Sécurité informatique

4e édition

Principes et méthodes
à l'usage des DSI, RSSI et administrateurs

Laurent Bloch

Christophe Wolfhugel

Préfaces de Christian Queinnec et Hervé Schauer
Avec la contribution de Nat Makarévitch

EYROLLES

 ISBN : 978-2-212-13737-8

Préface

L'Internet, on le lit souvent, est une jungle, un lieu plein de dangers sournois, tapis et prêts à frapper fort, péniblement et durablement. On aura intérêt à ne pas s'attarder sur cette banalité car la jungle est en l'occurrence l'endroit où l'on doit obligatoirement vivre. En revanche, tout comme pour certaines maladies transmissibles, être ignare, ne pas vouloir apprécier les dangers, persister à les ignorer sont des attitudes blâmables.

Par contre, un ordinateur est un assemblage hétéroclite, historiquement enchevêtré, de matériels et de logiciels dont les innombrables interactions sont au-delà de l'humainement appréhendable. Un ordinateur est tout autant une jungle, qui même s'étend au fil de ses expositions successives à Internet.

Comme dans tant d'autres domaines sociétaux, la « sécurité » est réputée être la solution à ces problèmes !

Mais plus que de bonnement nommer cette solution, d'espérer un monde meilleur où l'on pourrait enfin jouir de cette fameuse sécurité, il faut s'interroger sur son existence, sa nature, ses constituants, ses conditions d'apparition ou de disparition, son développement, etc. C'est précisément à ces interrogations que répond l'ouvrage de Laurent Bloch et Christophe Wolfhugel.

Un tel état de grâce ne s'obtient ni par décret, ni par hasard. C'est le résultat d'une confluence opiniâtre de comportements et de solutions techniques. Ces dernières existent depuis l'article séminal de Diffie et Hellman [50] publié en 1976, qui a permis de résoudre le problème, ouvert depuis des millénaires : comment deux personnes, ne se connaissant au préalable pas, peuvent-elles élaborer un secret commun à elles seules en n'ayant échangé que des messages publics ? Clés publiques

et privées, certificat, signature électronique sont les plus connues des innovations dérivées de cet article. Notariat électronique, respect de l'anonymat (réseau TOR), crypto-virus blindés en sont d'autres plus confidentielles.

Si, dès maintenant, des solutions techniques existent pour un monde meilleur, sur le plan humain le salut peine à s'instaurer. On ne peut souhaiter un monde sûr que si l'on prend la mesure de l'actuelle insécurité. On ne peut espérer un monde plus sûr que si l'on sait qu'il est réalisable, que si l'on est prêt à tolérer des changements personnels importants de comportement, si l'entière société humaine stimule l'adoption de ces nouvelles règles et veille à les adapter au rythme des inéluctables évolutions.

La sécurité n'est qu'un sentiment dont l'éclosion est due à la conjonction de facteurs techniques et sociétaux. La mise en place d'un contexte favorable à ce sentiment est complexe, tant sont grandes les difficultés de réalisation et les oppositions entre les différentes inclinations libertaires, dirigistes ou *Big Brother*-iennes. L'anonymat est-il autorisé sur Internet ? Puis-je mettre mon ordinateur en conformité avec mes désirs sécuritaires ? Comment rétribuer une création intellectuelle incarnée numériquement *(sic)* et dont la duplication est quasiment gratuite ? Devons-nous laisser l'offre des industriels diriger notre morale et notre liberté ?

L'excellent livre de Laurent Bloch et Christophe Wolfhugel a pour thème la sécurité. Loin de s'appesantir sur les seuls aspects techniques ou de broder autour de banalités comme « la sécurité parfaite n'existe pas » ou encore « avoir listé les menaces garantit une éternelle quiétude », ce livre est à lire et à méditer par tous ceux qui y croient et tous ceux qui n'y croient pas afin que tous puissent participer intelligemment à l'avènement de l'ère numérique. Cet espace incommensurablement démocratique (les internautes votent avec leur souris) que réalise l'interconnexion de toutes les puces calculantes, nous avons une chance de modeler son avenir tout autant que de le transformer en le plus effroyablement fliqué lieu communautaire. À nous de choisir, à la lueur de ce que nous en dit cet ouvrage.

Christian Queinnec
Professeur à l'université
Pierre et Marie Curie

Préface II

Alors que la sécurité des systèmes d'information était un produit de luxe, elle tend aujourd'hui à devenir un moyen d'apporter la confiance au cœur des affaires.

Cet ouvrage en rappelle les bases techniques et présente une perspective nouvelle, pertinente et utile à tous les acteurs du secteur de la sécurité des systèmes d'information, par deux esprits vifs, qui ont prouvé, par leur carrière et leurs réalisations, leur indépendance et leur compétence.

Hervé Schauer
Consultant en sécurité
des systèmes d'information
depuis 1989

Table des matières

Avant-propos

Ce livre procurera au lecteur les connaissances de base en sécurité informatique dont aucun utilisateur d'ordinateur ni aucun internaute ne devrait être dépourvu, qu'il agisse dans le cadre professionnel ou à titre privé. Nous proposons ainsi des pistes pour aider chacun à voir clair dans un domaine en évolution rapide, où l'information de qualité est parfois difficile à distinguer au sein du vacarme médiatique et des rumeurs sans fondement.

Plutôt que de proposer des recettes à appliquer telles quelles, et qui dans un domaine en évolution rapide seraient de toute façon vouées à une prompte péremption, nous présenterons des axes de réflexion accompagnés d'exemples techniques.

L'Internet est au cœur des questions de sécurité informatique : nous rappellerons brièvement ses principes de fonctionnement, placés sous un éclairage qui fera apparaître les risques qui en découlent. Pas de sûreté de fonctionnement sans un bon système d'exploitation : nous passerons en revue les qualités que nous sommes en droit d'en attendre. Nous examinerons les différentes formes de malfaisance informatique, sans oublier les aspects organisationnels et sociaux de la sécurité. Pour les entreprises, nous proposerons quelques modèles de documents utiles à l'encadrement des activités informatiques de leur personnel.

La protection des systèmes d'information repose aujourd'hui sur la cryptographie : nous donnerons un exposé aussi simple que possible des principes de cette science, qui permettra au lecteur qui le souhaite d'en comprendre les bases mathématiques. Celui qui serait rebuté par ces aspects pourra en première lecture sauter sans trop de dommages ces développements.

Nous poursuivrons par un tour d'horizon des possibilités récentes de l'Internet, qui engendrent de nouveaux risques : échanges de fichiers pair à pair, téléphonie sur IP, publication de données personnelles sur les réseaux sociaux...

Enfin l'Internet joue dans la politique et l'économie mondiales un rôle comparable à celui des océans entre 1800 et 1930, et les États-Unis y occupent une position dominante analogue à celle de la Grande-Bretagne sur les mers à l'époque victorienne, cependant que les points d'échanges de l'Internet (IXP) sont aussi importants stratégiquement que les Dardanelles et le canal de Suez l'étaient à cette époque. Il serait donc étonnant qu'un espace public d'une telle importance stratégique ne soit pas l'objet de rivalités et de conflits, et effectivement rivalités et conflits y éclatent. La *cyberdéfense* et la *cyberstratégie* deviennent des préoccupations centrales pour tous les gouvernements, plus de trente pays ont créé des unités de cyberdéfense. Nous avons consacré notre chapitre nº 13 p. 299 aux questions de sécurité, de défense et de stratégie dans le cyberespace.

Cyberespace

Nous pouvons définir le cyberespace comme un espace informationnel, c'est-à-dire comme une réunion d'ensembles de données, de circuits de communication et de modèles sémantiques, dont le support est l'Internet.

Michel Volle [1] nous suggère que « plusieurs dialectiques se nouent [dans le cyberespace] : celle de la centralisation des ressources informatiques, avec le "cloud computing" [l'informatique en nuage], et de la décentralisation des accès et interfaces avec l'Internet des objets ; celle du cyberespace, négation de la distance géographique, et de l'espace physique à trois dimensions dans lequel sont plongés nos corps et nos biens ; celle aussi, nous le verrons, du droit et de la violence. »

Les lignes qui suivent sont avant tout le fruit de nos expériences professionnelles respectives, notamment dans les fonctions de responsable de la sécurité des systèmes d'information de l'Institut national de la santé et de la recherche médicale (INSERM) pour l'un, d'expert des protocoles de l'Internet au sein de la division Orange Business Services de France Télécom pour l'autre.

L'informatique en général, ses domaines techniques plus que les autres, et celui de la sécurité tout particulièrement, sont envahis de « solutions » que des entreprises s'efforcent de vendre à des clients qui pourraient être tentés de les acheter avant d'avoir identifié les problèmes qu'elles sont censées résoudre. Il est vrai que la démarche inductive est souvent fructueuse dans les domaines techniques, et que la démonstration d'une solution ingénieuse peut faire prendre conscience d'un problème, et du coup aider à sa solution. Mais l'induction ne peut trouver son chemin

1. http://www.strato-analyse.org/fr/spip.php?article222

que dans un esprit déjà fécondé par quelques interrogations : le but des lignes qui suivent est de contribuer à cet effort de réflexion.

L'axe de ce livre, on l'aura compris, n'est pas dirigé vers les modes d'emploi de logiciels ou de matériels de sécurité, mais plutôt vers la position et l'explication des problèmes de sécurité, insérés dans un contexte technique dont il faut comprendre les tenants et les aboutissants si l'on veut adopter des solutions raisonnables. Et donner dans un livre des solutions techniques ou, pire, des recettes toutes faites, nous semblerait futile à une heure où le contexte technique évolue si vite que le Web et la presse spécialisée (qui se développe, y compris en langue française, cf. par exemple la revue MISC [109]) nous semblent bien mieux placés pour répondre à ce type d'attente. Il nous a paru plus judicieux de proposer au lecteur un tour d'horizon des problèmes afin qu'il puisse plus facilement, le moment venu, choisir entre plusieurs solutions techniques qui pourraient s'offrir à lui face à un problème concret.

Mode d'emploi du livre

Comment aborder la lecture de ce livre ? Il propose une progression des explications. Le chiffrement, point le plus difficile parce que assez technique mais à la base de tout le reste, fait d'abord l'objet d'une évocation informelle et succincte (chapitre 1), ensuite d'une présentation générale de la fonction de chiffrement, sans préjuger de ce qu'elle est (chapitre 2), puis d'une explication précise avec exposé mathématique (chapitre 4). Il semble difficile de faire autrement, car certains lecteurs ont le droit de ne pas lire les mathématiques du chapitre 4, mais ils ont aussi le droit de comprendre le reste quand même. Une explication complète, dès le début, risquerait de décourager le lecteur ; supprimer l'explication préalable du chapitre 2 saperait les développements qui suivent. Cette progression a un prix, des *flashbacks* : nous pensons qu'il vaut mieux revenir sur un sujet que d'égarer le lecteur par une attaque trop abrupte.

Conventions typographiques

Les textes encadrés ainsi sont destinés à des explications plus techniques que les autres passages, à des exemples pratiques ou à des apartés.

Les nombres entre crochets comme ceci [24] renvoient aux entrées de la bibliographie, en fin de volume.

Le livre comporte quatre parties, qui nous semblent correspondre aux quatre axes selon lesquels un responsable de sécurité doit déployer ses compétences et son activité :

- la première partie expose les principes généraux de sécurité, de façon aussi peu technique que possible ; vous devriez pouvoir la faire lire à votre directeur du système d'information ;
- la seconde partie, consacrée à la *science de la sécurité informatique*, présente les bases scientifiques sur lesquelles reposent les techniques pratiques ; elle est plus exigeante pour le lecteur en termes de difficulté conceptuelle ;
- la troisième partie aborde les aspects politiques, sociaux et psychologiques de la sécurité ; vous devriez pouvoir la placer sous les yeux de votre directeur juridique et de votre DRH ;
- la quatrième partie, qui envisage les évolutions récentes des menaces et de la sécurité, devrait intéresser quiconque navigue régulièrement sur l'Internet.

Remerciements

La liste de tous ceux à qui ce livre doit quelque chose est trop longue pour que nous prétendions la dresser sans oublier de noms.

Nous citerons Dominique Sabrier et Marie-Capucine Berthier, pour leurs relectures toujours précises et d'une exigence judicieuse. L'idée de ce livre naquit d'un enseignement de master organisé à l'université Paris 12 par Alexis Bès. Christian Queinnec (outre sa préface), Michel Gaudet, Bernard Perrot, Patrick Lerouge, Nat Makarévitch et Solveig ont relu, utilement commenté, conseillé et encouragé. Nos collègues de l'Inserm, de France Télécom et de l'université Paris-Dauphine, sans en avoir forcément eu conscience, ont aussi contribué tant par les échanges d'expériences et d'avis que par les situations concrètes soumises à notre examen. Muriel Shan Sei Fan fut une éditrice à l'exigence stimulante. Florence Henry et Sébastien Mengin ont mis à la composition la touche finale qui fait l'esthétique de l'ouvrage. Les activités et réunions organisées par l'Observatoire de la sécurité des systèmes d'information et des réseaux (OSSIR), par le Symposium sur la sécurité des technologies de l'information et de la communication (SSTIC) et par les Journées réseau de l'enseignement supérieur (JRES) ainsi que la conférence Hackito Ergo Sum furent des sources d'inspiration permanentes : parmi les intervenants, nous citerons notamment Éric Filiol, Nicolas Ruff, Hervé Schauer. Je remercie le

regretté François Bayen pour ses suggestions qui ont amélioré notablement les exposés cryptographiques du chapitre 4. La responsabilité des erreurs qui subsistent néanmoins dans ce texte ne peut être imputée qu'aux auteurs.

Ce livre a été écrit, composé et mis en page au moyen de logiciels libres, notamment GNU/Linux, GNU/Emacs, TEX, LATEX, BIBTEX et `xfig` : il convient d'en remercier ici les auteurs et contributeurs, dont le travail désintéressé élargit le champ de la liberté d'expression.

1

Premières notions de sécurité

Ce chapitre introduit les notions de base de la sécurité informatique : menace, risque, vulnérabilité ; il effectue un premier parcours de l'ensemble du domaine, de ses aspects humains, techniques et organisationnels, sans en donner de description technique.

Menaces, risques et vulnérabilités

La sécurité des systèmes d'information (SSI) est une discipline de première importance car le système d'information (SI) est pour toute entreprise un élément absolument vital : le lecteur de ce livre, *a priori*, devrait être déjà convaincu de cette évidence, mais il n'est peut-être pas inutile de lui procurer quelques arguments pour l'aider à en convaincre ses collègues et les dirigeants de son entreprise. Il pourra à cet effet consulter le livre de Michel Volle *e-conomie* [156], disponible en ligne, qui explique comment le SI d'une entreprise comme Air France, qui comporte notamment le système de réservation Amadeus, est un actif plus crucial que les avions. En effet, toutes les compagnies font voler des avions : mais la diffé-

rence entre celles qui survivent et celles qui disparaissent (rappelons l'hécatombe récente : Panam, TWA, Swissair, Sabena...) réside d'une part dans l'aptitude à optimiser l'emploi du temps des avions et des équipages, notamment par l'organisation de *hubs*, c'est-à-dire de plates-formes où convergent des vols qui amènent des passagers qui repartiront par d'autres vols de la compagnie, d'autre part dans l'aptitude à remplir les avions de passagers qui auront payé leur billet le plus cher possible, grâce à la technique du *yield management* qui consiste à calculer pour chaque candidat au voyage le prix à partir duquel il renoncerait à prendre l'avion et à lui faire payer juste un peu moins. Ce qui permet aux compagnies d'atteindre ces objectifs, et ainsi de l'emporter sur leurs rivales, c'est bien leur SI, qui devient dès lors un outil précieux, irremplaçable, en un mot vital. Il est probable que la valeur de la compagnie Air France réside plus dans le système de réservation Amadeus que dans ses avions, qui sont les mêmes pour toutes les compagnies, et souvent en location ou crédit-bail.

