Camille de Sagazan

Introduction à la cybersécurité



ellipses

Références sciences

Introduction à la cybersécurité

Camille de Sagazan

ellipses

Collection Références sciences

dirigée par Paul de Laboulaye
paul.delaboulaye@editions-ellipses.fr

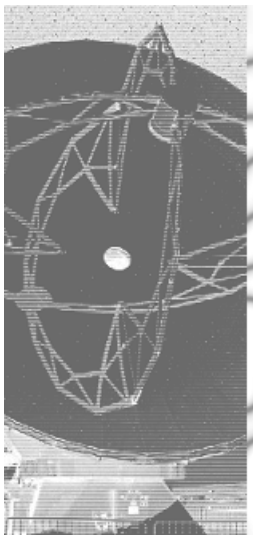
Retrouvez tous les livres de la collection et des extraits sur www.editions-ellipses.fr

ISBN 9782340-038011
©Ellipses Édition Marketing S.A., 2020
32, rue Bargue 75740 Paris cedex 15

DANGER
LE
PHOTOCOPILLAGE
TUE LE LIVRE

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

L'objectif général de cet ouvrage est de présenter un certain nombre de notions de base et de fixer certaines terminologies dans le domaine de la cybersécurité. Il correspond à une tentative de ma part d'articuler de manière cohérente et méthodique les connaissances que j'ai accumulées en vingt ans d'expérience dans ce domaine, et surtout de fournir des retours sur les avantages ou les difficultés pratiques d'application de tel ou tel concept.

Le contenu de cet ouvrage a été élaboré à partir d'un cours développé en 2016 dans le cadre de la licence professionnelle *Administration et Sécurité des réseaux* (ASUR) de l'IUT de Saint-Malo / Université Rennes 1[1]. Lors des discussions préparatoires avec les responsables de la licence, le but avait d'abord été informellement défini comme « de donner un vernis sécurité » aux étudiants, afin qu'ils aient des repères pour aborder la suite, plus technique, des enseignements de la licence professionnelle ASUR.

On estimait en effet préférable d'introduire, dès le début des enseignements, des termes comme « Identification & Authentification » ou bien « Contrôle d'Accès » – l'exemple n'est pas anodin, beaucoup de gens confondent encore les deux –, plutôt que de les expliquer « à chaud » en plein milieu d'une séance sur la sécurisation d'un routeur ou d'un système d'exploitation.

1 Cette formation a obtenu le label *SecNumEdu* de l'ANSSI en 2017.
Cf. https://www.ssi.gouv.fr/particulier/formations/secnumedu/

Plus généralement, il s'agissait de donner aux étudiants une idée du cadre général dans lequel leur activité future d'administrateurs de la sécurité des réseaux allait prendre place : la Politique de Sécurité des organisations pour lesquelles ils allaient travailler, ou leur Système de Management de la Sécurité de l'Information. Il fallait leur apporter des informations sur les notions pertinentes vis-à-vis de la Politique de Sécurité – les risques, les menaces, les contraintes légales et réglementaires, les (éventuelles) bonnes pratiques internes –, qui allaient directement influer sur le contenu de leur travail quotidien en environnement professionnel.

Le cours est donc le premier que suivent les étudiants de la licence professionnelle ASUR, et il sert d'entrée en matière pour la suite. Après quelques étapes de raffinement, ses objectifs ont été formalisés de la manière suivante :

- Donner un aperçu de ce en quoi consiste la cybersécurité : notions, vocabulaire, exemples, historique, références ;
- Fournir des conseils permettant d'initialiser une démarche de cybersécurité au sein d'une organisation. Donner des pistes et des points de repère sur les manières de construire la confiance dans les caractéristiques de cybersécurité d'un produit sur étagère, d'un système opérationnel ou d'une offre de services informatiques ;
- Développer le jugement critique, présenter des principes permettant de se positionner vis-à-vis d'un discours managérial, commercial, économique ou politique touchant à la cybersécurité.

Cela dit, en dehors des élèves en IUT d'informatique se spécialisant dans des disciplines ayant trait à la cybersécurité, qui ce cours est-il susceptible d'intéresser ? Je crois que pourront en tirer profit tous les lecteurs qui se demandent « *par où commencer pour comprendre la cybersécurité ?* ».

Je pense à des personnes en charge de la gestion des « moyens informatiques » d'une organisation, bien souvent à côté d'autres responsabilités comme les moyens généraux, les achats, la sécurité des personnes et des conditions de travail, ou la gestion du patrimoine immobilier. Ces gens travaillent dans des petites entreprises, voire dans des structures associatives, ou bien encore dans des entreprises de taille moyenne, qui ont des moyens financiers plus significatifs à consacrer à l'informatique, mais une culture encore peu développée en ce qui concerne la cybersécurité.

C'est un euphémisme de dire qu'ils peuvent se sentir un peu désarmés face au monde de la cybersécurité, tel qu'il se présente dans les articles des journaux et des blogs, ou à travers les reportages télévisés, les ouvrages spécialisés, les discours des « vendeurs de sécurité » ayant pignon sur rue, ou encore celui des autorités.

