SI du groupe). Au vu de ces éléments, il conseillera de déposer plainte pour abus de confiance (article 314-1 du Code pénal), car de la part du contrevenant, il y a eu détournement de la finalité du poste de travail.

Bibliographie



- [1] DARPA Internet Program. Internet protocol, rfc 791. <https://www.rfc-editor.org/rfc/pdfrfc/rfc791.txt.pdf>, 1981.
- [2] S. Deering and R. Hinden. Internet protocol, version 6 (ipv6) specification, rfc 2460. <https://www.rfc-editor.org/rfc/pdfrfc/rfc2460.txt.pdf>, 1998.
- [3] Y. Rekhter, B. Moskowitz, D. Karrenberg, G.J. De Groot, and E. Lear. Address allocation for private internet, rfc 1918. <https://www.rfc-editor.org/rfc/pdfrfc/rfc1918.txt.pdf>, 1996.
- [4] ANSSI. Recommandations pour la définition d'une politique de filtrage réseau d'un pare-feu. https://www.ssi.gouv.fr/uploads/IMG/pdf/NP_Politique_pare_feu_NoteTech.pdf, 2013.
- [5] J-P. Briffaut. *Processus d'entreprise pour la gestion*. Hermes, 2004.
- [6] L. Atzori, A. Iera, and G. Morabito. The internet of things : a survey. *Computer Networks*, 54 :2787–2805, 2010.
- [7] B. Dorsemaine and J-Ph. Wary. Une approche de l'internet des objets en entreprise et de la déperimétrisation. *MISC*, 86 :25–40, 2016.
- [8] Mitre.org. Att&ck matrix for enterprises. <https://attack.mitre.org/matrices/enterprise/>, 2022.
- [9] CERT-FR. Etat de la menace rançongiciel à l'encontre des entreprises et des institutions. <https://cert.ssi.gouv.fr/cti/CERTFR-2020-CTI-001/>, 2020.
- [10] CLUSIF. Les fondamentaux de mehari. <https://clusif.fr/services/management-des-risques/les-fondamentaux-de-mehari/>, 2022.
- [11] ANSSI. La méthode ebios rm. <https://www.ssi.gouv.fr/administration/management-du-risque/la-methode-ebios-risk-manager>, 2022.
- [12] Parlement européen. Règlement général sur la protection des données- rgpd. <https://www.cnil.fr/fr/reglement-europeen-protection-donnees>, 2018.
- [13] CNIL. Outil privacy impact assessment (pia). <https://www.cnil.fr/fr/outil-pia-telechargez-et-installez-le-logiciel-de-la-cnil>, 2018.
- [14] Parlement. Décret du 20 octobre 2021, relatif aux catégories de données conservées par les opérateurs de communication électronique,

- pris en application de l'article l34-1 du code des postes et communications électronique. <https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000044228877>, 2021.
- [15] ANSSI. Protection des oiv en france. <https://www.ssi.gouv.fr/entreprise/protection-des-oiv/protection-des-oiv-en-france/>, 2013.
- [16] ANSSI. Nis, un dispositif de cybersécurité pour les opérateurs de services essentiels. <https://www.ssi.gouv.fr/entreprise/reglementation/directive-nis/nis-un-dispositif-de-cybersecurite-\pour-les-operateurs-de-service-essentiel/#a1>, 2018.
- [17] ANSSI. Pssi- guide d'élaboration de politiques de sécurité des systèmes d'information. <https://www.ssi.gouv.fr/guide/pssi-guide-delaboration-de-politiques-de-securite-des-\systemes-dinformation/>, 2004.
- [18] ANSSI. Agence nationale de la sécurité des systèmes d'information. <https://www.ssi.gouv.fr/>, 2022.
- [19] ANSSI. Programme secnumedu. <https://www.ssi.gouv.fr/entreprise/formations/secnumedu/contenu-pedagogique-cyberedu/>, 2022.
- [20] CNIL. Commission nationale de l'informatique et des libertés. <https://www.cnil.fr/>, 2022.
- [21] SDLC. Sous-direction de lutte contre la cybercriminalité. <https://oclcctic.fr/>, 2022.
- [22] SDLC. La plateforme pharos. <https://www.gouvernement.fr/la-plateforme-pharos>, 2009.
- [23] DGSI. Direction générale de la sécurité intérieure. <https://www.dgsi.interieur.gouv.fr/>, 2014.
- [24] TRACFIN. Traitement du renseignement et action contre les circuits financiers clandestins. <https://www.economie.gouv.fr/tracfin>, 2014.
- [25] P. Lallement, G. Malnoury, and A. Corpel. Les besoins de formation en cybersécurité, enquête auprès des entreprises. <https://www.cecycf.fr/activites/formation>, 2014.
- [26] ANSSI. Panorama des métiers de la cybersécurité. www.ssi.gouv.fr/guide/panorama-des-metiers-de-la-cybersecurite/, 2018.

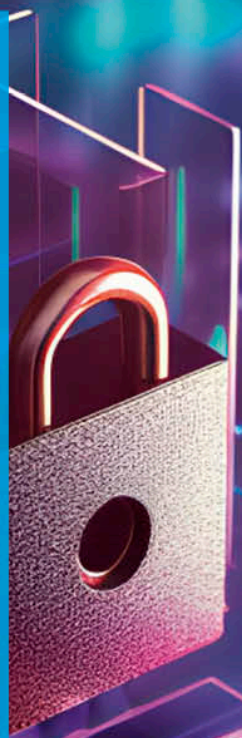
CYBERSÉCURITÉ

Définitions - Concepts - Métiers

Ce livre sur la cybersécurité est structuré en trois parties :

- les **notions clés** de l'informatique et des données du **cyber-espace** ;
- les **failles et les menaces** exploitables par la **cyber-criminalité** ;
- les **différents acteurs et métiers** engagés dans la lutte pour la **cybersécurité**.

Pour les **étudiants, informaticiens** ou **curieux**, c'est une porte d'entrée vers les fondamentaux de la cybersécurité qui posent plusieurs jalons essentiels à la compréhension des **enjeux du numérique** : des **schémas**, des **QCM** et leurs **corrigés** sur un sujet qui concerne tout un chacun.



www.editions-ellipses.fr