Vocabulaire : sécurité et sûreté

Le plus gros de la littérature relative à l'informatique est écrit en anglais, et les questions de traduction sont importantes pour qui veut avoir les idées claires. Pierre-Luc Réfalo a attiré mon attention sur un couple particulièrement pernicieux de faux-amis : l'anglais *security* désigne, dans notre domaine, tout ce qui a trait aux actes de malveillance, et doit être traduit par le français *sûreté*, cependant que l'anglais *safety* concerne ce qui a trait aux dommages accidentels, et doit être traduit en français par *sécurité*.

La même chose est déjà vraie depuis longtemps pour les banques, bien sûr, et les événements financiers de la fin de l'année 2008 ont bien montré que le SI, selon qu'il était utilisé à bon ou mauvais escient, pouvait avoir des effets puissants en bien ou en mal.

Puisque le SI est vital, tout ce qui le menace est potentiellement mortel : cela semble couler de source, et pourtant les auteurs de ce livre peuvent témoigner des difficultés qu'ils ont pu éprouver en essayant de convaincre leurs employeurs de consacrer quelques efforts à la sécurité de leur SI. Conjurer les menaces contre le SI est devenu impératif, et les lignes qui suivent sont une brève description de ce qu'il faut faire pour cela.

Les menaces contre le système d'information entrent dans l'une des catégories suivantes : atteinte à la disponibilité des systèmes et des données, destruction de données, corruption ou falsification de données, vol ou espionnage de données, usage illicite d'un système ou d'un réseau, usage d'un système compromis pour attaquer d'autres cibles.

Les menaces engendrent des risques et des coûts humains et financiers : perte de confidentialité de données sensibles, indisponibilité des infrastructures et des données, dommages pour le patrimoine intellectuel et la notoriété. Les risques peuvent se réaliser si les systèmes menacés présentent des vulnérabilités.

Il est possible de préciser la notion de risque en la décrivant comme le produit d'un préjudice par une probabilité d'occurrence :

$$\text{risque} = \text{préjudice} \times \text{probabilité d'occurrence}$$

Cette formule exprime qu'un événement dont la probabilité à survenir est assez élevée, par exemple la défaillance d'un disque dur, mais dont il est possible de prévenir le préjudice qu'il peut causer par des sauvegardes régulières, représente un risque acceptable ; il en va de même pour un événement à la gravité imparable, comme l'impact d'un météorite de grande taille, mais à la probabilité d'occurrence faible. Il va de soi que, dans le premier cas, le risque ne devient acceptable que si les mesures de prévention contre le préjudice sont effectives et efficaces : cela irait sans dire, si l'oubli de cette condition n'était très fréquent (cf. page 20).

Si la question de la sécurité des systèmes d'information a été radicalement bouleversée par l'évolution rapide de l'Internet, elle ne saurait s'y réduire ; il s'agit d'un vaste problème dont les aspects techniques ne sont qu'une partie. Les aspects juridiques, sociaux, ergonomiques, psychologiques et organisationnels sont aussi importants, sans oublier les aspects immobiliers, mais nous commencerons par les aspects techniques liés à l'informatique.

Aspects techniques de la sécurité informatique

Les problèmes techniques actuels de sécurité informatique peuvent, au moins provisoirement, être classés en deux grandes catégories :

- ceux qui concernent la sécurité de l'ordinateur proprement dit, serveur ou poste de travail, de son système d'exploitation et des données qu'il abrite ;
- ceux qui découlent directement ou indirectement de l'essor des réseaux, qui multiplie la quantité et la gravité des menaces.

Si les problèmes de la première catégorie citée ici existent depuis la naissance de l'informatique, il est clair que l'essor des réseaux, puis de l'Internet, en a démul-

tiplié l'impact potentiel en permettant leur combinaison avec ceux de la seconde catégorie.

La résorption des vulnérabilités repose sur un certain nombre de principes et de méthodes que nous allons énumérer dans la présente section avant de les décrire plus en détail.

Définir risques et objets à protéger

Fixer un périmètre de sécurité et élaborer une politique de sécurité

Inutile de se préoccuper de sécurité sans avoir défini ce qui était à protéger : en d'autres termes, toute organisation désireuse de protéger ses systèmes et ses réseaux doit déterminer son *périmètre de sécurité*. Le périmètre de sécurité, au sein de l'univers physique, délimite l'intérieur et l'extérieur, mais sa définition doit aussi englober (ou pas) les entités immatérielles qui peuplent les ordinateurs et les réseaux : essentiellement les logiciels et en particulier les systèmes d'exploitation.

Une fois ce périmètre fixé, il faut aussi élaborer une politique de sécurité, c'est-à-dire décider de ce qui est autorisé et de ce qui est interdit. À cette politique viennent en principe s'ajouter les lois et les règlements en vigueur, qui s'imposent à tous. Nous disons « en principe », parce que l'identification des lois en vigueur n'est rien moins qu'évidente : en vigueur où ? La législation française interdit la mise en ligne de certaines œuvres à qui n'en possède pas les droits, et réprime certains propos discriminatoires, mais d'autres pays ont des législations plus laxistes ; or qui peut m'empêcher d'installer un site xénophobe et de téléchargement illégal dans un tel pays, et d'y attirer les internautes français ?

Si avec l'aide du service juridique de votre entreprise vous avez réussi à surmonter ces difficultés et à mettre sur pied une politique de sécurité des systèmes d'information, il vous sera possible de mettre en place les solutions techniques appropriées à la défense du périmètre selon la politique choisie. Mais déjà, il est patent que les dispositifs techniques ne pourront pas résoudre tous les problèmes de sécurité. De surcroît, la notion même de périmètre de sécurité est aujourd'hui battue en brèche par des phénomènes comme la multiplication des ordinateurs portables et autres objets mobiles informatiques en réseau (iPhone 3G, BlackBerry et tablettes...) qui, par définition, se déplacent de l'intérieur à l'extérieur et inversement – à quoi s'ajoute encore l'extraterritorialité de fait des activités sur l'Internet.

Périmètres et frontières

La notion de périmètre de sécurité, ainsi que le signalait déjà l'alinéa précédent, devient de plus en plus fragile au fur et à mesure que les frontières entre l'extérieur et l'intérieur de l'entreprise ainsi qu'entre les pays deviennent plus floues et plus poreuses. Interviennent ici des considérations topographiques : les ordinateurs portables entrent et sortent des locaux et des réseaux internes pour aller se faire contaminer à l'extérieur ; mais aussi des considérations logiques : quelles sont les lois et les règles qui peuvent s'appliquer à un serveur hébergé aux États-Unis, qui appartient à une entreprise française et qui sert des clients brésiliens et canadiens ?

La justice et les fournisseurs français d'accès à l'Internet (FAI) en ont fait l'expérience : un certain nombre d'organisations ont déposé devant les tribunaux français des plaintes destinées à faire cesser la propagation de pages Web à contenus négationnistes, effectivement attaquables en droit français. Mais ces sites étaient installés aux États-Unis, pays dépourvu d'une législation anti-négationniste, ce qui empêchait tout recours contre les auteurs et les éditeurs des pages en question. Les plaignants se sont donc retournés contre les FAI français, par l'intermédiaire desquels les internautes pouvaient accéder aux pages délictueuses, mais sans succès. En effet, ainsi que nous le verrons à la page 282, le filtrage de contenus sur l'Internet est une entreprise coûteuse, aux résultats incertains, et en fin de compte vaine, car les éditeurs des pages en question disposent de nombreux moyens pour déjouer les mesures de prohibition.

Sur le filtrage de contenu, on peut lire le rapport Kahn-Brugidou [32] ; le site `www.legalis.net` [101] assure une veille juridique bien faite sur toutes les questions liées aux développements de l'informatique et de l'Internet ; les livres de Solveig Godeluck [76] et de Lawrence Lessig [102] replacent ces questions dans un contexte plus général.

Ressources publiques, ressources privées

Les systèmes et les réseaux comportent des données et des programmes que nous considérerons comme des *ressources*. Certaines ressources sont d'accès public, ainsi certains serveurs Web, d'autres sont privées pour une personne, comme une boîte à lettres électronique, d'autres enfin sont privées pour un groupe de personnes, comme l'annuaire téléphonique interne d'une entreprise. Ce caractère plus ou moins public d'une ressource doit être traduit dans le système sous forme de *droits d'accès*, comme nous le verrons à la page 44 où cette notion est présentée.

Identifier et authentifier

Les personnes qui accèdent à une ressource non publique doivent être *identifiées* ; leur identité doit être *authentifiée* ; leurs droits d'accès doivent être *vérifiés* au regard des *habilitations* qui leur ont été attribuées. À ces trois actions correspond un premier domaine des techniques de sécurité : les méthodes d'**authentification**, de signature, de vérification de l'**intégrité** des données et d'attribution de droits.

Concepts : habilitation

Une *habilitation* donnée à un utilisateur et consignée dans une base de données adéquate est une liste de droits d'accès et de pouvoirs formulés de telle sorte qu'un système informatique puisse les vérifier automatiquement.

La sécurité des accès par le réseau à une ressource protégée n'est pas suffisamment garantie par la seule identification de leurs auteurs. Sur un réseau local de type Ethernet ou Wi-Fi où la circulation des données fonctionne selon le modèle de l'émission radiophonique que tout le monde est censé pouvoir capter, il est possible à un tiers de détourner cette circulation. Si la transmission a lieu à travers l'Internet, les données circulent de façon analogue à une carte postale, c'est-à-dire qu'au moins le facteur et la concierge y ont accès. Dès lors que les données doivent être protégées, il faut faire appel aux techniques d'un autre domaine de la sécurité informatique : le **chiffrement**.

Authentification et chiffrement sont indissociables : chiffrer sans authentifier ne protège pas des usurpations d'identité (comme notamment l'attaque par interposition, dite en anglais attaque de type *man in the middle*, et décrite à la page 55), authentifier sans chiffrer laisse la porte ouverte au vol de données.

Empêcher les intrusions

Ces deux méthodes de sécurité ne suffisent pas, il faut en outre se prémunir contre les intrusions destinées à détruire ou corrompre les données, ou à en rendre l'accès impossible. Les techniques classiques contre ce risque sont l'usage de *pare-feu (firewalls)* et le *filtrage* des communications réseau, qui permettent de protéger la partie privée d'un réseau dont les stations pourront communiquer avec l'Internet sans en être « visibles » ; le terme *visible* est ici une métaphore qui exprime que nul système connecté à l'Internet ne peut accéder aux machines du réseau local

de sa propre initiative (seules ces dernières peuvent établir un dialogue) et que le filtre interdit certains types de dialogues ou de services, ou certains correspondants (reconnus dangereux).

La plupart des entreprises mettent en place des ordinateurs qu'elles souhaitent rendre accessibles aux visiteurs extérieurs, tels que leur serveur Web et leur relais de messagerie. Entre le réseau privé et l'Internet, ces machines publiques seront placées sur un segment du réseau ouvert aux accès en provenance de l'extérieur, mais relativement isolé du réseau intérieur, afin qu'un visiteur étranger à l'entreprise ne puisse pas accéder aux machines à usage strictement privé. Un tel segment de réseau est appelé *zone démilitarisée* (DMZ), en souvenir de la zone du même nom qui a été établie entre les belligérants à la fin de la guerre de Corée. Les machines en DMZ, exposées donc au feu de l'Internet, seront appelées *bastions*.

Certains auteurs considèrent que ces techniques de sécurité par remparts, ponts-levis et échauguettes sont dignes du Moyen Âge de l'informatique ; ils leur préfèrent les systèmes de détection d'intrusion (IDS), plus subtils, qui sont décrits à partir de la page 278. Cette innovation a suscité une surenchère, qui proclame que si l'on a détecté une intrusion, autant la stopper, et les IDS sont ainsi devenus des IPS (systèmes de prévention d'intrusion). Et l'on verra plus loin que les IPS sont critiqués par les tenants des mandataires applicatifs, plus subtils encore. Cela dit, dans un paysage informatique où les micro-ordinateurs et autres objets communiquants prolifèrent sans qu'il soit réaliste de prétendre vérifier la configuration de chacun, le filtrage et le pare-feu sont encore irremplaçables.

Pour couper court à toutes ces querelles autour des qualités respectives de telle ou telle méthode de sécurité, il suffit d'observer l'état actuel des menaces et des vulnérabilités. Il y a encore une dizaine d'années, le paramétrage de filtres judicieux sur le routeur de sortie du réseau d'une entreprise vers l'Internet pouvait être considéré comme une mesure de sécurité bien suffisante à toutes fins pratiques. Puis il a fallu déployer des antivirus sur les postes de travail. Aujourd'hui, les CERT (*Computer Emergency Response Teams*, voir page 20 pour une description de ces centres de diffusion d'informations de sécurité informatique) publient une dizaine de vulnérabilités nouvelles par semaine, et l'idée de pouvoir se prémunir en flux tendu contre toutes est utopique. La conception moderne (en cette année 2013) de la protection des systèmes et des réseaux s'appuie sur la notion de *défense en profondeur*, par opposition à la défense frontale rigide, où l'on mise tout sur l'efficacité absolue d'un dispositif unique.

Concevoir la défense en profondeur

La défense en profondeur – au sujet de laquelle on lira avec profit un article du Général Bailey [12] qui évoque à son propos une véritable « révolution dans les affaires militaires » – consiste à envisager que l'ennemi puisse franchir une ligne de défense sans pour cela qu'il devienne impossible de l'arrêter ; cette conception s'impose dès lors que les moyens de frappe à distance et de déplacement rapide, ainsi que le combat dans les trois dimensions, amènent à relativiser la notion de ligne de front et à concevoir l'affrontement armé sur un territoire étendu. Plus modestement, la multiplication des vulnérabilités, la généralisation des ordinateurs portables qui se déplacent hors du réseau de l'entreprise, la transformation des téléphones en ordinateurs complets, l'usage de logiciels novateurs (code mobile, *peer to peer*, sites interactifs, téléphonie et visioconférence sur IP) et d'autres innovations ont anéanti la notion de « périmètre de sécurité » de l'entreprise, et obligent le responsable SSI à considérer que la menace est partout et peut se manifester n'importe où. Il faut continuer à essayer d'empêcher les intrusions dans le SI de l'entreprise, mais le succès de la prévention ne peut plus être garanti, et il faut donc se préparer à limiter les conséquences d'une attaque réussie, qui se produira forcément un jour. Et ce d'autant plus que le SI contemporain n'est pas comme par le passé contenu par un « centre de données » monolithique hébergé dans un bunker, mais constitué de multiples éléments plus ou moins immatériels qui vivent sur des ordinateurs multiples, dispersés dans toute l'entreprise et au dehors ; et c'est cette nébuleuse qu'il faut protéger.

Nous allons au cours des chapitres suivants examiner un peu plus en détail certaines sciences et techniques qui s'offrent au responsable SSI, en commençant par la cryptographie dont sont dérivées les techniques de l'authentification.