La cybersécurité est un sujet à la mode : on en parlait bien moins avant. L'émergence de ces sujets est liée, nous allons le voir, à deux facteurs : (1º) nous sommes devenus en deux décennies de plus en plus dépendants de l'informatique, et surtout

de l'informatique connectée (Internet…), (2º) durant les deux dernières décennies, la menace a évolué, de sorte que des attaques qui paraissaient auparavant compliquées à mettre en œuvre sont devenues communément réalisables, parce que les acteurs derrière ces attaques ont basculé d'un profil de dilettante solitaire à celui de délinquant organisé.

Il y a de quoi ne pas dormir la nuit, quand on pense à tout ce qui peut arriver. « Et tel produit "bleeding-edge technology" dont le commercial m'a chanté les louanges au dernier salon professionnel, est-il vraiment efficace ? Et est-ce que je vais arriver à le configurer et à le maintenir ? Et à justifier le coût de son achat ? Et tel choix d'architecture, est-il pertinent ? Et telle vulnérabilité dont untel m'a parlé à midi en disant que c'était super-dangereux, est-ce que je suis exposé ? » Etc.

Ce livre a aussi pour but de permettre à ces gens de dormir la nuit.

Pour qu'ils puissent dormir la nuit, il faut qu'ils aient confiance dans le fait qu'ils sont en sécurité. Je parle bien sûr d'une confiance *relative*, car nous allons voir que la sécurité absolue n'existe pas. Il faut qu'ils puissent se dire que, si un problème survient, il sauront justifier vis-à-vis de leur direction :

- soit que l'occurrence de ce problème était hautement improbable,
- soit qu'il était imprévisible compte-tenu de la compréhension qu'on avait des risques au moment où les décisions portant sur la cybersécurité ont été prises,
- soit que les moyens qui auraient permis de prévenir le problème avaient un coût bien supérieur au préjudice subi,
- soit, tout simplement, que d'autres moyens permettant de corriger ou de pallier le problème – faute de pouvoir empêcher son occurrence – ont été prévus et ont fonctionné.

Il faut donc pouvoir raisonner, penser la sécurité, dérouler des arguments convaincants. Commencer par se convaincre soi-même, bien dormir, puis arriver frais et dispos en comité de direction pour convaincre les autres.

C'est ce que je me propose de vous apporter dans ce livre : des briques de base, des manières de penser, des réflexes intellectuels qu'on trouve dans les grandes structures qui ont les moyens d'entretenir des populations d'experts et autres responsables sécurité, dont le rôle est précisément et uniquement cela : construire et maintenir la confiance dans la sécurité du Système d'Information de l'entreprise.

Au fil des années, ces groupes ont développé un cadre conceptuel et de travail – les Systèmes de Management de la Sécurité de l'Information – servant à structurer et à contrôler l'action dans le domaine de la cybersécurité.

Je suis convaincu que ce cadre est adaptable de manière pragmatique aux structures plus petites ou moins bien armées pour relever les défis informatiques, à condition bien sûr de se fixer des objectifs en rapport avec les problèmes que les moyens de la structure peuvent adresser.

J'espère que vous trouverez dans ce livre les éléments qui vous permettront de *bien penser* la cybersécurité. Et de bien dormir.

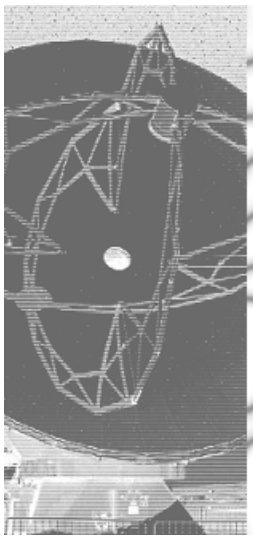


Table des matières

Avant-propos....3

Chapitre 1. Introduction....9

1.1 Les enjeux de la cybersécurité....9
1.2 Une définition de la cybersécurité....11
1.3 Principe et plan de cet ouvrage....14

Chapitre 2. Systèmes de Management de la Sécurité de l'Information....17

2.1 Justifier les mesures de sécurité....17
2.2 Généralités sur les mesures de sécurité....21
2.2.1 Mesures et objectifs de sécurité....21
2.2.2 Mesures de sécurité techniques et non-techniques....23
2.2.3 Des mesures de sécurité au SMSI....24
2.3 Contrôle d'accès....28
2.4 Journalisation, imputabilité et audit....30
2.5 Identification & authentification....39
2.6 Sécurisation du réseau....44
2.7 Sécurisation des locaux et de l'environnement de travail....56
2.8 Mesures de sécurité relatives au personnel....60
2.9 Classification et marquage....65
2.10 Estimation et traitement des risques....68
2.11 Gestion des biens sensibles....72
2.12 Résumé....77

Chapitre 3. La cybersécurité dans le développement....79

3.1 Notions-clés pour la cybersécurité dans le développement....84
3.1.1 Menace....85
3.1.2 Vulnérabilités et bugs de sécurité....86
3.1.3 Mécanismes de sécurité....89
3.1.4 Argumentaires de sécurité....90

3.2 Rôles et responsabilités pour la sécurité dans le développement....94
3.2.1 Le pôle d'expertise en cybersécurité....95
3.2.2 L'expert cybersécurité projet....96
3.2.3 L'équipe de développement....97
3.3 La cybersécurité à chaque étape du développement....98
3.3.1 Études, préparation, démarrage....99
3.3.2 Planification, spécification et conception....104
3.3.3 Implémentation, vérification et validation....110
3.3.4 La sécurité de l'environnement de développement....115
3.4 Résumé....116