Aspects organisationnels de la sécurité

À côté des mesures techniques destinées à assurer la protection des systèmes et des réseaux, la sécurité du SI comporte un volet humain et social au moins aussi important : la sécurité dépend en dernière analyse des comportements humains et, si ces derniers sont inadaptés, toutes les mesures techniques seront parfaitement vaines parce que contournées.

Abandonner les utilisateurs inexpérimentés aux requins ?

Un article de Marcus J. Ranum [123] (cf. page 272), qui n'est rien moins que l'inventeur du pare-feu et une autorité mondiale du domaine de la SSI, soutient l'idée paradoxale qu'il serait inutile, voire nuisible, d'éduquer les utilisateurs du SI à la sécurité : son argument est que les utilisateurs incapables de maîtriser suffisamment leur ordinateur, notamment en termes de mesures de sécurité, sont condamnés à être expulsés du marché du travail, et qu'il ne faut rien faire pour les sauver. Cette idée ne peut manquer de séduire les RSSI (responsables de sécurité des systèmes d'information) épuisés non pas tant par l'inconscience et l'ignorance de leurs utilisateurs, que par le fait que ceux-ci *ne veulent rien savoir*. Cela dit, après avoir jubilé quelques instants à l'idée de la disparition en masse de ses utilisateurs les plus insupportables, le RSSI se retrouve par la pensée dans la situation du narrateur d'un récit de Roland Topor [152], naufragé reçu comme un dieu vivant sur une île du Pacifique, et qui un jour, exaspéré par une rage de dents, crie à ses fidèles « Vous pouvez tous crever ! », suggestion à laquelle ils obéissent incontinent.

Si la suggestion de M. Ranum n'est pas à adopter à la légère, il convient néanmoins de considérer que les questions de SSI sont fort complexes et évoluent vite, si bien que même les utilisateurs avertis peuvent être pris de court par des menaces dont ils n'étaient pas informés. Nous pouvons même risquer une assertion plus générale : en informatique, *aucune compétence n'est pérenne ni complète*. Il convient donc que les RSSI et de façon plus générale tous les informaticiens responsables des infrastructures techniques et des réseaux consacrent une part de leur activité à informer, sensibiliser et former les utilisateurs à la problématique SSI. Eux-mêmes doivent se tenir en permanence au courant de l'évolution du sujet, être abonnés aux bulletins d'alerte des CERT et aux revues spécialisées, fréquenter les forums et les conférences, et mettre en application les enseignements qu'ils en auront tirés. Tout cela semblerait aller de soi, si l'on ne voyait combien peu de ces conseils sont entendus.

Idéalement, dans une entreprise, aucun utilisateur ne devrait être laissé « à l'abandon », c'est-à-dire avec un accès incontrôlé au réseau de l'entreprise et à ses communications avec l'Internet. Il devrait y avoir dans chaque groupe de travail un correspondant informatique en contact avec les responsables des infrastructures et du réseau. En l'absence d'une telle structure d'échanges ne manqueront pas d'être adoptés des comportements dangereux, bientôt suivis des incidents graves qui en sont la conséquence inéluctable.

La nature du « contact » entre le correspondant informatique et les responsables du SI et des infrastructures pourra dépendre du type d'organisation : dans une entreprise assez centralisée et hiérarchisée, la fonction de correspondant informatique sera définie en termes opérationnels, il aura des directives précises à appliquer et devra rendre compte de leur application ainsi que de tout problème informatique qui pourrait survenir. Dans une entreprise à la structure plus lâche, un organisme de recherche par exemple, la mise en place d'une telle organisation peut se révéler difficile, les relations de contact seront moins formelles, mais il sera néanmoins important qu'elles existent – ne serait-ce que par des conversations régulières au pied de la machine à café.

Externalisation radicale et accès Web

En septembre 2004 un article de *Computer Weekly* [135] a signalé une politique d'une nouveauté bouleversante pour faire face à la dissolution du périmètre de sécurité (on parle désormais de *dépérimétrisation*). *British Petroleum* (BP), la firme pétrolière bien connue, était obligée d'administrer 380 extranets pour communiquer avec 90 000 correspondants d'entreprises clientes, fournisseurs ou partenaires de par le monde, et ce au travers des infrastructures infiniment variées en nature et en qualité des opérateurs locaux. Elle a décidé qu'il serait beaucoup plus simple et efficace de leur offrir, par l'Internet, un accès analogue à celui que les banques offrent à leurs clients pour gérer leur compte.

La démarche ne s'est pas arrêtée là : BP s'est rendu compte que cette solution d'accès pourrait être étendue à une fraction de son propre personnel, estimée à 60 % de ses 96 200 employés, qui n'avaient pas besoin d'utiliser de systèmes client-serveur particuliers, un navigateur suffirait.

Les avantages d'une telle solution semblent considérables : l'entreprise n'a plus besoin de se soucier de la sécurité sur le poste de travail des correspondants ou des employés ainsi « externalisés », pas plus que la banque ne s'occupe de l'ordinateur de son client. C'est leur problème. Il y a bien sûr un revers de la médaille : l'entreprise, qui n'avait déjà qu'un contrôle relatif de la sécurité de ses postes de travail, n'en a plus du tout.

Une machine virtuelle pour chaque application

Une application moins radicale et sans doute plus satisfaisante de ce principe pourrait être la suivante : les utilisateurs légitimes du système d'information de l'entreprise font leur affaire de leur équipement en postes de travail, qu'ils configurent à leur guise, mais pour chaque application à laquelle ils doivent accéder, la Direction du système d'information leur remet une copie d'une machine virtuelle spécialement adaptée, dotée des certificats de sécurité, de la configuration réseau et des métadonnées adéquates.

Sauvegarder données et documents

La sauvegarde régulière des données et de la documentation qui permet de les utiliser est bien sûr un élément indispensable de la sécurité du système d'information, elle constitue un sujet d'étude à elle seule, qui justifierait un livre entier. Aussi ne ferons-nous, dans le cadre du présent ouvrage, que l'évoquer brièvement, sans aborder les aspects techniques. Mentionnons ici quelques règles de bon sens :

- pour chaque ensemble de données, il convient de déterminer la périodicité des opérations de sauvegarde en fonction des nécessités liées au fonctionnement de l'entreprise ;
- les supports de sauvegarde doivent être stockés de façon à être disponibles après un sinistre tel qu'incendie ou inondation : armoires ignifugées étanches ou site externe ;
- les techniques modernes de stockage des données, telles que *Storage Area Network* (SAN) ou *Network Attached Storage* (NAS), conjuguées à la disponibilité de réseaux à haut débit, permettent la duplication de données à distance de plusieurs kilomètres (voire plus si l'obstacle financier n'est pas à considérer), et ce éventuellement en temps réel ou à intervalles très rapprochés ; ce type de solution est idéal pour un site de secours ;
- de l'alinéa précédent, on déduit que, dans un système d'information moderne, toutes les données doivent être stockées sur des SAN ou des NAS, rien ne justifie l'usage des disques attachés directement aux serveurs, qui seront réservés aux systèmes d'exploitation et aux données de petit volume ;
- les dispositifs et les procédures de sauvegarde et, surtout, de restauration et de reprise doivent être vérifiés régulièrement (cf. la section suivante).

Vérifier les dispositifs de sécurité

Le dispositif de sécurité le mieux conçu ne remplit son rôle que s'il est opérationnel, et surtout si ceux qui doivent le mettre en œuvre, en cas de sinistre par exemple, sont eux aussi opérationnels. Il convient donc de vérifier régulièrement les capacités des dispositifs matériels et organisationnels.

Les incidents graves de sécurité ne surviennent heureusement pas tous les jours : de ce fait, si l'on attend qu'un tel événement survienne pour tester les procédures palliatives, elles risquent fort de se révéler défaillantes. Elles devront donc être exécutées « à blanc » périodiquement, par exemple en effectuant la restauration d'un ensemble de données à partir des sauvegardes tous les six mois, ou le redémarrage d'une application à partir du site de sauvegarde.

Outre ces vérifications régulières, l'organisation d'exercices qui simulent un événement de sécurité impromptu peut être très profitable. De tels exercices, inspirés des manœuvres militaires, révéleront des failles organisationnelles telles que rupture de la chaîne de commandement ou du circuit d'information. Un rythme bisannuel semble raisonnable pour ces opérations.

La nécessaire veille auprès des CERT

Les CERT *(Computer Emergency Response Teams)* centralisent, vérifient et publient les alertes relatives à la sécurité des ordinateurs, et notamment les annonces de vulnérabilités récemment découvertes. Les alertes peuvent émaner des auteurs du logiciel, ou d'utilisateurs qui ont détecté le problème. Détecter une vulnérabilité ne veut pas dire qu'elle soit exploitée, ni même exploitable, mais le risque existe.

Organisation des CERT

Les vulnérabilités publiées par les CERT sont relatives à toutes sortes de systèmes ; leur publication constitue une incitation forte pour que les industriels concernés (les producteurs du système ou du logiciel le plus souvent) les corrigent. Certains tentent aussi de ralentir le travail des CERT, dont ils aimeraient bien qu'ils ne dévoilent pas leurs faiblesses.

Le premier CERT a vu le jour à l'université Carnegie Mellon de Pittsburgh (Pennsylvanie) en novembre 1988, sur une initiative de la DARPA *(Defense Advanced Re-*

search Projects Agency) consécutive à la propagation du ver de Morris, la première attaque, involontaire [1] mais de grande envergure, contre l'Internet. En 2013, la France dispose de trois CERT : le CERTA [2] pour les besoins des administrations et services publics, le CERT Renater [3] qui s'adresse aux universités et centres de recherche, et le CERT-IST [4] qui s'adresse au monde industriel. En fait, la coopération au sein de la communauté mondiale des CERT est assez étroite, surtout en période de crise. Cette communauté est concrétisée par l'existence d'un Centre de coordination des CERT [5], hébergé par l'université Carnegie Mellon.

Pour ce qui concerne la France, il convient de signaler le rôle de l'Agence nationale de la sécurité des systèmes d'information (ANSSI) ; cet organisme placé auprès du Premier ministre, dirigé par Patrick Pailloux et rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDSN), est chargé d'élaborer la politique nationale de sécurité des systèmes d'information et de coordonner sa mise en œuvre. L'ANSSI supervise le CERTA [6].

La publication des avis des CERT est une contribution majeure et vitale à la sécurité des systèmes d'information. Leur volume est tel que le dépouillement, qui ne peut être confié qu'à des ingénieurs réseau de haut niveau, représente un travail considérable.

Faut-il publier les failles de sécurité ?

Un débat s'est engagé sur le bien-fondé de certains avis, et sur la relation qu'il pourrait y avoir entre le nombre d'avis concernant un logiciel ou un système donné et sa qualité intrinsèque. Les détracteurs des logiciels libres ont mis en exergue le volume très important d'avis des CERT qui concernaient ces logiciels (par exemple Linux, le serveur Web Apache, Sendmail, etc.) pour en inférer leur fragilité. Leurs défenseurs ont riposté en expliquant que les avis des CERT concernaient par définition des failles de sécurité découvertes et donc virtuellement corrigées, alors que l'absence d'avis relatifs à tel ou tel système commercial pouvait simplement signifier que l'on passait sous silence ses défauts de sécurité en profitant de son opacité. Or l'expérience montre que tout dispositif de sécurité a des failles ; les attaquants

1. Du moins à en croire son auteur Robert Tappan Morris.
2. http://www.certa.ssi.gouv.fr/
3. http://www.renater.fr/spip.php?rubrique=19
4. http://www.cert-ist.com/
5. http://www.cert.org/
6. http://www.ssi.gouv.fr/index.html

ne perdent pas leur temps à faire de la recherche fondamentale sur la factorisation des grands nombres entiers, ils essaient de repérer les failles d'implémentation et ils les exploitent.

Faille de conception ou d'implémentation ?

Pour attaquer un système logiciel dont on veut prendre le contrôle, il est possible de rechercher d'éventuelles erreurs de conception dans les méthodes employées par ses auteurs : algorithme inapproprié ou faux, mauvais choix de représentation des données, formule de calcul fausse... Par exemple, beaucoup d'algorithmes de chiffrement (notamment RSA, cf p. 89) reposent sur le fait qu'il n'existe pas d'algorithme praticable pour décomposer en facteurs premiers de grands nombres entiers, de plus de 1 000 chiffres binaires. Si demain les progrès de l'informatique quantique mettent à la disposition des pirates l'algorithme de Shor [7], toutes ces méthodes de chiffrement s'effondrent.

Plutôt que d'ouvrir un laboratoire de recherche en algorithmique quantique (et un autre pour réaliser un calculateur quantique opérationnel), il vaut mieux espérer que les programmeurs soient paresseux et insouciants, et qu'il y ait des erreurs de programmation dans leurs logiciels, par exemple un débordement de zone mémoire (cf. p. 100), de nature à faciliter l'attaque, ainsi que nous le verrons dans les prochains chapitres : c'est ce que l'on nomme une *faille d'implémentation*. Cet espoir est souvent exaucé.

Failles « zero-day »

Dans les publications relatives à la sécurité informatique, il est une notion qui apparaît de façon récurrente, la *faille zero-day*. Il s'agit d'une faille de sécurité inconnue ou non corrigée. Dès lors, un attaquant qui la découvre ou qui l'achète (il existe un lucratif marché des *zero-day*) peut l'exploiter avec grand profit. En effet, une faille connue, c'est-à-dire dont la description a été dûment publiée par un CERT, après concertation avec l'éditeur du logiciel concerné qui aura publié une correction ou un contournement, sera corrigée sur beaucoup de systèmes, tandis qu'une faille *zero-day*, non corrigée par définition, est exploitable *a priori* sur tous les systèmes, ce qui procure à l'attaquant un avantage considérable.

Le ver Stuxnet (cf. chapitre 13 p. 317) a suscité l'étonnement, voire l'admiration de la communauté de la sécurité informatique lors de sa découverte, entre autres par le fait qu'il exploitait quatre *zero-day*, luxe inouï : en effet, le *zero-day* est une ressource rare, et en griller quatre d'un coup est une dépense somptuaire.

Face au risque induit par les failles des logiciels, la meilleure protection est une capacité de riposte rapide, qui consiste le plus souvent à commencer par désactiver le composant pris en défaut en attendant la correction. La communauté du logiciel libre excelle dans cet exercice, mais avec les logiciels commerciaux les utilisateurs n'ont souvent aucun moyen d'agir : ils ne peuvent qu'attendre le bon vouloir de leur fournisseur. Dans ce contexte, la publication d'avis des CERT relatifs à des logiciels commerciaux est très bénéfique parce qu'elle incite les fournisseurs à corriger plus rapidement un défaut dont la notoriété risque de nuire à leur réputation. Mais

7. http://fr.wikipedia.org/wiki/Algorithme_de_Shor

certains fournisseurs cherchent à obtenir le silence des CERT en arguant le fait que leurs avis risquent de donner aux pirates des indications précieuses... ce qui est fallacieux car les sites Web des pirates sont de toute façon très bien informés et mis à jour, eux, selon les principes du logiciel libre, ce qui indique bien où est l'efficacité maximale. L'expérience tend à prouver qu'une faille de sécurité est d'autant plus vite comblée qu'elle est publiée tôt et largement. L'accès au code source du logiciel en défaut constitue bien sûr un atout.