Chapitre 4. Cybersécurité opérationnelle....119
4.1 Gestion des identités et des autorisations....121
4.2 Maintien en Condition de Sécurité....124
4.3 Audits de sécurité périodiques....127
4.4 Fin de vie et recyclage....131
4.5 Résilience opérationnelle des SI....132
4.6 Réponse à incident de sécurité informatique....135
4.6.1 Préparation....137
4.6.2 Détection & Analyse....140
4.6.3 Endiguement, Éradication & Reprise....144
4.6.4 Clôture....146
4.7 Plan de Secours des Systèmes d'Information....150
4.7.1 Préparation....150
4.7.2 Détection & analyse....155
4.7.3 Reprise....158
4.7.4 Clôture....162
4.8 Résumé....163

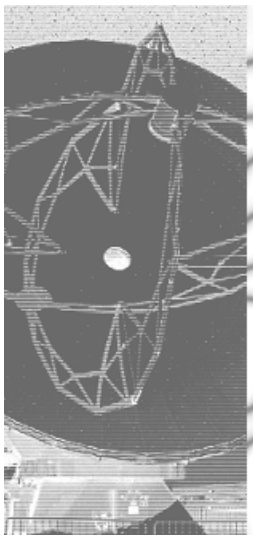
Chapitre 5. Cyberattaques, cybercriminalité, cyberguerre….....165
5.1 Une brève histoire de la SSI / cybersécurité....166
5.2 Cyberattaques, cybercriminalité, cyberespionnage....172
5.2.1 Les malwares....172
5.2.2 La cybercriminalité....173
5.2.3 Le cyberespionnage....178
5.3 Cyberguerre et cyberdéfense....185
5.3.1 Un exemple de cyberattaque étatique : Stuxnet....186
5.3.2 Stratégie de cyberdéfense des États....190
5.3.3 L'approche française....195
5.4 Résumé....198

Perspectives et conclusions....201
L'informatique en nuage....202
Le Big Data....206
Les objets communicants....210
Conclusion : Penser la cybersécurité....212

Liste des abréviations....219

Bibliographie....223

Index....231



Chapitre 1. Introduction

1.1 Les enjeux de la cybersécurité

Pourquoi parle-t-on de cybersécurité ?

Les cinq dernières années ont vu apparaître une discipline *apparemment* nouvelle, et un terme nouveau pour la désigner, au sein du domaine technique des Technologies de l'Information et de la Communication. Cette discipline, c'est la *cybersécurité*. Or, cela fait environ cinquante ans que les problèmes relevant de ce qui s'appelait auparavant la « sécurité informatique » ou encore la « sécurité des systèmes d'information » ont été énoncés, et que certaines solutions ont été apportées. Pourquoi parle-t-on *maintenant* de cybersécurité ? Pourquoi en parle-t-on de plus en plus ?

Une première réponse est que c'est parce que de plus en plus de monde s'en préoccupe. Nous sommes de plus en plus dépendants d'« Internet » – plus exactement des informations et des services qu'il fournit – dans notre vie privée et professionnelle, et ce changement de notre mode de vie s'accompagne de nouvelles, d'histoires, de rumeurs concernant des fraudes, des escroqueries, du chantage, des usurpations d'identité, de la manipulation mentale, etc. véhiculées par ce medium.

Pour le grand public, ces problèmes n'existaient pas il y a vingt ans, puisqu'il y a vingt ans les smartphones existaient à peine, on ne passait pas sa vie sur les réseaux

sociaux, le commerce, la vidéo et le jeu en ligne étaient moins développés à cause de la faiblesse du débit du réseau et de celle des performances des technologies Web.

Les problèmes de sécurité informatique se posaient alors principalement dans le contexte des réseaux d'entreprise, et les « hackers » étaient vus comme des bidouilleurs isolés qui dévoyaient leur talent à tenter de « casser » les systèmes pour des raisons narcissiques et ludiques.

Or – et c'est un deuxième élément de réponse – cette vision des *attaquants* a également dû être remise en cause durant les vingt dernières années. Nous allons voir que la *cybercriminalité* est en réalité le fait de groupes structurés, mêlant experts en informatique et délinquants classiques, et essentiellement motivés par l'appât du gain. *L'impact financier de la cybercriminalité se chiffre en centaines de milliards d'euros*. Mais cette prise de conscience du public est récente, elle remonte tout au plus à une dizaine d'années.

Enfin, une troisième réponse est qu'Internet a longtemps eu l'image d'un milieu ouvert à la liberté d'expression et soustrait à l'autorité des États – en particulier totalitaires. C'était l'outil rêvé de la mondialisation et de l'expansion de la démocratie libérale. Or, un certain nombre d'affaires, comme les révélations d'Edward Snowden en 2013, les polémiques sur le traitement des données personnelles par les géants du Web, ou encore les informations sur la manière dont les terroristes djihadistes utilisent Internet pour recruter des individus influençables et coordonner leur actions à distance, ont fait apparaître l'« espace Internet » comme un milieu soumis à la surveillance et au contrôle d'acteurs puissants, beaucoup plus dangereux et porteur de risques que l'image qui a prévalu dans la première décennie du XXI^{e} siècle.