La réponse à la question posée par le titre de cette section est donc : *oui, il faut publier les failles de sécurité, mais de façon organisée et responsable,* c'est-à-dire de façon certifiée, sur le site d'un organisme accrédité, typiquement un CERT, et après avoir prévenu l'auteur ou l'éditeur du logiciel en défaut et lui avoir laissé un délai raisonnable pour au moins trouver un palliatif d'urgence. Il faut savoir qu'il existe aujourd'hui un marché de la faille, qui parfois n'est pas loin de s'apparenter à du chantage.

Le management de la sécurité

Qui sont les spécialistes ?

Cette section doit beaucoup à la formation *ISO 27001 Lead Auditor*, dispensée par Alexandre Fernandez-Toro et Hervé Schauer, de Hervé Schauer Consultants. Qu'ils soient ici remerciés pour avoir su rendre captivante une matière plutôt aride. Les erreurs et imprécisions ne peuvent être imputées qu'à l'auteur.

Nous recommandons la lecture du livre qu'Alexandre Fernandez-Toro a consacré au sujet, *Management de la sécurité du système d'information : Implémentation ISO 27001* [65].

La présente section sur le management de la sécurité présente des normes et des méthodes qui nous inspirent de sérieuses réserves. Néanmoins il convient qu'elles aient leur place dans ce livre, d'abord parce que sans elles cet exposé serait incomplet, ensuite parce que tout responsable de la sécurité a intérêt à les connaître s'il veut conserver son emploi. Nous ne saurions trop recommander au responsable sécurité soucieux de son avenir professionnel de suivre une formation du type de celle qui est mentionnée en exergue de cette section. Il devra presque certainement en mettre les enseignements en pratique, en tout cas s'il travaille dans une grande entreprise acquise aux idées managériales.

Culture : « Management », un faux anglicisme

Pour se résigner à l'emploi du mot management, on se rappellera que, loin d'être un anglicisme, il s'agit d'un vieux mot français remis à l'honneur : Olivier de Serres (1539-1619) emploie en effet le terme *ménager* dans une acception qui en fait le *manager* contemporain (on nous fera grâce de la variation orthographique, courante à l'époque). Et l'emploi du mot *gestion* à toutes les sauces serait bien pire.

Les systèmes de management

L'Organisation internationale de normalisation, ou *International organization for standardization* en anglais (ISO pour la forme abrégée) est une organisation internationale, créée en 1947, composée de représentants des organismes de normalisation nationaux d'environ 150 pays, qui produit des normes internationales dans des domaines industriels et commerciaux.

L'ISO a entrepris d'encadrer par des normes les *systèmes de management*, et pour ce faire a commencé par en donner une définition, qui fait l'objet de la norme IS (pour *International Standard*) 9000 ; un système de management est un système qui permet :

- d'établir une politique ;
- de fixer des objectifs ;
- de vérifier que l'on a atteint les objectifs fixés.

Plus concrètement, un système de management comporte un ensemble de mesures organisationnelles et techniques destinées à mettre en place un certain contexte organisationnel et à en assurer la pérennité et l'amélioration. L'idée cruciale au cœur de cette problématique est que le système de management repose sur un référentiel écrit, et qu'il est donc *vérifiable*, au moyen d'un *audit* qui consistera à comparer le référentiel à la réalité pour relever les divergences, nommées *écarts* ou *non-conformités*. L'essor de la demande d'audits a déclenché la prolifération des référentiels : sans référentiel, l'auditeur aurait beaucoup de mal à accomplir sa mission, et son rapport ne serait étayé que par sa réputation personnelle d'expert.

Il existe actuellement (en 2013) sept normes relatives aux systèmes de management :

- la norme IS 9001 consacrée aux systèmes de management de la qualité et aux exigences associées ;

- la norme IS 14001 consacrée aux systèmes de management de l'environnement ;
- la norme IS 20000 consacrée aux services informatiques ;
- la norme ID 22000 consacrée au management de la sécurité des aliments ;
- la norme ID 31000 consacrée au management du risque ;
- la norme ID 50001 consacrée au management de l'énergie ;
- la norme IS 27001 consacrée aux systèmes de management de la sécurité de l'information ; c'est cette dernière qui nous intéressera plus particulièrement ici.

Pour couronner cet édifice remarquable, la norme IS 19001 formule les directives à respecter pour la conduite de l'audit d'un système de management.

Le système de management de la sécurité de l'information

La norme IS 27001 [90] est destinée à s'appliquer à un système de management de la sécurité de l'information (SMSI) ; elle comporte notamment un schéma de certification susceptible d'être appliqué au SMSI au moyen d'un audit.

Comme toutes les normes relatives aux systèmes de management, IS 27001 repose sur une approche par *processus*, et plus précisément sur le modèle de processus formulé par W.E. Deming, du MIT, et nommé *roue de Deming*, ou PDCA, comme *Plan, Do, Check, Act* :

- phase *Plan* : définir le champ du SMSI, identifier et évaluer les risques, produire le document (*Statement of Applicability,* SOA) qui énumère les *mesures de sécurité* à appliquer ;
- phase *Do* : affecter les ressources nécessaires, rédiger la documentation, former le personnel, appliquer les mesures décidées, identifier les risques résiduels ;
- phase *Check* : audit et revue périodiques du SMSI, qui produisent des *constats* et permettent d'imaginer des corrections et des améliorations ;
- phase *Act* : prendre les mesures qui permettent de réaliser les corrections et les améliorations dont l'opportunité a été mise en lumière par la phase *Check*, préparer une nouvelle itération de la phase *Plan*.

Le SMSI a pour but de maintenir et d'améliorer la position de l'organisme qui le met en œuvre du point de vue, selon les cas, de la compétitivité, de la profitabilité, de la conformité aux lois et aux règlements, et de l'image de marque. Pour cela

il doit contribuer à protéger les actifs *(assets)* de l'organisme, définis au sens large comme tout ce qui compte pour lui.

Pour déterminer les mesures de sécurité dont la phase *Plan* devra fournir une énumération, la norme IS 27001 s'appuie sur le catalogue de mesures et de bonnes pratiques proposé par la norme IS 27002 (ex-17799), « *International Security Standard* » [91], plus volumineuse et au contenu plus technique.

Afin de mieux en parler, le SMSI est accompagné d'une norme qui en définit le vocabulaire : IS 27000.

IS 27001 impose une analyse des risques, mais ne propose aucune méthode pour la réaliser : l'auteur du SMSI est libre de choisir la méthode qui lui convient, à condition qu'elle soit documentée et qu'elle garantisse que les évaluations réalisées avec son aide produisent des résultats comparables et reproductibles. Un risque peut être accepté, transféré à un tiers (assurance, prestataire), ou réduit à un niveau accepté. Le corpus ISO propose néanmoins sa méthode d'analyse : IS 27005.

Un autre exemple de méthode d'analyse de risque utilisable dans le cadre d'IS 27001 est la méthode EBIOS® (Expression des Besoins et Identification des Objectifs de Sécurité) [8], qui « permet d'apprécier et de traiter les risques relatifs à la sécurité des systèmes d'information (SSI). Elle permet aussi de communiquer à leur sujet au sein de l'organisme et vis-à-vis de ses partenaires afin de contribuer au processus de gestion des risques SSI. »

Tout RSSI (Responsable de la sécurité des Systèmes d'information) amené à effectuer une analyse de risque dans le cadre du déploiement d'un SMSI peut s'appuyer sur EBIOS, de l'avis des praticiens c'est la méthode la plus conforme aux exigences pratiques.

Élaboration et mise en place du SMSI

La norme IS 27001 précise la démarche qui doit être suivie pour élaborer et mettre en place le SMSI : sans entrer trop dans les détails, ce qui risquerait d'enfreindre les droits des organismes de normalisation qui vendent fort cher les textes des normes, disons que l'organisme désireux de se voir certifier devra :

- définir le champ du SMSI ;
- en formuler la politique de management ;

8. http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html

- préciser la méthode d'analyse de risques utilisée ;
- identifier, analyser et évaluer les risques ;
- déterminer les traitements qui seront appliqués aux différents risques, ainsi que les moyens d'en vérifier les effets ;
- attester l'engagement de la direction de l'organisme dans la démarche du SMSI ;
- rédiger le *Statement of Applicability* (SOA) qui sera la charte du SMSI et qui permettra de le soumettre à un audit.

Suivi et application du SMSI

Ici, la norme précise que, une fois que le SMSI a été formulé, il faut faire ce qu'il stipule, vérifier que c'est fait, identifier les erreurs dans son application, les failles qui s'y manifestent et les modifications du contexte nécessitant sa mise à jour ou sa modification.

Pour ces tâches elles-mêmes, l'ISO a produit des documents normatifs : IS 27003 pour l'implémentation, IS 27004 définit des indicateurs de qualité pour le SMSI, IS 27006 encadre le processus de certification du SMSI, IS 27007 le processus d'audit.

Récapitulation des normes ISO pour la SSI

IS 27001 : système de management de la sécurité des systèmes d'information (SMSI) ;
IS 27000 : vocabulaire SSI ;
IS 27002 (ex-17799) : catalogue de mesures de sécurité ;
IS 27003 : implémentation du SMSI ;
IS 27004 : indicateurs de suivi du SMSI ;
IS 27005 : évaluation et traitement du risque ;
IS 27006 : certification du SMSI ;
IS 27007 : audit du SMSI.

On pourra consulter des analyses de ces normes et de leurs conditions d'application sur le site de la société Hervé Schauer Consultants [9]. Nous recommandons aussi la lecture du livre qu'Alexandre Fernandez-Toro a consacré au sujet, *Management de la sécurité du système d'information : Implémentation ISO 27001* [65].

9. http://www.hsc.fr/ressources/articles/hakin9_edito_ISO27001/index.html.fr

Tâches de direction et d'encadrement

À la direction de l'organisme, dont il a déjà été dit qu'elle devait s'engager activement dans la démarche, incombent d'autres obligations : vérifier que tout est bien fait selon les règles, affecter à la démarche du SMSI des ressources suffisantes en personnel et en moyens matériels, déterminer les besoins qui en résultent en termes de compétence et de formation, fournir les efforts qui conviennent en termes de sensibilisation et de formation, effectuer le contrôle des effets de ces efforts. Il faut aussi organiser des revues et des exercices, etc., tout cela afin d'assurer l'*amélioration continue* du SMSI. Cette vision idyllique d'un univers en marche vers le Bien, le Beau, le Juste ne saurait manquer de soulever l'enthousiasme du lecteur !

Un modèle de maturité ?

La norme ISO/IEC 21827 [87] propose un « Modèle de maturité de capacité » : qui peut traduire ce jargon invraisemblable ?

Critères communs

Les *Critères Communs* (norme ISO/IEC 15408) sont étrangers ou plutôt parallèles à la démarche IS 27001 ; ils se proposent de servir de base pour l'évaluation des propriétés de sécurité des produits et des systèmes de traitement de l'information. Nous n'en dirons guère plus ici, parce que cette norme s'adresse aux concepteurs de produits de sécurité plutôt qu'à ceux qui les utilisent pour construire des systèmes d'information sûrs.

Faut-il adhérer aux normes de sécurité de l'information ?

L'auteur de ces lignes n'est pas convaincu que les normes évoquées à la section précédente soient un remède à l'insécurité ; ces méthodes sont d'une grande lourdeur, leur seul apprentissage peut absorber une énergie considérable. Or, on aura beau connaître par cœur les critères communs et savoir appliquer EBIOS à la perfection, on n'aura pas mis en place une seule mesure concrète de SSI, on sera en tout et pour tout capable, en principe, d'évaluer les mesures que d'autres auront éventuellement mises en place.

Pour reprendre des termes entendus dans une conférence professionnelle consacrée à IS 27001, il n'y a que trois raisons possibles de se plier à un tel exercice :

- l'environnement de l'entreprise fait de la certification IS 27001 une obligation légale ;
- l'entreprise noue des relations contractuelles avec un partenaire qui exige la certification IS 27001 ;
- l'entreprise recherche, par la certification IS 27001, une élévation morale supérieure.

Il est possible d'en ajouter une quatrième : certaines législations, comme Sarbanes-Oxley aux États-Unis ou Bâle 2 en Europe (cf. page 32), exigent que les entreprises de leur champ d'application se plient à une certification selon une norme de Système de management, en laissant à l'impétrant le choix de la norme : or, IS 27001 est la moins lourde de ces normes.

Tout RSSI (Responsable de la sécurité des Systèmes d'information) doit avoir conscience du fait qu'en 2013 il a de fortes chances de travailler pour un employeur soumis à au moins une de ces quatre obligations.

À la lecture de ces normes, il est frappant de voir que la vérification formelle de conformité à leur texte peut être effectuée par un auditeur dépourvu de compétence technique : il suffit de lire les documents obligatoires et de vérifier que les mesures mentionnées ont bien été appliquées, ce qui doit être écrit dans un autre document. On pourrait presque imaginer un audit par ordinateur : il serait sans doute mauvais, mais formellement conforme. Reste à écrire le compilateur de normes et le compilateur de SOA. Évidemment, pour réaliser un *bon* audit, l'intuition de l'auditeur, nourrie par son expérience, jouera un rôle important. Certains collègues, dont nous tairons les noms de crainte de leur attirer des ennuis, vont jusqu'à dire que l'adoption d'une démarche telle que celle proposée par IS 27001 ou IS 21827 est nuisible : elle empêcherait les gens de penser correctement, de se poser les bonnes questions. S'il osait, l'auteur de ces lignes serait d'accord avec eux, mais il est trop respectueux des normes et des autorités pour cela. Les auteurs de ces normes semblent croire que l'univers peut être décrit de façon adéquate par un tableau de cases à cocher, analogue à un questionnaire à choix multiples : on se demande pourquoi de grands nigauds nommés Aristote, Descartes, Newton, Kant et Einstein n'y ont pas pensé.

Une autre faiblesse de ces démarches, c'est leur déterminisme : la lecture de leurs documentations suggère que l'univers des risques et des menaces qu'elles sont censées conjurer est parfaitement ordonné et prévisible, alors que justement ses caractéristiques premières sont le chaos et la surprise. De ce fait, le temps passé à cocher

consciencieusement les cases du tableau Excel où l'on aura reporté les rubriques de son SOA risque d'avoir été perdu, et il aurait sans doute été plus judicieux de le consacrer à de la sécurité réelle. Soulignons à cette occasion les ravages exercés par un logiciel par ailleurs bien pratique, Excel : pour certains managers, le monde semble pouvoir être décrit par un tableau de cases ; dès qu'un problème a plus de deux dimensions, c'est la panique parce que cela n'entre plus dans le tableur.

Une telle vision, malgré sa pauvreté, comporte une métaphysique implicite, dont Isabelle Boydens [29] donne un énoncé explicite (p. 62) :

> « Une telle approche repose implicitement sur trois postulats :
>
> - le monde est composé d'éléments discrets, univoques, clairement identifiables et perceptibles ;
> - les combinaisons et la connaissance de ces éléments sont gouvernées par des lois ;
> - il est possible d'établir une relation bi-univoque entre le réel observable et sa représentation informatique en vertu de l'isomorphisme qui les relierait l'un à l'autre. »

Bien sûr, le monde n'est pas ainsi. Cela dit, il ne convient pas d'ignorer que, dans les grandes structures bureaucratisées, ce type de démarche est devenu à peu près inévitable, un peu comme ISO 9001. Les procédures destinées à évaluer des travaux techniques deviennent une charge de travail plus lourde que l'objet de l'évaluation, les procédures de gestion demandent plus de travail que les activités qu'elles servent à gérer, bref ce qui devrait être une aide pour l'action devient un fardeau, de surcroît ennuyeux. Pour résumer cette analyse en une formule : toutes ces normes et ces procédures n'ont qu'une finalité, permettre à des incompétents de diriger.

Un autre défaut de ces procédures d'évaluation est qu'elles ne sont pas uniquement construites en fonction des buts à atteindre, mais aussi, sinon surtout, en fonction de ce qui, dans les processus étudiés, se prête bien à l'évaluation, parce que par exemple il est facile d'y adapter une métrique. Conformément au proverbe, pour celui qui ne dispose que d'un marteau, tout ressemble à un clou, et les normalisateurs de la sécurité n'ont pas toujours échappé à ce travers.

Le RSSI qui aura pu échapper à la lourdeur de ces carcans normalisés aura à cœur d'élaborer une politique et des règles de sécurité raisonnables, sobres, les plus

simples possible, et adaptées à la situation locale. Le présent ouvrage se veut un guide pour rédiger une politique de sécurité [10].

De toutes les façons, il faut savoir que des règles de sécurité complexes ou trop contraignantes seront simplement inappliquées, parce que trop difficiles à comprendre. La simple lecture des critères communs et des manuels EBIOS représente des milliers de pages : autant dire que leur étude détaillée laissera peu de temps pour se consacrer à l'élaboration d'une politique réelle de sécurité. En fait, seuls des cabinets de consultants spécialisés peuvent maîtriser de tels outils, parce qu'ils les mettent en œuvre à longueur d'année.

Un projet de certification de sécurité Open Source : OSSTMM

L'*Institute for Security and Open Methodologies* (ISECOM) [11] est un organisme de recherche en sécurité fondé en 2001, qui se proclame « ouvert ». Cet institut a élaboré un référentiel de mesures de sécurité et d'audit, *Open Source Security Testing Methodology Manual* (OSSTMM) [12]. Ce manuel, disponible librement en ligne, propose donc une méthodologie de vérification de la sûreté des systèmes.

La fonction d'un référentiel est de pouvoir faire des audits. Si l'on a construit son système en suivant des règles écrites dans un référentiel, l'auditeur pourra vérifier la conformité du système au référentiel, ce qui est l'essentiel du métier d'audit. Encore faut-il que le référentiel soit pertinent.

Le manuel OSSTMM peut éventuellement être utilisé comme catalogue de vérifications à faire et de mesures à prendre, comme il en existe beaucoup. Mais, comme tout catalogue, il risque de se substituer à la compréhension substantielle de la situation de sécurité à étudier et à résoudre. En outre, il ne sera pas d'un emploi très commode pour un auditeur, parce qu'il mêle deux genres : le référentiel de règles et de contrôles, et le manuel explicatif. Il y a certes des listes de choses à vérifier, mais formulées dans des termes assez étroitement techniques, ce qui risque de les périmer assez rapidement. L'auteur de ces lignes n'a pas été convaincu par l'ensemble.

Par ailleurs, l'utilité première d'un processus de certification est de procurer au certifié une garantie institutionnelle dont il puisse se prévaloir vis-à-vis de ses par-

10. Le lecteur pourra aussi se reporter avec profit au livre bénéfiquement concis de Scott Barman, *Writing Information Security Policies* [13].
11. http://www.isecom.org/
12. http://www.isecom.org/osstmm/

tenaires, des autorités légales et de son conseil d'administration. C'est la principale qualité, par exemple, du processus de certification IS 27001, qui, au moins en France, est encadré assez rigoureusement. De ce point de vue, le processus OSSTMM, où les auditeurs sont autocertifiés et la communauté d'origine autoproclamée, semble assez faible.

Législation financière et système d'information

Les questions techniques et organisationnelles ne sont pas les seules à avoir des effets sur la sécurité du système d'information. Après le management de la sécurité et ses excès, nous aborderons ici l'application de la sécurité au management, qui engendre elle aussi des pratiques abusives.

L'ubiquité de l'informatique est telle que des mesures législatives destinées à réglementer des domaines que l'on pourrait croire très éloignés de l'objet du présent ouvrage finissent par se trouver au cœur de sa problématique. Un de nos collègues distinguait la « sécurité dure » (crypto-processeurs, pare-feu, réseaux privés virtuels, séparation des privilèges) de la « sécurité molle », qui par analogie avec les sciences affublées du même adjectif se préoccupe des aspects simplement humains : il sera ici question de certains d'entre eux. L'administrateur de système et de réseau pourrait se croire à l'abri des monstres bureaucratiques mentionnés ci-dessous : qu'il s'estime heureux si on ne lui impose pas les procédures éléphantesques qu'ils engendrent.

Prolifération des systèmes de contrôle et d'audit

Depuis les scandales financiers de la période 2001-2002 (nous ne mentionnerons ici que les affaires Enron et Worldcom), sont apparues comme champignons après la pluie des réglementations destinées à améliorer le contrôle des autorités et des actionnaires sur la gestion des entreprises. Le signal a été donné par les États-Unis en juillet 2002 avec la loi Sarbanes-Oxley (plus familièrement SOX), qui impose aux entreprises qui font appel au capital public (c'est-à-dire cotées en bourse) toute une série de règles comptables et administratives destinées à assurer la traçabilité de leurs opérations financières. Ainsi les actionnaires ne courent plus le risque de voir leurs actions partir en fumée après une déconfiture que des comptes truqués n'auraient pas permis de prévoir, cependant que les dirigeants initiés auraient re-

vendu à temps leurs stock-options pour se retirer sur leur yacht aux îles Caïmans... La France a bien sûr emboîté le pas avec la loi du 1er août 2003 sur la sécurité financière (LSF) qui concerne principalement trois domaines : la modernisation des autorités de contrôle des marchés financiers, la sécurité des épargnants et des assurés, et enfin le contrôle légal des comptes ainsi que la transparence et le gouvernement d'entreprise. Cette loi française ne concerne pas seulement les sociétés cotées, mais toutes les sociétés anonymes ; elle est complétée par le dispositif réglementaire européen « Bâle 2 » de 2004, qui concerne les établissements financiers.

La conséquence pratique la plus visible des législations de type SOX est la prolifération des systèmes de contrôle et d'audit que nous avons évoqués à la page 23, et c'est bien pourquoi le responsable de sécurité ne peut les ignorer.

La loi Sarbanes-Oxley concerne la sécurité du système d'information en ceci qu'elle impose aux entreprises des procédures de contrôle interne, de conservation des informations, et de garantie de leur exactitude. La description détaillée de ces procédures, et de leur réalisation dans le système d'information, est un élément clé de la loi, notamment pour ce qui a trait aux points suivants :

1. la continuité des opérations ;
2. la sauvegarde et l'archivage des données ;
3. l'externalisation et son contrôle.

Les législations européennes ont emprunté les mêmes chemins.

Sauvés par la régulation ?

Le lecteur de 2013 sait évidemment que tous ces dispositifs juridiques et réglementaires n'ont en rien empêché les scandales bien plus graves de la crise des *subprimes* en 2008-2009 : cette simple constatation devrait suffire à les considérer avec suspicion. Dans le numéro d'automne 2010 de *Commentaire*, un article d'Augustin Landier et David Thesmar intitulé « Action publique et intelligence collective » [98] explique dans sa section intitulée « Capture du régulateur et anesthésie du politique » (p. 714) que le remède à de telles crises n'est pas à chercher dans la multiplication et le durcissement des règles et des organes de régulation : ces organes étaient déjà nombreux et puissants, simplement ils avaient été captés par le monde de la finance, non pas le plus souvent par corruption, mais par séduction, conviction, influence. Le salut, s'il en est, serait plutôt à chercher dans l'amélioration de la réactivité et de la qualité de la régulation. « Pour répondre à ce besoin, nous proposons donc une action publique en architecture ouverte, à la manière des logiciels

libres. Ce nouveau mode d'action publique soumet l'État à une double exigence : informer et écouter. » (p. 716).

Brève critique de la sécurité financière

On peut lire sur le site de VLSI Research un article [86] dans lequel son président G. Dan Hutcheson fait une analyse très pessimiste des perspectives de l'économie américaine postérieures à l'affaire Enron et à la floraison de ces législations.

Hutcheson retient les points suivants :

1. la quasi-disparition des stock-options prive les entreprises émergentes du moyen de motiver leur personnel ;
2. la lourdeur et le coût considérables de l'adaptation à la loi Sarbanes-Oxley empêcheront pratiquement les entreprises émergentes d'entrer en bourse, c'est-à-dire d'accéder aux sources de capital (notons que les éventuelles entreprises émergentes françaises n'auront pas à souffrir d'un tel dommage, puisque l'accès au marché boursier leur est déjà pratiquement impossible) ;
3. cette fermeture du marché boursier aux entreprises émergentes casse le modèle américain de capital-risque, sur lequel reposait la créativité industrielle du pays ;
4. les analystes financiers optimistes, accusés d'entraîner les épargnants dans des aventures dangereuses, risquent désormais la prison : on peut s'attendre à une flambée de pessimisme ;
5. l'orientation des entreprises selon les nouveaux impératifs de réduction des coûts et d'optimisation des achats coupe court à toute tentation d'innover.

Hutcheson est d'autant plus sévère à l'égard de la législation Sarbanes-Oxley que, selon lui, les lois existantes étaient tout à fait suffisantes pour assurer la transparence et lutter contre la fraude.

Ajoutons que ces différentes législations souffrent, selon nous, d'un vice de conception : elles suggèrent que la comptabilité des entreprises pourrait résulter de l'observation neutre et objective de phénomènes naturels, un peu comme les sciences de la nature, alors qu'un système comptable est construit selon des objectifs et des intentions. La comptabilité des entreprises est construite de façon à limiter l'exposition à la fiscalité, ce qui est un impératif autrement vital que la transparence économique ; quant à la comptabilité des organismes publics, en France tout au moins, elle essaye de se couler dans un carcan réglementaire dont les premières

planches ont été clouées au XIVe siècle (cf. le livre de Laurent Bloch [20], ou sur le Web [21]).

La sécurité procédurale n'est pas la solution

Après ce tour d'horizon des normes de sécurité basées sur des procédures administratives et des excès de la sécurité appliquée au management, nous évoquerons les analyses de Jean-Pierre Dupuy [55], qui jettent une lumière vive aussi bien sur toutes ces normes que sur la mode récente du principe de précaution.

Pour décrire ces systèmes de pensée, Dupuy introduit la notion de « rationalité procédurale », qui serait le produit de réunions de comités d'experts, éventuellement à l'écoute de la société civile, et qui serait la forme consensuelle de la démocratie contemporaine. Ce modèle peut facilement être transposé à la gestion des entreprises, notamment par les méthodes de conduite de projet. « Dire que la rationalité est procédurale, c'est dire qu'une fois l'accord réalisé sur les justes et bonnes procédures, ce qu'elles produiront sera *ipso facto*, par propriété héritée en quelque sorte, juste et bon. C'est donc renoncer à chercher, indépendamment de et antérieurement à toute procédure, les critères du juste et du bien... » [nous pourrions ajouter : du vrai].

Les normes de systèmes de management (IS 9001 pour le management de la qualité, 14001 pour l'environnement, 27001 pour la sécurité de l'information) sont des outils à produire de la rationalité procédurale. Les normalisateurs eux-mêmes le revendiquent : disposer d'une organisation certifiée IS 9001 ne prouve en rien que l'organisation soit d'une qualité particulièrement excellente, cela signifie uniquement que les règles de fonctionnement de cette organisation sont documentées conformément à la norme (qui impose des règles dans certains domaines précis), et que des procédures existent pour vérifier que les règles sont appliquées, mais l'objet de ces procédures n'est en aucun cas de chercher à savoir si les décisions qui ont engendré ces règles étaient judicieuses. On peut dire la même chose des normes IS 14001 et 27001, chacune dans son domaine.

Pour continuer avec Dupuy : « La rationalité procédurale a du bon, sauf lorsqu'elle se construit au prix du renoncement à toute rationalité substantielle. » La sociologie des entreprises et l'évolution des rapports de pouvoir au sein des organisations techniques telles que les directions des systèmes d'information des entreprises, que j'ai décrites dans un ouvrage précédent [20], donnent à penser que c'est bien au re-

noncement à toute rationalité substantielle que conduisent les normes de système de management IS 9001 et IS 27001. En effet, pour un dirigeant paresseux, la grande supériorité de la rationalité procédurale sur sa cousine substantielle, c'est qu'elle dispense de toute compétence sur son objet, et surtout de toute compétence technique, ce qui dans notre beau pays est une vertu cardinale, tant la compétence technique y est méprisée. Grâce aux systèmes de management, de simples cadres administratifs pourront exercer le pouvoir sur des ingénieurs compétents, puisqu'il leur suffira pour cela de cocher dans un tableur les cases qui correspondent aux étapes des procédures, et de prendre en défaut les acteurs opérationnels qui n'auront pas rempli toutes les cases, cependant qu'eux-mêmes ne seront bien sûr jamais exposés à telle mésaventure. Une caractéristique aussi attrayante rend inévitable le triomphe de ces normes, d'autant plus que la lourdeur des opérations de constitution des feuilles de tableur et de cochage des cases (il existe aussi un marché lucratif de logiciels spécialisés) permettra le développement démographique de la caste administrative et le renforcement de son hégémonie, sans oublier l'essor des cabinets spécialisés qui pourront vendre à prix d'or la mise en place de ces systèmes, puis la rédaction de rapports vides de tout contenu « substantiel ».

Il peut sembler hasardeux de formuler un jugement aussi négatif sur les méthodes désormais classiques de conduite de projet et sur les normes de système de management : si pratiquement tous les directeurs de système d'information les adoptent, c'est qu'il doit y avoir de bonnes raisons à cela, qu'ils doivent y trouver des avantages.

La réponse tient en deux points :

- Les dirigeants qui adoptent des méthodes administratives de management des activités techniques en tirent effectivement des avantages, ceux que j'ai décrits ci-dessus, notamment en termes de renforcement du pouvoir administratif et de diminution de l'exigence de compétence.
- Jean-Pierre Dupuy a emprunté à Friedrich von Hayek une théorie qui est de plus en plus utilisée par les économistes, et qui étudie les phénomènes d'imitation au sein de l'économie de marché. Alors que l'économie néoclassique se représente un *homo œconomicus* autosuffisant et indépendant, parfaitement informé et rationnel dans des choix censés le mener à un optimum qui, à l'échelle du marché, produirait un équilibre, Hayek met en évidence, après Adam Smith et Keynes, le rôle central de l'*imitation* dans les phénomènes collectifs dont le marché est le cadre. Le rôle de l'imitation semble particulièrement important dans les situations de choix entre techniques rivales, et aucun mécanisme ne garantit que la technique qui va l'emporter sera

> la meilleure. En effet, dans le jeu de miroirs qui précède l'engouement mimétique, une simple rumeur peut orienter quelques acteurs vers la cible, ce qui déclenchera un effet d'avalanche : « [l'imitation généralisée] suscite des dynamiques autorenforçantes qui convergent si résolument vers leur cible qu'il est difficile de croire que cette convergence n'est pas la manifestation d'une nécessité sous-jacente... ». Nous ne saurions écarter l'hypothèse que le succès universel des méthodes de gestion de projet pourrait résulter d'un phénomène mimétique de ce type : dit en d'autres termes, pour citer un proverbe du réseau, « 100 000 lemmings ne peuvent pas avoir tort ».