Mais les solutions que propose la cybersécurité ne sont pas apparues aussi récemment que la popularisation de la discipline peut le laisser penser. De notre point de vue, il y a plutôt eu, en vingt ans, une *transition* du domaine de la sécurité des systèmes d'information vers celui de la cybersécurité. Comme nous le verrons plus tard, la différence entre les deux est essentiellement une question de contexte, d'époque et de perception du grand public, mais pas de méthodes.

Pourquoi en faire un métier ?

Une des raisons qui vous a peut-être amené·e à acheter cet ouvrage est que vous souhaitez faire carrière dans la cybersécurité. C'est un très bon choix – de carrière ; pour l'ouvrage, vous jugerez ! La cybersécurité est *un secteur qui recrute* et *qui peut être très bien payé* : en 2016, un article du *Monde* [1] estimait que le marché proposait 5 000 offres d'emploi dans le secteur, et que 1 000 d'entre elles n'étaient

pas pourvues. Pour des profils d'ingénieurs débutants, des salaires annuels de départ avoisinant les 38 000 euros bruts étaient annoncés.

Mais un des grands attraits de la cybersécurité réside pour nous dans le fait que *c'est techniquement passionnant*. C'est une activité dans laquelle il faut être *polyvalent*, posséder une vaste culture aussi bien dans le domaine de l'informatique (systèmes d'exploitation, langages de programmation, serveurs d'application, bases de données, cryptographie, etc.) que des réseaux. Il importe également, vis-à-vis du corpus technique, d'avoir du *recul*, de l'*esprit critique* ainsi qu'un *esprit de synthèse*. Et puis ce n'est *pas que technique* : quand on doit contribuer à la sécurisation d'un système d'information, il faut savoir *comprendre les besoins métier* auxquels le système d'information répond, *justifier et valoriser les mesures de sécurité* vis-à-vis des parties prenantes et également prendre en compte certains *facteurs humains* relevant de l'ergonomie, de la communication ou de la psychologie.

Et enfin : *cela bouge tout le temps* ! Nous avons illustré le fait que l'état actuel de la menace est très différent de celui d'il y a vingt ans. Dans les années à venir, avec la généralisation de l'informatique en nuage et surtout des objets communicants, de nouvelles menaces apparaîtront et de nouveaux défis devront être relevés.

1.2 Une définition de la cybersécurité

La cybersécurité semble recouvrir le domaine d'étude de ce qu'on appelait auparavant la *sécurité informatique*. On parle, dans l'une comme dans l'autre, de contrôle d'accès, de mots de passe, de cryptographie, de vulnérabilités, de failles informatiques, d'attaques, de hackers, etc. Pourtant, de nos jours, le terme « cybersécurité » est le plus fréquemment employé, d'une manière qui suggère qu'il s'agit d'une discipline nouvelle, ayant émergé pour faire face aux nouvelles menaces liées à l'informatisation croissante de la société.

Quelle différence y a-t-il alors entre cybersécurité et sécurité informatique ?

La réponse est simple : *sur le fond, il n'y en a aucune*. Mais alors, pourquoi utilise-t-on deux termes différents ?

C'est essentiellement une question de contexte, d'époque et de perception du grand public. La sécurité informatique représente la facette historique et orientée vers la technique du domaine d'étude dédié à la protection du patrimoine informationnel des organisations.

Sans rentrer dans les détails, au début des années 2000, a émergé l'idée que cette problématique de la protection du patrimoine informationnel ne pouvait pas être garantie de manière satisfaisante uniquement par la maîtrise et la mise en œuvre d'un savoir-faire purement technique, qu'il s'agît par exemple de la sécurité

des systèmes d'exploitation, de celle des réseaux, des antivirus, ou encore de la cryptographie.

Il apparaissait souhaitable de replacer la « sécu » technique dans le cadre de la stratégie de l'organisation, et de fixer des priorités dans la mise en œuvre de ses actions, en confrontant les discours alarmistes des experts sur les attaques, les menaces et les vulnérabilités avec le point de vue de leur applicabilité réelle, de leur vraisemblance et de leur impact. Il semblait également opportun coordonner les efforts consentis pour la sécurité informatique et ceux investis dans la sécurité « du monde réel » : protection des locaux, aspects RH, juridiques ou relatifs aux achats, plans de continuité d'activité, etc. C'est ainsi qu'apparut le terme de « sécurité de l'information », ou encore de « sécurité des systèmes d'information », en France et dans les pays européens.

Aux États-Unis, une réflexion similaire s'était faite, mais elle fut orientée différemment par deux facteurs :

- une prise de conscience brusque et aiguë de l'« attractivité » du pays comme cible d'attaques terroristes, suite aux attentats du 11 septembre 2001,
- une grande sensibilité, dès le début des années 2000, aux problèmes liés à l'interconnexion des systèmes informatiques de contrôle des environnements de fabrication industriels et de production d'énergie (dits « SCADA »), avec les réseaux ouverts comme Internet [2], [3].

C'est pour désigner et adresser cette problématique que le terme « *cyber security* » fut initialement créé. La cybersécurité désignait ainsi spécifiquement la protection contre les risques informatiques susceptibles d'avoir un impact sur les systèmes de contrôle industriels et de distribution d'énergie[1], dans la crainte d'un « cyber-Pearl Harbor », voire d'un « cybergeddon ». Dans les années 2000, seul le gouvernement américain parlait de cybersécurité, et d'une manière qui semblait plus souligner la vastitude du problème que proposer des pistes de solution.

Finalement, la décennie 2010 vit le paysage de la menace informatique évoluer radicalement, comme nous le verrons au chapitre 5. Notre sentiment est que les experts tenants de la « sécurité des systèmes d'information » (SSI) des années 2000 parurent alors un peu dépassés par une menace devenue plus ubiquitaire et plus

1 À l'origine du préfixe « cyber », le terme *cybernétique*, du grec *κυβερνητικός* : art de piloter (un navire), art de gouverner, a été défini au milieu du XIX^{e} siècle comme « l'étude des moyens de gouvernement » – ce qu'on appelle aujourd'hui la « gouvernance » –, puis son sens s'est déplacé vers « l'étude des processus de contrôle et de communication chez l'être vivant et la machine » [4], [5]. Il évoque l'image du *robot*, des systèmes électromécaniques présentant des pièces en mouvement, pilotés par l'informatique.

vraisemblable que le tableau qu'ils en peignaient, qui datait d'avant l'interconnexion généralisée, la mobilité et la généralisation des services Web.

De plus, la SSI ayant été développée par des personnes souvent issues du domaine du développement logiciel, elle n'avait pas de propositions pertinentes à formuler vis-à-vis du domaine de la *sécurité informatique opérationnelle*, c'est-à-dire celui de la sécurité informatique des *plate-formes en exploitation*. Des sujets comme la *détection* et la *réponse aux incidents de sécurité informatique* étaient somme toute assez peu développés par les experts SSI « historiques » – on restait dans des banalités du genre « il faut surveiller les logs et corriger les vulnérabilités » –, alors que ce sujet s'avéra critique dans le cadre de la montée en puissance de l'hébergement de services en ligne qui s'opéra dans cette période – aboutissant au « Cloud ».

L'emploi du terme « cybersécurité » à partir des années 2010 renvoie donc, pour nous, à la nécessité de souligner la réalité des dangers de la menace informatique, par opposition à la décennie 2000 où cette menace paraissait plus hypothétique, au moins du point de vue des organisations. La vision qu'a le grand public du cyberespace bascule de celle d'un formidable outil porteur de la promesse d'un avenir radieux, vers celle d'un médium inquiétant, sous la coupe d'adversaires imprévisibles et exotiques – les « hackers » –, et de ce fait porteur d'un risque illimité car insondable, correspondant à la vision de ceux qui parlaient de « cybersécurité ». Mais sur le fond, on parle de la même chose qu'avec la SSI : concevoir des *mesures de sécurité* pour *réduire*, voire *contrer* les *risques* informatiques.

Terminons par une définition adaptée d'un article de 2017 [6] spécialement dédié à la résolution des ambiguïtés liées au terme :

> « La **cybersécurité** est la stratégie et les actions associées aux processus de gestion des risques sur la sécurité suivis par les organisations et les États dans le but de protéger la confidentialité, l'intégrité et la disponibilité des données et des biens sensibles utilisés dans le cyberespace. Ce concept inclut les lignes directrices, les règles, politiques et ensembles de contrôles, technologies, outils et formations visant à protéger de la meilleure manière l'état de l'environnement cyber et de ses utilisateurs. »

Cette définition nous paraît suffisamment large pour réconcilier, pour autant qu'il y en ait besoin, les différents courants historiques de la sécurité informatique. Dans la suite de cet ouvrage, nous utiliserons de manière interchangeable les termes « cybersécurité », « Sécurité des Systèmes d'Information » (avec ou sans

majuscules) et « sécurité informatique », et cela renverra au champ d'étude délimité par la définition ci-dessus.

1.3 Principe et plan de cet ouvrage

Cet ouvrage se veut consister en une *introduction* à la cybersécurité. Il s'agit pour nous de donner une information générale – nous assumons le terme de « vernis » – sur un certain nombre de notions, de principes et de faits dans ce domaine.

Le découpage, la progression dans l'explication des notions, ainsi que les avis et les conseils que nous avons apportés dans cet ouvrage sont issus de notre expérience professionnelle d'évaluateur SSI, d'ingénieur d'études et de consultant, ainsi que des activités de veille que nous menons. En tant que tels, ils sont nécessairement biaisés par la subjectivité déterminée par ce parcours ; c'est-à-dire qu'un autre professionnel de la cybersécurité, ayant un parcours différent, pourrait présenter les notions dans un ordre différent – voire en choisir d'autres –, et apporter des avis et des conseils différents. Dans la mesure du possible, pour corriger les effets de ce biais inévitable, nous nous sommes astreint à baser nos assertions sur des sources publiques, à recouper ces sources, et à les documenter.