De ce qui précède peut-on déduire qu'il faut forcément être ingénieur informaticien pour devenir directeur du système d'information ? Non, mais un DSI (et d'ailleurs tout dirigeant) devra posséder, pour remplir ses fonctions, un certain nombre de compétences, et il ne pourra pas faire face aux problèmes qui se posent à lui uniquement avec des procédures administratives normalisées. Le rôle de l'informatique dans le monde contemporain est tel que nul ne peut plus se passer d'en connaître les techniques de base.

Dans le contexte français, où l'absence de compétence technique est devenue un atout déterminant pour l'accès aux postes de direction des systèmes d'information [13], les méthodes de management de système selon les normes IS 9001 et IS 27001 acquièrent la propriété de prédictions autoréalisatrices : pour les raisons évoquées ci-dessus, de nombreux DSI ont d'ores et déjà emprunté cette démarche, et leurs collègues en retard, qui n'ont pour boussole dans cet univers que l'air du temps et le qu'en dira-t-on, trouveront facilement auprès de leurs pairs la confirmation que c'est bien dans cette voie qu'il faut aller. Les sommes considérables englouties par ces méthodes n'apparaissent pas forcément comme des inconvénients, puisqu'elles renforcent l'importance et le prestige de celui qui les ordonne, et donnent satisfaction à la direction générale qui ne dispose en général ni des informations ni des moyens d'investigation nécessaires pour se former une opinion sur le sujet, et qui peut faire état du recours à ces méthodes éprouvées pour répondre aux questions des auditeurs ou des actionnaires.

Quant à nous, nous nous efforcerons au cours des chapitres suivants de dispenser les principes de sécurité substantielle qui nous semblent le socle de ce que doit être aujourd'hui un système sûr, et que plus grand monde ne peut se permettre d'ignorer

13. Cette phrase pourrait en fait être remplacée par la suivante : en France, surtout dans les services publics, l'absence de compétence technique est depuis longtemps un atout déterminant pour l'accès aux postes de direction.

totalement, que ce soit dans l'entreprise ou dans l'usage privé des ordinateurs et des réseaux.

Richard Feynman à propos de la conduite de projet

Un des derniers écrits du physicien Richard P. Feynman, prix Nobel 1965, fut une annexe [66] au rapport de la Commission Rogers rédigé à la demande des autorités gouvernementales américaines à la suite de l'accident dramatique de la navette spatiale Challenger et destiné à en élucider les circonstances. Il y a suffisamment de points communs entre un sinistre spatial et un sinistre informatique pour que les leçons tirées de celui-là puissent être utiles à ceux qui se préoccupent de celui-ci ; en effet, si les objets produits par l'industrie spatiale et par l'industrie informatique paraissent très dissemblables, les méthodes de conduite de projet mises en œuvre dans l'un et l'autre cas puisent à la même source d'inspiration (le projet Apollo dans les années 1960), et risquent donc d'avoir des effets similaires. En outre, même si le risque semble bien moindre de mettre en danger des vies humaines dans le second cas que dans le premier, il convient de noter qu'une navette spatiale incorpore des millions de lignes de logiciel informatique, soit embarqué soit dans les installations au sol, sans oublier les programmes qui ont servi à sa conception. Il n'y a donc aucune raison de se priver des enseignements prodigués à cette occasion par un des scientifiques les plus réputés du XX^{e} siècle, notamment pour ses talents pédagogiques.

Pour établir son rapport, R. Feynman a rencontré différents experts qui avaient participé à la conception et à la réalisation de la navette spatiale, ou qui avaient donné des consultations à son sujet avant ou après l'accident, et il a lu leurs rapports. Il a été frappé par la discordance extraordinaire, parmi les experts et les officiels de la NASA, des opinions relatives au risque d'accident mortel, puisqu'elles vont de 1 accident sur 100 vols à 1 accident sur 100 000 vols, où les premières émanent surtout des ingénieurs qui ont réellement travaillé sur le projet, et les dernières plutôt des managers. Il a également observé la diminution au fil du temps de la sévérité des critères de certification, au fur et à mesure que les vols sans incidents instauraient l'idée que « puisque le risque avait été encouru jusqu'à présent sans qu'un accident survienne, il pouvait être accepté pour la prochaine fois ».

Pour ce qui nous concerne ici, la passage le plus intéressant du texte est celui qui a trait aux moteurs à combustible liquide de la navette (*Space Shuttle Main Engines*, SSME). Ces composants sont parmi les plus complexes de l'ensemble. Feynman explique que la méthode habituelle de conception de tels moteurs (par exemple

pour des avions civils ou militaires) procède selon une démarche *de bas en haut (bottom up)* : on commence par étudier les caractéristiques souhaitables des matériaux à utiliser, puis on teste des pièces élémentaires au banc d'essai. Sur la base des connaissances acquises ainsi, on commence à tester des sous-ensembles plus complexes. Les défauts et les erreurs de conception sont corrigés au fur et à mesure : comme ils ne portent que sur des parties de l'ensemble, les coûts sont modérés. Si des défauts sont encore détectés au moment de l'assemblage de l'ensemble, ils restent relativement faciles à localiser et à corriger, notamment du fait de l'expérience acquise par les tests de sous-ensembles.

Or les moteurs à combustible liquide de la navette n'ont pas été conçus selon cette démarche *bottom up*, mais selon l'approche inverse, de *haut en bas (top down)*, c'est-à-dire que le moteur a été conçu et réalisé tout en même temps, avec très peu d'études et d'essais préalables des matériaux et des composants ; avec une telle démarche, la recherche de l'origine d'un défaut ou d'une erreur de conception est beaucoup plus difficile qu'avec la méthode *bottom up*, parce que l'on dispose de peu d'informations sur les caractéristiques des composants. Il faut alors utiliser le moteur complet comme banc d'essai pour trouver la panne, ce qui est très difficile et onéreux. Il est en outre difficile dans ces conditions d'acquérir une compréhension détaillée des caractéristiques et du fonctionnement du moteur, compréhension qui aurait été de nature à fonder la confiance que l'on aurait pu avoir en lui.

La méthode *top down* a un autre inconvénient : si l'on trouve une erreur de conception sur un sous-ensemble, comme la conception n'en a pas été isolée, mais intégrée dans la conception d'ensemble, il faut repenser la conception générale. Il est à craindre que pour des erreurs jugées mineures (à tort ou à raison), la lourdeur des investigations à entreprendre n'incite pas à renoncer à reprendre la conception de l'ensemble, alors qu'il faudrait le faire.

Nous pensons que cette critique de la méthode *top down* par Richard P. Feynman s'applique bien aux systèmes informatiques, et particulièrement aux systèmes de sécurité informatique. Mais ne lui faisons pas dire ce qu'elle ne dit pas : il convient bien sûr d'avoir une vision d'ensemble du système, simplement il ne faut pas lui accorder les vertus qu'elle n'a pas, elle ne doit pas être trop précise, ce n'est pas d'elle qu'il faudra déduire la conception détaillée des éléments et des sous-systèmes.

9

Une charte de l'administrateur système et réseau

La multiplication de questions de plus en plus complexes liées à la sécurité des systèmes et des réseaux, l'imbrication de plus en plus intime des aspects techniques et juridiques de ces questions et le risque accru de conséquences judiciaires en cas d'erreur incitent à la rédaction, au sein de chaque entreprise ou organisation, d'une *charte de l'administrateur de système et de réseau* qui rappelle les devoirs, les pouvoirs et les droits des ingénieurs et des techniciens qui administrent la sécurité des réseaux, des ordinateurs et en fin de compte du système d'information. Le présent chapitre énonce les principes qui peuvent conduire la rédaction d'un tel document, puis en propose un exemple pour une entreprise fictive.

Complexité en expansion et multiplication des risques

L'activité de l'administrateur de système et de réseau le confronte à un certain nombre de paradoxes : par exemple, il doit configurer son système d'acheminement de messagerie électronique (*Mail Transfer Agent*, MTA, ou passerelle de messagerie) de façon à tenir un journal de tous les messages émis et reçus par le point d'accès à l'Internet dont il est responsable, c'est une obligation légale. Mais s'il oublie de détruire ces journaux à l'issue d'un délai maximal d'un an, il enfreint une autre obligation légale qui résulte des directives de la CNIL.

Cette activité d'administration de la passerelle de messagerie de l'entreprise lui permet de détecter les usages contraires à la loi qui pourraient en être faits par des employés indélicats, dont les exemples les plus courants sont, non limitativement :

- envoi de messages ou abonnement à des listes de diffusion susceptibles de tomber sous le coup des lois qui répriment le racisme et la xénophobie, la pédophilie ou le trafic d'êtres humains ;
- communication à des tiers d'informations couvertes par le secret professionnel, qui constituent le patrimoine intellectuel de l'entreprise, et dont la divulgation à des concurrents est de nature à causer un préjudice certain ;
- infraction à la législation sur la propriété littéraire et artistique, lorsque les serveurs de l'entreprise sont utilisés pour télécharger ou, pire, redistribuer des œuvres musicales ou cinématographiques couvertes par des droits d'auteur ;
- délit de presse, par l'ouverture de sites Web ou de forums au contenu susceptible d'être attaqué au titre des lois sur la diffamation, le plagiat, etc.

La constatation de telles infractions oblige l'administrateur à y mettre fin, mais dans les cas où les manifestations de ces actes ne sont pas publiques (cas du courrier électronique), s'il en fait état dans un rapport à la direction de l'entreprise, il s'expose à être condamné par un tribunal en vertu de la loi qui protège le secret de la correspondance. En effet, si la jurisprudence (arrêt du 17 décembre 2001 de la cour d'appel de Paris, « ESPCI », École Supérieure de Physique et Chimie industrielle) reconnaît que l'administrateur détient la possibilité technique de lire les contenus des messages, celui-ci n'est en revanche pas autorisé à les divulguer même à ses supérieurs hiérarchiques.

« Ainsi la délicate mission de l'administrateur sera de mettre fin au comportement frauduleux ou préjudiciable sans en informer son supérieur hiérarchique qui

dispose pourtant de l'autorité et du pouvoir de décision », note Laurence Freyt-Caffin [72].

De façon plus générale, l'administrateur de système et de réseau a accès à toutes les données de l'entreprise et des utilisateurs qui stationnent ou circulent sur les machines et les réseaux dont il a la responsabilité : ce pouvoir le soumet en permanence à la tentation d'en abuser, même si ce n'est que pour simplifier sa tâche, ou rendre service aux utilisateurs, ou pour assurer le bon fonctionnement des infrastructures en question.

De façon nettement plus embarrassante, il peut recevoir de sa hiérarchie des injonctions contraires aux lois : il est alors placé devant le dilemme d'avoir à désobéir à ces injonctions, ce qui peut mettre en péril sa situation professionnelle, ou d'enfreindre la loi, ce qui risque de le mener devant un juge.

Règles de conduite

L'administrateur de systèmes et de réseaux dispose de pouvoirs importants : il importe de circonscrire avec soin l'usage qu'il peut en faire afin d'éviter les abus, notamment par l'atteinte à la confidentialité des échanges et des données.

Secret professionnel

Le devoir de secret professionnel s'impose aux administrateurs ayant accès aux données personnelles des utilisateurs dans le cadre de leurs fonctions [1].

1. Arrêt de la chambre sociale de la Cour de cassation en date du 2 octobre 2001 : « Attendu que le salarié a droit, même au temps et au lieu de travail, au respect de l'intimité de sa vie privée ; que celle-ci implique en particulier le secret des correspondances ; que l'employeur ne peut dès lors sans violation de cette liberté fondamentale prendre connaissance des messages personnels émis par le salarié et reçus par lui grâce à un outil informatique mis à sa disposition pour son travail et ceci même au cas où l'employeur aurait interdit une utilisation non professionnelle de l'ordinateur. »

1. On consultera avec profit le livre que Fabrice Mattatia a consacré au traitement des données personnelles [107].

2. Code du travail, articles L432-2-1 : « Le comité d'entreprise est informé, préalablement à leur utilisation, sur les méthodes ou techniques d'aide au recrutement des candidats à un emploi ainsi que sur toute modification de celles-ci. Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci. Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. »

Mots de passe

J'emprunte ici à Patrick Chambet les idées qu'il a exprimées sur la liste de diffusion de l'Ossir[2] :

« — Non ! Les administrateurs ne doivent jamais connaître les mots de passe des utilisateurs.

— Pourquoi l'administrateur n'a-t-il pas besoin de connaître les mots de passe ?

— Un administrateur est, par définition, celui qui possède des privilèges élevés. En particulier, il peut effectuer toutes les tâches nécessaires en l'absence des utilisateurs, comme par exemple la prise de possession de fichiers, la modification des permissions d'accès à des ressources, etc. Pour cela, il n'a pas besoin et ne doit pas [commettre d'usurpation de personnalité] (se loger avec le *login* et le mot de passe de l'utilisateur).

S'il doit tout de même se résoudre à cela, l'utilisateur légitime devrait être présent (ce point devrait être débattu par les juristes de la liste, car le règlement intérieur de l'entreprise, la charte informatique, la politique de sécurité et les lois, décrets et jurisprudence entrent en jeu).

Il arrive que l'administrateur fasse tourner un *craqueur* de mots de passe pour vérifier la robustesse des mots de passe des utilisateurs. Mais dans ce cas, dès qu'un mot de passe est craqué, il doit demander immédiatement à l'utilisateur de le changer pour un mot de passe de robustesse au moins équivalente. Il ne le connaît donc plus.

— Pourquoi l'administrateur ne doit-il pas connaître les mots de passe ?

2. http://www.ossir.org

— Tout d'abord pour dégager sa responsabilité en cas d'activité délictueuse effectuée à l'aide d'un compte utilisateur particulier : l'utilisateur en question ne pourra plus dire que ce n'est pas lui, mais l'administrateur qui a envoyé tel [message électronique].

Ensuite, pour le respect de la confidentialité des ressources utilisateurs (classifiées ou non), même si, par définition, un administrateur pourra toujours, à l'aide d'une action volontaire et avec une intention évidente (plaidable devant un juge si l'administrateur n'a pas reçu d'ordre explicite), accéder aux ressources en question.

D'un côté l'administrateur est protégé, de l'autre il devient plus facilement condamnable. »

Les injonctions hiérarchiques à violer le secret des mots de passe sont fréquentes, souvent pour des raisons en apparence excellentes : accéder aux données cruciales détenues par un utilisateur en vacances et inaccessible en est l'exemple typique. Il peut être très difficile de résister à une telle demande, et l'utilisateur à son retour peut détecter l'intrusion en consultant les journaux du système. Certes l'administrateur peut détruire ou modifier les éléments de journalisation relatifs à son action, mais cette altération même des journaux peut être détectée, quoique plus difficilement, et en cas de comparution devant un tribunal il aura ainsi considérablement aggravé sa faute. Si pour une raison ou pour une autre les relations entre le possesseur des données et son employeur ou l'administrateur sont conflictuelles, on voit toutes les conséquences fâcheuses que peut entraîner cet enchaînement de circonstances. Il convient donc d'éviter absolument de commettre de telles actions.

Proposition de charte

La présente charte de l'administrateur de système et de réseau de l'INSIGU [3], ci-dessous désigné « l'institut », est destinée à déterminer les devoirs, les pouvoirs et les droits des ingénieurs et des techniciens qui administrent la sécurité des réseaux, des ordinateurs et du système d'information de l'institut.

Cette charte est promulguée en référence à la charte de l'utilisateur des ressources informatiques et des services Internet de l'institut (cf. chapitre 8, page 195), qu'elle complète et dont elle est inséparable.

3. L'Institut national des sciences informatiques et géographiques de l'univers (INSIGU) est un organisme de recherche fictif, pour les besoins de notre exemple.

Définitions

Les *entités* de l'INSIGU, ses *ressources informatiques*, ses *services Internet* et les *utilisateurs* du système d'information qu'ils constituent sont définis ici comme dans la charte de l'utilisateur des ressources informatiques et des services Internet de l'institut (cf. chapitre 8, page 196).

L'*administrateur* d'un système ou d'un réseau de l'INSIGU est toute personne, employée ou non par l'institut, à laquelle a été confiée explicitement et par écrit, sous la forme d'une lettre de mission, d'un profil de poste annexé au contrat de travail ou d'un contrat de prestations de service, la responsabilité d'un système informatique, d'un réseau ou d'un sous-réseau administrés par une entité de l'institut, ou de plusieurs de ces éléments. Une personne à qui a été conférée une telle responsabilité sera désignée dans la suite de ce document par le terme *administrateur*. L'ensemble des éléments sur lesquels s'exerce cette responsabilité constitue le *périmètre d'activité* de l'administrateur.

Le *comité de coordination* de sécurité du système d'information (SSI) est constitué de responsables chargés d'émettre des règles et des recommandations dans le domaine SSI, de prendre les mesures appropriées pour qu'elles soient mises en vigueur, et d'organiser les activités de formation, d'information et de sensibilisation de nature à améliorer les conditions de leur application ; il est en outre chargé de suivre la juridiction et notamment les arrêtés et jurisprudences. Les membres de ce comité de coordination sont le Responsable de sécurité des systèmes d'information (RSSI) de l'institut, le responsable de la sécurité opérationnelle au sein du département du système d'information (DSI) de l'institut, le correspondant informatique et libertés de l'institut et d'autres personnes désignées par le directeur général de l'institut ou son représentant autorisé, notamment un représentant du département des affaires juridiques.

Les devoirs, les pouvoirs et les droits de l'administrateur, définis dans la présente charte, constituent ensemble les *responsabilités SSI* de l'administrateur.

Les consignes du comité de coordination SSI s'imposent aux administrateurs de systèmes et de réseaux pour l'exercice de leurs responsabilités SSI dans leur périmètre d'activité.

Responsabilités du comité de coordination SSI

Surveillance et audit

Le comité de coordination SSI organise la surveillance et l'audit de toutes les activités des systèmes et de tous les trafics réseau sur les infrastructures administrées par l'INSIGU.

Pour ce faire, le comité de coordination SSI est habilité à donner des consignes de surveillance, de recueil d'information et d'audit aux administrateurs concernés.

Contrôle d'accès

Le comité de coordination SSI définit des règles de contrôle d'accès aux systèmes et aux réseaux conformes à la présente charte et à la charte de l'utilisateur des ressources informatiques et des services Internet de l'institut.

Vérification

Le comité de coordination SSI et les administrateurs concernés sont habilités à entreprendre toutes actions appropriées pour vérifier la bonne application des règles de contrôle d'accès aux systèmes et aux réseaux définies à l'article précédent, ainsi que pour détecter leurs vulnérabilités.

Responsabilités de l'administrateur de système et de réseau

Enregistrement des incidents de sécurité

L'administrateur conserve une trace écrite des incidents de sécurité survenus dans son périmètre d'activité. Cette trace doit comporter les indications de date et d'heure des événements considérés, et une description de ces événements.

Notification des incidents de sécurité

Les administrateurs de système et de réseau sont tenus de déclarer tout incident de sécurité au RSSI et au responsable de la sécurité opérationnelle. Les directives du RSSI et du responsable de la sécurité opérationnelle pour des actions relatives aux incidents sont mises en application sans délais.

Journalisation et archivage

L'administrateur active sur les systèmes dont il a la responsabilité les journaux nécessaires à l'identification et à la reconstitution des séquences d'événements qui pourraient constituer un incident de sécurité, ou qui pourraient faire l'objet d'une commission rogatoire émise par les autorités judiciaires. Il archive les données ainsi recueillies dans des conditions propres à en assurer l'intégrité, la disponibilité, l'authenticité et la confidentialité.

Il mène cette activité de journalisation et d'archivage dans des conditions qui garantissent le respect des lois et des règlements relatifs aux libertés publiques et privées, au secret des correspondances, au droit d'accès à l'information, et il veille notamment à détruire tous les journaux qui comportent des données nominatives à l'expiration d'un délai qui ne peut excéder un an, ou le délai légal à la date considérée.

Parmi les textes législatifs et réglementaires qui s'appliquent à cette activité, il convient d'accorder une attention particulière à la norme simplifiée nº 46 de la Commission nationale informatique et libertés, « destinée à simplifier l'obligation de déclaration des traitements mis en œuvre par les organismes publics et privés pour la gestion de leurs personnels » [4].

Examen des journaux

L'administrateur examine régulièrement les journaux mentionnés à l'article ci-dessus.

Dérogations aux règles SSI

Les règles SSI mentionnées dans la présente charte, dans la charte de l'utilisateur des ressources informatiques et des services Internet de l'INSIGU, ou édictées par le RSSI de l'institut, par le responsable de la sécurité opérationnelle au sein du DSI de l'institut ou par le comité de coordination SSI s'imposent à tous les utilisateurs des systèmes d'information de l'institut, qu'ils soient on non des employés de l'institut. Les administrateurs de systèmes et de réseaux de l'institut ont pour mission de les mettre en œuvre et de les faire respecter dans leur périmètre d'activité.

Les responsables d'entités qui voudraient passer outre ces règles SSI, ou entreprendre des actions qui dérogeraient à ces règles, doivent :

4. http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/169/

- remettre à l'administrateur responsable des infrastructures concernées un document écrit et signé par lequel ils assument explicitement la responsabilité de cette dérogation, des risques qui en découlent, et de leurs conséquences ;
- obtenir du directeur général de l'INSIGU ou de son représentant désigné une décharge écrite pour le RSSI, le DSI et affiliés.

Les utilisateurs qui ne seraient pas responsables d'entités et qui voudraient bénéficier de telles dérogations doivent obtenir qu'elles soient endossées par leur responsable d'entité, dans les conditions indiquées à l'alinéa précédent.

Identification des utilisateurs et contrôles d'accès

Dans leur périmètre d'activité, les administrateurs responsables sont seuls habilités à mettre en place et à administrer les systèmes d'identification et d'authentification des utilisateurs, conformes aux directives du comité de coordination SSI. Il en va de même pour les dispositifs de contrôle d'accès aux systèmes, aux réseaux et aux données.

Sauf exception formulée par un document écrit signé d'un responsable d'entité, seuls l'administrateur local et ses collaborateurs immédiats possèdent les droits d'administrateur sur les postes de travail des utilisateurs des SI de l'institut.

Audits périodiques

Les administrateurs procèdent deux fois par an à un audit des comptes des utilisateurs et des droits d'accès associés, pour vérifier leur validité et leur exactitude.

Mise en œuvre et litiges

Rapport des violations des règles SSI

Pour toute violation des règles SSI qu'il est amené à constater, l'administrateur établit un rapport écrit destiné au comité de coordination SSI et à ses responsables hiérarchiques.

Veille SSI

Les administrateurs exercent régulièrement une activité de veille scientifique et technologique dans le domaine SSI. Ils sont abonnés aux listes de diffusion qui

publient les découvertes de vulnérabilités. Ils participent notamment aux activités de formation, d'information et de sensibilisation entreprises par le comité de coordination SSI.

Attitude à l'égard des violations de la loi

Lorsque l'administrateur constate des violations de la loi dans son périmètre d'activité, il en fait rapport au comité de coordination SSI et à ses responsables hiérarchiques, qui prendront les mesures adéquates afin de coordonner leurs actions avec les autorités judiciaires.

Attitude à l'égard des violations des règles SSI

La direction de l'INSIGU, ou son représentant qualifié, peut révoquer le compte et les droits d'accès au réseau et aux données d'un utilisateur qui aurait violé les règles SSI mentionnées dans la Charte de l'utilisateur des ressources informatiques et des services Internet de l'institut.

Première partie

Principes de sécurité du système d'information

Deuxième partie

Science de la sécurité du système d'information

Troisième partie

Politiques de sécurité du système d'information

Quatrième partie

Avenir de la sécurité du système d'information

Conclusion

Dans le domaine de la sécurité des systèmes d'information, mieux vaut prévenir que guérir.

Prévenir est impératif, parce que guérir est impossible et ne sert à rien. Lorsqu'un accident ou un pirate a détruit les données de l'entreprise et que celle-ci n'a ni sauvegarde ni site de secours, elle est condamnée, tout simplement : les personnels ne savent plus quoi produire, ni pour quels clients, les comptables ne peuvent plus encaisser les factures ni payer personnels et débiteurs, ses commerciaux n'ont plus de fichier de prospects.

Oui, le responsable de sécurité doit être agnostique et pessimiste : il *sait* que son pare-feu sera franchi, que son antivirus ne sera pas à jour, que son système de détection d'intrusion ne le préviendra pas de l'attaque, que ses copies de sauvegarde seront corrompues, que son site de secours sera inondé ou détruit par un incendie, que son système redondant ne se déclenchera pas ; mais, éduqué dans la religion probabiliste, il *sait* que toutes ces catastrophes ne surviendront pas simultanément.

L'idée de *défense en profondeur* se distingue de la démarche agnostique probabiliste : si la garnison de mon pare-feu est finalement submergée par l'assaillant, elle en aura néanmoins réduit les effectifs avant de succomber, ce qui facilitera la mission des escadrons d'antivirus, et ainsi mon système redondant risquera moins d'être saboté par un ver qui pourrait l'empêcher de se déclencher. Si, au contraire, je mise tout sur mon pare-feu ou sur mon réseau privé virtuel et que derrière cette protection je commets des imprudences, je succombe au syndrome de la *ligne Maginot* : le jour où la défense est enfoncée ou contournée, tout est perdu. Or, une chose est sûre, la défense sera enfoncée. Un jour.

Une autre certitude : le risque ne vient pas seulement de l'extérieur. Les sources de danger prolifèrent aussi à l'intérieur du réseau, et d'ailleurs la frontière entre l'intérieur et l'extérieur tend non pas à disparaître, mais à devenir poreuse et floue, avec les systèmes mobiles en tout genre qui entrent et qui sortent, les tunnels vers d'autres réseaux, les nouveaux protocoles infiltrables et furtifs. Les protocoles de téléphonie par Internet, de visioconférence et autres systèmes multimédia sont *tous* des failles béantes de sécurité, et la situation sur ce front ne s'améliorera pas avant des années.

Nous voyons que les menaces sont protéiformes, les vulnérabilités foisonnantes et le tout en transformation constante : c'est dire que le responsable de sécurité ne choisit pas le terrain sur lequel il va devoir manœuvrer, il va lui falloir faire preuve d'adaptabilité et de pragmatisme. S'il ne veut pas se trouver condamné à réagir frénétiquement mais trop tard à des avalanches d'incidents mystérieux, il devra néanmoins établir un socle stable pour son activité, dont nous avons établi en principe qu'elle sera essentiellement préventive. Pour cela, il lui faudra principalement deux choses : une vraie compétence technique dans son domaine, suffisamment large et profonde pour embrasser réseaux et systèmes, et, au sein de son entreprise, le pouvoir d'édicter les règles dans son domaine, et de les faire respecter : interdire les protocoles dangereux, imposer la mise à jour automatique des antivirus, mettre son veto à tel ou tel passe-droit dans le pare-feu. Cela s'appelle une politique de sécurité.

Il serait vain d'espérer faire l'économie de cette compétence technique et de son instanciation dans une politique de sécurité en lui substituant des procédures. Il ne manque pas de méthodes qui laissent croire que que la sécurité des systèmes d'information pourrait être assurée par des routines administratives : nous avons signalé et expliqué leur vanité à la fin du premier chapitre de ce livre. Nous dirons que ces méthodes de sécurité sont procédurales, ou, plus crûment, qu'elles sont bureaucratiques.

Nous avons donc le choix entre ces méthodes bureaucratiques et celles que nous appellerons méthodes de sécurité négative, parce qu'elles proposent de colmater les failles dès que celles-ci sont découvertes et d'interdire les malfaisances après qu'elles se sont manifestées : aucune de ces méthodes n'est satisfaisante, nous l'avons vu. Nous préconiserons plutôt celles qui visent ce que nous appellerons la *sécurité positive*, parce qu'elles posent *a priori* ce qui est sûr, et qu'elles établissent la sécurité dès la conception des systèmes, par la définition de ce qu'ils doivent faire et l'interdiction du reste selon une règle que nous énoncerons ainsi : « N'est permis que ce qui est explicitement autorisé, tout le reste est interdit. » Une règle aussi sévère ne

saurait s'appliquer qu'aux systèmes sensibles de l'entreprise : pour le reste, il faut laisser un peu plus de latitude aux utilisateurs, mais uniquement dans les zones moins sensibles du Système d'information et du réseau.

Par exemple, à l'heure où pratiquement toutes les applications informatiques sont fondées sur les techniques du Web, nous pensons, en suivant Marcus J. Ranum, qu'un outil de choix pour la sécurité positive est le *mandataire applicatif (reverse proxy)* : il s'agit d'un serveur Web spécialisé, qui reçoit les messages du protocole HTTP, les filtre, rejette ce qui n'est pas autorisé et *réécrit* les requêtes avant de les transmettre au « vrai » serveur, ce qui élimine tout imprévu et pare aux déficiences du véritable serveur, et notamment à toute une famille d'attaques par injection de code. Cette méthode revient à écrire sa propre version du protocole, adaptée exactement à ce que l'on veut faire.

De façon générale, l'évolution de l'informatique, de ses usages, et par conséquent des systèmes d'information est déterminée par l'offre de technologie plus que par les demandes des utilisateurs, parce que celle-là évolue plus vite que celles-ci. Pour des raisons évidentes, voikà qui est encore plus vrai pour les questions de sécurité, parce que les utilisateurs ne « demandent » rien, et que l'« offre » est par définition destinée à surprendre ses « clients » par des attaques auxquelles ils ne s'attendent pas. La lutte contre cette « offre » un peu spéciale ne peut donc reposer sur les attentes du client, et la veille technologique « tous azimuts », si elle est nécessaire, ne saurait prétendre à l'efficacité totale. Ce qui renforce l'argument pour la sécurité positive.

Pour toutes les raisons qui viennent d'être énoncées, nous pouvons conclure en disant avec Bruce Schneier ? que la sécurité du système d'information n'est pas et ne peut pas être contenue dans un dispositif ni dans un ensemble de dispositifs, qu'elle ne peut pas non plus être contenue dans les limites temporelles d'un *projet*, mais qu'elle est un *processus* ou, si l'on veut, une *activité*. Nous entendons par là que les ingénieurs de sécurité du SI doivent se consacrer à cette activité, pas forcément à plein temps, mais en permanence, sur plusieurs fronts : veille scientifique et technologique, surveillance des journaux d'événements, audit des infrastructures et des applications, sensibilisation et formation des utilisateurs, expérimentation de nouveaux outils et de nouveaux usages. La démarche de sécurité doit être active : la détection des failles et des attaques, et les réponses qui leur sont données, ne sont pas suffisantes, mais elles sont nécessaires, parce qu'avec l'ubiquité de l'Internet nous sommes entrés dans une ère où le régime de menaces est de basse intensité, mais où les menaces sont permanentes. Il faut savoir que parmi ces menaces

certaines se réaliseront, qu'il faut s'y préparer et apprendre à leur survivre, ce qui suppose que l'on y ait pensé *avant*.