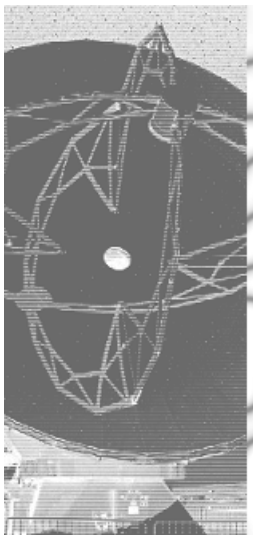
Le plan de cet ouvrage est le suivant :

- Le chapitre 2 introduit la problématique de la sécurisation du système d'information d'une *organisation* – principalement une entreprise, mais aussi potentiellement une administration, ou encore une organisation à but non lucratif. On donne un aperçu des dilemmes auxquels peut être confronté le Responsable de la Sécurité des Systèmes d'Information (RSSI) de l'organisation. Des exemples de mesures de sécurité techniques et non-techniques sont fournis.

  Par delà la mise en œuvre de *mesures de sécurité*, nous argumentons de la nécessité de définir un *cadre* pour le pilotage cette mise en œuvre, son maintien dans la continuité, ainsi que l'énonciation de la problématique de sécurité à laquelle les mesures répondent. Ce cadre constitue le *Système de Management de la Sécurité de l'Information* de l'organisation ;
- Le chapitre 3 met le focus sur les mesures servant à mettre en place *la cybersécurité dans les projets de développement* de systèmes ou de services intégrés dans le système d'information (SI) global de l'organisation. Nous décrivons un modèle standard de processus de développement et expliquons la manière dont l'*Assurance Sécurité* peut se greffer sur les différentes étapes du processus de développement ;
- Dans le chapitre 4, nous abordons la modélisation de l'environnement d'exploitation du SI, dans le but de décrire les processus de *cybersécurité*

opérationnelle. Les thèmes principaux abordés par la cybersécurité opérationnelle sont : la surveillance et le maintien des mesures de sécurité créées lors de la phase de développement, la correction des vulnérabilités du SI au fur et à mesure qu'elles sont publiées, et surtout : la *résilience* face aux événements qui menacent le fonctionnement et la sécurité du SI – c'est l'objet des processus de réponse à incident de sécurité et de secours des systèmes d'information (*contingency planning*) ;

- Le chapitre 5 sort du point de vue du RSSI et met en lumière celui des attaquants. Nous expliquons la manière dont la menace informatique a évolué au cours des vingt dernières années, nous donnons des détails sur les *cyberattaques*, sur le modèle économique de la *cybercriminalité*, ainsi que sur les attaques persistantes avancées (APT). Enfin, nous abordons le sujet de la lutte entre États dans le cyberespace – ce que certains appellent la *cyberguerre* –, et nous présentons la posture stratégique de la France en la matière ;
- Enfin, notre dernier chapitre de *perspectives et conclusions* est l'occasion de faire le point, sous l'angle de la cybersécurité, sur trois technologies qui devraient avoir un fort impact dans les années à venir – le Big Data, l'informatique en nuage (*Cloud computing*), et les objets communicants (*IoT*) – et d'énoncer quelques principes qui devraient, selon nous, guider la pratique et la réflexion des professionnels de la cybersécurité.



Chapitre 2. Systèmes de Management de la Sécurité de l'Information

Pour le néophyte, la cybersécurité est un sujet inquiétant et complexe.

Inquiétant par nature, puisqu'on s'intéresse précisément à la manière dont les choses peuvent *mal* se passer : on prend alors conscience qu'on court des *risques*, qu'on est soumis à la *menace* d'*attaques* cherchant à découvrir et à exploiter des *vulnérabilités*.

Complexe par la quantité et la variété des points à aborder, des solutions et des discours censés répondre à la problématique. Complexe également par l'exigence d'être constamment prêt à justifier à sa direction le caractère nécessaire des actions de mise en œuvre de la sécurité informatique, et leur meilleur rapport efficacité / coût, compte tenu de leur coût et des contraintes qu'elles peuvent entraîner. Complexe enfin parce qu'on cherche à adresser et à raisonner sur l'imprévisible, le peu vraisemblable ou le non-renseigné, ce qui amène nécessairement à développer des argumentaires comprenant des faits plus ou moins avérés, des expériences de pensée de caractère spéculatif, et des scénarios arborescents ; bref des discours difficiles à faire passer auprès d'une direction.

2.1 Justifier les mesures de sécurité

Au sein d'une organisation, le **Responsable de la Sécurité des Systèmes d'Information** (**RSSI**) est donc pratiquement obligé d'adopter une démarche structurée et reconnue pour la mise en œuvre des mesures relevant de son périmètre.

Le point le plus critique sur lequel il va être attendu est celui de la *justification du coût* des mesures de sécurité qu'il a commanditées :

- les coûts directs d'acquisition, de développement et de mise en œuvre,
- et aussi les coûts indirects causés par les changements dans les habitudes, les contraintes nouvelles, l'impossibilité, suite à la mise en œuvre de nouvelles mesures de sécurité, de « faire comme on faisait avant », l'accroissement de la rigueur dans la conduite des processus opérationnels.

Et tout cela – va-t-on lui dire – pour ne pas augmenter le chiffre d'affaires d'un centime, et pour ne pas non plus réduire les coûts de l'informatique d'un centime.

Il faut dire les choses clairement : la cybersécurité *inquiète* les directions parce qu'elle adresse des questions inquiétantes, mais aussi parce qu'elle peut fournir des réponses peu réjouissantes quant aux coûts. Au fond, quand un ensemble de mesures de sécurité fonctionne bien, il ne se passe… rien, puisqu'on ne subit aucun préjudice, *précisément à cause de l'efficacité desdites mesures*. Cela peut vite donner l'idée que les dépenses liées à la mise en œuvre de ces mesures sont inutiles.

Pour répondre à cette interpellation, le RSSI a à sa disposition trois types d'arguments, qui constituent autant d'approches pour la justification de la mise en œuvre des mesures de sécurité :

Estimation des risques

Les défauts de sécurité peuvent entraîner des **préjudices**, typiquement par l'effet de *pertes d'exploitation* qui, en fin de compte, vont se traduire par des *coûts*. Le coût des mesures de sécurité est présenté comme un *investissement*, dont le retour correspond à une « non-perte d'exploitation ». Ce genre d'argument est plus facile à dérouler lorsque les préjudices revêtent effectivement *directement* la forme d'une perte d'exploitation – par exemple, une attaque en déni de service rendant une ou plusieurs fonctions du **Système d'Information** (SI) inopérantes, assortie d'une extorsion de fonds qu'on doit bien consentir à payer pour que cela s'arrête.

Les préjudices de nature commerciale – par exemple : perte de chiffres d'affaires suite à la perte d'un appel d'offres, à cause de la divulgation d'éléments de la réponse commerciale – interpellent également les directions.

Les préjudices de nature juridique sont plus difficiles à chiffrer, et ceux relatifs à l'image de marque le sont encore plus.

Par ailleurs, il importe également de prendre en compte la *vraisemblance* de l'occurrence future de chaque préjudice dans l'estimation du coût qui lui est attaché. Toutefois, l'évaluation de cette vraisemblance – la *probabilité* de l'occurrence du préjudice, ou encore sa *fréquence* – peut prêter à discussion, surtout si le préjudice n'est encore jamais survenu.

Cette approche, qu'on peut qualifier d'*actuarielle* en référence au métier d'assureur, consiste donc à justifier le coût des mesures de sécurité comme inférieur, et préférable, à celui des *préjudices potentiels* auxquels l'organisation est censée s'exposer faute de mettre en œuvre ces mesures. Le terme de **risque** est utilisé pour désigner cette notion de « préjudice potentiel », et la démarche consistant à démontrer l'efficacité des mesures de sécurité en termes de réduction du niveau de ces risques forme le cœur de ce qu'on appelle l'**estimation des risques**.

Exigences externes

Lorsque la situation est trop complexe ou trop incertaine pour dérouler une estimation des risques, ou bien face à un auditoire qui n'est pas prêt à entendre ce genre de discours, le deuxième type d'argument pouvant servir à justifier un ensemble de mesures de sécurité est celui des *exigences externes*. Celles-ci peuvent être de nature :

- *légale ou réglementaire* – par exemple, les exigences de la CNIL ou le RGPD,
- *marketing ou business* – par exemple : on veut développer des services impliquant le paiement en ligne, ce qui impose d'être certifié conforme aux exigences du référentiel PCI-DSS,
- ou encore *contractuelle* : on souhaite répondre à des appels d'offres exigeant a priori d'être conforme à un jeu d'exigences donné, ou bien on a conclu un contrat qui comporte la mise en conformité avec ce genre d'exigences.

Bonnes pratiques

Le troisième type d'argument consiste à faire appel à une notion d'*état de l'art*, ou encore de *bonnes pratiques* en matière de sécurité. Il ressemble au second type d'argument, sauf qu'au lieu de s'appuyer sur des exigences externes qui s'imposent de manière impérative à l'organisation, il fait appel à des bases de légitimité soit *internes* (« les règles opérationnelles disent qu'il faut faire comme cela »), soit externes mais non impératives, correspondant à une notion d'*état de l'art* (« les experts disent qu'il faut faire comme cela »).

Dans certaines organisations de grande taille ayant une bonne maturité dans le domaine informatique, les pratiques de mise en œuvre des systèmes informatiques peuvent être soumises à des *règles d'urbanisme du SI*, dont certaines sont de nature sécuritaire. Ces règles constituent une base de légitimité interne pour les mesures de sécurité qui en découlent.

Dans un registre moins rigoureux – et pour nous moins convaincant –, on peut également ranger dans cette catégorie d'argumentation la justification de l'achat de

Tableau 1. Différents types d'arguments pour la mise-en-œuvre de la sécurité

Type d'argument	Avantages	Inconvénients
Estimation des risques	■ Arguments en termes de coûts qui parlent aux décideurs. ■ Permet de fixer des priorités dans le traitement des risques : on traite en priorité ceux dont le niveau est le plus élevé.	■ L'estimation des risques nécessite une bonne compréhension des enjeux métier, des biens sensibles et de l'architecture à protéger. Elle peut être infaisable pour des systèmes complexes ou mal documentés. ■ Elle peut entraîner des argumentations complexes et, de ce fait, moins convaincantes.
Exigences externes	■ Dans la mesure où la satisfaction des exigences conditionne la recette du SI, la légitimité pour mettre en œuvre les mesures de sécurité est meilleure que dans l'approche basée sur les risques. ■ Les budgets pour mettre en œuvre la sécurité sont présents au titre du contrat.	■ Les exigences externes ne sont pas toujours présentes, ou alors elles sont identifiées a posteriori. ■ Elles peuvent être décorrélées des enjeux de sécurité et des menaces réellement applicables au SI.
Bonnes pratiques	■ La légitimité est presque aussi bonne que celle des exigences externes. ■ Les équipes de développement et d'exploitation savent normalement déjà comment mettre en œuvre les mesures de sécurité. ■ L'existence d'une infrastructure dédiée à la mise en œuvre des bonnes pratiques de sécurité au sein de l'urbanisme du SI global peut constituer un facilitateur.	■ Les bonnes pratiques peuvent être décorrélées des enjeux de sécurité et des menaces réellement applicables au SI, car elles font complètement l'impasse sur ces sujets. ■ Elles peuvent manquer de flexibilité. Elles peuvent être remises en cause par le business car vues comme des facteurs de blocage.

tel ou tel équipement de sécurité sur la base de sa réputation, parfois sans la moindre considération pour l'adéquation de ses fonctionnalités de sécurité vis-à-vis des risques opérationnels.

Cependant, cette argumentation basée sur les bonnes pratiques et l'expertise aura beaucoup de mal à faire face aux considérations de « gouvernance responsable », d'« alignement sur le business » et autres « lean management », qui placent l'analyse de la valeur, la transparence et la justification au cœur des processus de décision et d'organisation.

En effet, l'approche basée sur les bonnes pratiques et l'expertise présente l'inconvénient d'un certain arbitraire. En faisant référence à des bonnes pratiques que l'interlocuteur ne connaît pas, ou à une expertise qu'il ne possède pas, on court

le risque d'être perçu comme ayant recours à un argument d'autorité à l'emporte-pièce.

Cette approche peut aussi donner une impression de manque de flexibilité : les bonnes pratiques sont conçues par rapport à des situations standard et bien éprouvées, et elles peuvent ainsi s'avérer difficiles à adapter aux « ruptures » qui tendent à devenir la norme dans les métiers de l'informatique.

Le tableau 1 récapitule les avantages et les inconvénients de chaque approche. Une bonne stratégie de justification des mesures de sécurité repose sur une combinaison de ces trois approches qui soit adaptée :

- À l'auditoire, c'est-à-dire aux décideurs auxquels il va falloir « vendre » la mise en œuvre des mesures de sécurité. N'oublions pas que ce sont eux qui, si les risques se réalisent, vont en assumer la responsabilité ;
- À la complexité de la problématique de sécurité à adresser, en liaison avec celle du SI et de l'organisation. Une situation trop complexe ou trop incertaine ne permet pas de dérouler l'exercice de sécurité raisonnée que constitue l'estimation des risques ;
- Aux exigences et à l'appétence du business pour la mise en œuvre de la sécurité. Certains segments de marchés ne sont tous simplement pas encore prêts à financer cette mise en œuvre. Par exemple, le secteur des objets connectés (« l'Internet des objets ») manque encore de la culture sécurité de base qui lui permettrait de ne plus laisser persister les failles de sécurité les plus élémentaires dans ses produits [7], [8], [9], [10].

2.2 Généralités sur les mesures de sécurité

2.2.1 Mesures et objectifs de sécurité

Avant d'introduire et de développer plus en détail les notions de SMSI et d'estimation des risques, il nous semble utile de donner des exemples de ce en quoi consistent les fameuses *mesures de sécurité*, dont la mise en œuvre constitue la quête principale du RSSI.

Tableau 2. Exemples de mesures de sécurité

Catégorie	Exemples
Techniques	■ contrôle d'accès ■ journalisation ■ filtrage réseau ■ VPN ■ redondance d'équipements avec bascule à chaud ou à froid
Relatives au personnel	■ enquêtes avant embauche ■ sensibilisation et formation à la sécurité ■ dispositions du contrat de travail relatives au secret professionnel ■ séparation des tâches
Organisationnelles	■ répartition des rôles et des responsabilités dans la définition et la mise en œuvre des mesures de sécurité ■ inventaire des biens sensibles ■ définition des niveaux de sensibilité ■ sécurité dans les relations avec les tiers (clients, fournisseurs, partenaires, autorités) ■ prise en compte de la conformité légale et réglementaire ■ amélioration continue de la sécurité
Physiques	■ contrôle d'accès aux locaux, vidéosurveillance, alarmes anti-intrusion ■ prévention des sinistres ■ protection contre les signaux électromagnétiques compromettants ■ protection de l'accès physique aux réseaux (filaires ou sans-fil) ■ stockage des supports d'information sensible dans des tiroirs fermant à clé, voire dans des armoires fortes ■ destruction / recyclage des supports d'information sensible

Nous définissons les *mesures de sécurité* et les *objectifs de sécurité* de la manière suivante :

> Une **mesure de sécurité** est une disposition, procédure, action, règle ou activité contribuant à satisfaire un ou plusieurs *objectifs de sécurité*.
>
> Un **objectif de sécurité** est un but intermédiaire, mesurable, à atteindre pour satisfaire un des types d'exigences suivants :
>
> ■ réduire, voire contrer, un *risque*,
>
> ■ satisfaire une *exigence externe* de type légal, réglementaire, business ou contractuel,
>
> ■ respecter une *bonne pratique* correspondant à l'état de l'art, ou bien encore faisant partie des règles d'urbanisme du SI.