Si l'on peut risquer quelques hypothèses sur ce à quoi ressembleront l'informatique et l'Internet qui nous attendent dans les années qui viennent, nous pouvons dire que les questions de sécurité informatique y tiendront beaucoup plus de place, et que la gestion des identités numériques sera au cœur des réponses qui pourront être apportées à ces questions.

Nous ne saurions refermer ce livre sur une note angoissante de risques et de menaces : parmi les apports à la société de l'informatique en général, et plus particulièrement des techniques de sécurité étudiées dans ce livre, il faut compter la mise à la disposition du citoyen ordinaire de moyens réservés jusque là aux services secrets des grandes puissances et aux grandes sociétés multinationales, tels que le chiffrement et la communication confidentielle à grande distance. Plus généralement, les possibilités de publier des informations et d'en recevoir ont connu un essor inimaginable il y a seulement une vingtaine d'années, par la combinaison des logiciels libres et de l'Internet, indissociables dès leur origine. Nul doute que ce soit une contribution significative à la liberté d'expression et, *in fine*, à la démocratie.

Bibliographie

[1] « Projet Tor ». Avril 2011. http://www.torproject.org.

[2] « The web's trust issues ». *The Economist*, avril 2011. http://www.economist.com/blogs/babbage/2011/04/internet_security&fsrc=nwl.

[3] Jean-François Abramatic. « Croissance et évolution de l'Internet ». Dans *Université de tous les savoirs – Les Technologies*, volume 7, Paris, 2002. Odile Jacob.

[4] Jean-Raymond Abrial. *The B Book - Assigning Programs to Meanings*. Cambridge University Press, Cambridge, 1996.

[5] Adullact. « Site de l'Adullact ». *Association des développeurs et des utilisateurs de logiciels libres pour l'administration et les collectivités territoriales*, 2005. http://www.adullact.org/archives/285-un-cadre-de-reflexion-pour-comprendre-l-impact-du-choix-des-licences-copyleft-telle-que-la-gpl-par-opposition-aux-licences-non-copyleft.

[6] Agence nationale de la sécurité des systèmes d'information. « EBIOS 2010 – Expression des Besoins et Identification des Objectifs de Sécurité ». 2010. http://www.ssi.gouv.fr/fr/bonnes-pratiques/outils-methodologiques/ebios-2010-expression-des-besoins-et-identification-des-objectifs-de-securite.html.

[7] Tris Alcatrinei-Aldea. « Le BYOD et le droit : le couple mal assorti ». *MISC*, (66), mars-avril 2013.

[8] Pascal Aubry, Julien Marchal, et Vincent Mathieu. Single Sign-On Open Source *avec CAS*. 2003. http://2003.jres.org/actes/paper.139.pdf.

[9] Autorité de régulation des communications électroniques et des postes (ARCEP). « Le cadre réglementaire des réseaux RLAN / Wi-Fi depuis le 25 juillet 2003 ». 8 août 2003. http://www.arcep.fr/index.php?id=8127.

[10] Gildas Avoine, Pascal Junod, et Philippe Oechslin. *Sécurité informatique – Exercices corrigés*. Vuibert, Paris, 2004. Préface de Robert Longeon.

[11] Daniel Azuelos. « Architecture des réseaux sans fil ». Dans JRES, editor, *Actes du congrès JRES*, 2005. http://2005.jres.org/tutoriel/Reseaux_sans_fil.livre.pdf.

[12] Général de Brigade Bailey, MBE. « Le combat dans la profondeur 1914-1941 : la naissance d'un style de guerre moderne ». *Les cahiers du Retex*, (15), Mars 2005.

[13] Scott Barman. *Writing Information Security Policies*. New Riders, Indianapolis, USA, 2002.

[14] Salman A. Baset et Henning Schulzrinne. « An Analysis of the Skype Peer to Peer Internet Telephony Protocol ». *arXiv.org*, Septembre 2004. http://arxiv.org/ftp/cs/papers/0412/0412017.pdf.

[15] Robert Belk et Matthew Noyes. « On the Use of Offensive Cyber Capabilities – A Policy Analysis on Offensive US Cyber Policy ». mars 2012. http://belfercenter.ksg.harvard.edu/files/cybersecurity-pae-belk-noyes.pdf.

[16] Daniel Berg-Domscheit. *Inside WikiLeaks*. Grasset, Paris, 2011. 319 p.

[17] Didier Bert, Henri Habrias, et Véronique Viguié Donzeau-Gouge (éd.). « Méthode B (numéro spécial) ». *Technique et science informatique*, 22, 1/2003.

[18] Philippe Biondi et Fabrice Desclaux. « Silver Needle in the Skype ». *Black-Hat Europe*, 2-3 mars 2006. http://www.secdev.org/conf/skype_BHEU06.pdf.

[19] Laurent Bloch. *Les systèmes d'exploitation des ordinateurs – Histoire, fonctionnement, enjeux*. Vuibert, Paris, 2003. Texte intégral disponible ici : http://www.laurentbloch.org/MySpip3/spip.php?article13.

[20] Laurent Bloch. *Systèmes d'information, obstacles et succès – La pensée aux prises avec l'informatique*. Vuibert, Paris, 2005. Texte intégral disponible en ligne ici : http://www.laurentbloch.org/MySpip3/spip.php?rubrique5.

[21] Laurent Bloch. « Théorie et pratique de la commande publique ». 2005. http://www.laurentbloch.org/MySpip3/spip.php?article135.

[22] Laurent Bloch. *Systèmes de fichiers en réseau : NFS, SAN et NAS*. 2008. Texte disponible ici : http://www.laurentbloch.org/MySpip3/spip.php?article121.

[23] Laurent Bloch. « La régulation universelle de l'Internet, enjeu économique et culturel ». *Questions internationales*, (39), septembre-octobre 2009. http://www.ladocumentationfrancaise.fr/revues-collections/questions-internationales/39/sommaire39.shtml.

[24] Laurent Bloch. « La maîtrise d'Internet : des enjeux politiques, économiques et culturels ». *Questions internationales*, (47), janvier-février 2011. Numéro spécial Internet http://www.ladocumentationfrancaise.fr/revues-collections/questions-internationales/47/sommaire47.shtml.

[25] Laurent Bloch et Nat Makarévitch. « La signature électronique universelle ». *Site Web de Laurent Bloch*, mars 2007. http://www.laurentbloch.org/MySpip3/spip.php?article107.

[26] Frédéric Bonnaud. « Signer et chiffrer avec GnuPG ». *Lea-Linux.org*, Décembre 2010. http://www.lea-linux.org/documentations/index.php/Reseau-secu-gpg-intro.

[27] Stéphane Bortzmeyer. « Mon blog ». Avril 2011. http://www.bortzmeyer.org.

[28] Matthieu Bouthors. « NAC, Firewall 3.0 ? ». *MISC*, (66), mars-avril 2013.

[29] Isabelle Boydens. *Informatique, normes et temps*. Bruylant, Bruxelles, 1999.

[30] Philippe Breton. *La tribu informatique – Enquête sur une passion moderne*. Métailié, Paris, 1991.

[31] Christophe Brocas et Jean-Michel Farin. « De la sécurité d'une architecture DNS d'entreprise ». *MISC*, (23), Janvier-février 2006.

[32] Antoine Brugidou et Gilles Kahn. « Étude des solutions de filtrage des échanges de musique sur Internet dans le domaine du *peer-to-peer* ». 9 mars 2005. http://www.culture.gouv.fr/culture/actualites/rapports/filtrage/charte.pdf.

[33] Franck Cappello. « P2P : Développements récents et perspectives ». Dans *6e journées réseau JRES*, 2005. En ligne ici : http://2005.jres.org/slides/152.pdf.

[34] Centre d'Expertise de Réponse et de Traitement des Attaques informatiques (Cert-RENATER). 10 septembre 2006. http://www.renater.fr/spip.php?rubrique=19.

[35] Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA). « Site du CERTA ». 10 septembre 2006. http://www.certa.ssi.gouv.fr/.

[36] Centre d'Expertise Gouvernemental de Réponse et de Traitement des Attaques informatiques (CERTA). « Sécurité des réseaux sans fil (Wi-Fi) ». 26 octobre 2004. http://www.certa.ssi.gouv.fr/site/CERTA-2002-REC-002/.

[37] D. Brent Chapman et Elizabeth D. Zwicky. *Firewalls – La sécurité sur l'Internet*. O'Reilly, Sebastopol, Californie (Paris pour la traduction), 2000. Traduction de Jean Zundel.

[38] Bill Claycomb et Alex Nicoll. « Insider Threats Related to Cloud Computing ». *CERT Insider Threat Blog*, août 2012. http://www.cert.org/blogs/insider_threat/2012/08/title_insider_threats_related_to_cloud_computing--installment_3_insiders_who_exploit_cloud_vulnerabi.html.

[39] Société ClearSy. « Atelier B ». juin 2004. http://www.clearsy.com/nos-outils/atelier-b/.

[40] Commission Nationale Informatique et Libertés. « Norme simplifiée n° 46 ». 13 janvier 2005. http://www.cnil.fr/en-savoir-plus/deliberations/deliberation/delib/169/.

[41] Computer Emergency Response Team - Coordination center. « Site du Cert-CC ». 10 septembre 2006. http://www.cert.org/.

[42] Computer Emergency Response Team - Industrie, Services et Tertiaire (Cert-IST). « Site du Cert-IST ». 10 septembre 2006. http://www.cert-ist.com/.

[43] François Contat, Guillaume Valadon, Stéphane Bortzmeyer, Samia M'timet, et Mohsen Souissi. « Résilience de l'Internet français 2011 : état des lieux ». juin 2012. http://www.ssi.gouv.fr/IMG/pdf/rapport-obs-20120620.pdf.

[44] Thomas Cormen, Charles Leiserson, Ronald Rivest, et Clifford Stein. *Introduction à l'algorithmique*. Dunod (pour la traduction française), Paris, 2002. NDA : une somme d'une complétude impressionnante ; si les exposés mathématiques des algorithmes sont d'une grande clarté, le passage à la programmation (en pseudo-code) est souvent difficile.

[45] Alan Cox et Edd Dumbill. « The Next 50 Years of Computer Security : An Interview with Alan Cox ». *O'Reilly Network*, Mars 2009. http://www.oreillynet.com/pub/a/network/2005/09/12/alan-cox.html.

[46] CROCUS (COLLECTIF). *Systèmes d'exploitation des ordinateurs*. Dunod, Paris, 1975. NDA : ce manuel, quoique assez ancien, conserve un intérêt certain par sa rigueur dans l'introduction des concepts et du vocabulaire, et en a acquis un nouveau, de caractère historique, par la description de systèmes aujourd'hui disparus.

[47] Cunningham et Cunningham. « Cee Language and Buffer Overflows ». *Cunningham and Cunningham, Inc.*, Mars 2010. http://c2.com/cgi/wiki?CeeLanguageAndBufferOverflows.

[48] Dr. M.A.C. Dekker. « Critical Cloud Computing - A CIIP perspective on cloud computing services ». *Site de l'ENISA*, décembre 2012. http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing.

[49] Fabrice Desclaux. « Skype uncovered – Security study of Skype ». *OSSIR – Groupe sécurité Windows*, 7 novembre 2005. http://www.ossir.org/windows/supports/2005/2005-11-07/EADS-CCR_Fabrice_Skype.pdf.

[50] Whitfield Diffie et Martin E. Hellman. « New Directions in Cryptography ». *IEEE Transactions on Information Theory*, vol. IT-22, nov. 1976. http://www.cs.tau.ac.il/~bchor/diffie-hellman.pdf.

[51] Edsger Wybe Dijkstra. « The Structure of the THE-Multiprogramming System ». *Communications of the ACM (CACM)*, 11(5), Mai 1968. http://www.cs.virginia.edu/~zaher/classes/CS656/p341-dijkstra.pdf.

[52] Cory Doctorow. « What I wish Tim Berners-Lee understood about DRM ». 12 mars 2013. http://www.guardian.co.uk/technology/blog/2013/mar/12/tim-berners-lee-drm-cory-doctorow.

[53] Gilles Dubertret. *Initiation à la cryptographie*. Vuibert, Paris, 2002.

[54] Albert Ducrocq et André Warusfel. *Les mathématiques – Plaisir et nécessité*. Vuibert, Paris, 2000. NDA : plaidoyer pour une discipline malmenée, au moyen de nombreux exemples historiques et modernes auxquels l'érudition des auteurs et leur talent de vulgarisateurs confèrent un rythme trépidant et passionnant.

[55] Jean-Pierre Dupuy. *Pour un catastrophisme éclairé – Quand l'impossible est certain*. Éditions du Seuil, Paris, 2002.

[56] Kjeld Borch Egevang et Paul Francis. « RFC 1631 – The IP Network Address Translator (NAT) ». Mai 1994. http://www.ietf.org/rfc/rfc1631.txt.

[57] Carl Ellison et Bruce Schneier. « Ten Risks of PKI : What You're Not Being Told About Public Key Infrastructure ». *Computer Security Journal*, vol. 16, nº 1, 2000. http://www.schneier.com/paper-pki.html.

[58] ENSTIMAC. « Sécurité de Perl ». *Site Perl de l'ENSTIMAC*, 23 mars 2006. http://perl.enstimac.fr/DocFr/perlsec.html.

[59] Yves Eudes. « Hackers d'État ». *Le Monde*, février 2013. http://www.lemonde.fr/technologies/article/2013/02/19/hackers-d-etat_1834943_651865.html.

[60] Société européenne de l'Internet. « Le nouveau DNS chinois ». *TIC & Développement*, novembre 2009.

[61] David Evans. « What Biology Can (and Can't) Teach Us About Security ». *USENIX Security Symposium*, Octobre 2008. http://www.cs.virginia.edu/~evans/usenix04/usenix.pdf.

[62] Karen Evans et Franklin Reeder. « A Human Capital Crisis in Cybersecurity : Technical Proficiency Matters ». novembre 2010. http://csis.org/publication/prepublication-a-human-capital-crisis-in-cybersecurity.

[63] James P. Farwell et Rafal Rohozinski. « Stuxnet and the Future of Cyber War ». 53(1), février-mars 2011. http://www.informaworld.com/smpp/title~content=t713659919.

[64] Edward W. Felten. « DRM and Public Policy ». *Communications of the ACM (CACM)*, (vol. 48, nº 7), juillet 2005. http://www.csl.sri.com/users/neumann/insiderisks05.html.

[65] Alexandre Fernandez-Toro. *Management de la sécurité du système d'information : Implémentation ISO 27001*. Eyrolles, Paris, 2007.

[66] Richard P. Feynman. « Personal observations on the reliability of the Shuttle ». 1986. http://science.ksc.nasa.gov/shuttle/missions/51-l/docs/rogers-commission/Appendix-F.txt.

[67] Éric Filiol. *Les virus informatiques : théorie, pratique et applications*. Collection IRIS. Springer Verlag, Paris, 2003.

[68] Éric Filiol. « Le danger des virus blindés ». *La lettre – Techniques de l'ingénieur – Sécurité des systèmes d'information*, (6), novembre-décembre 2005.

[69] Éric Filiol. « Évaluation des logiciels antiviraux : quand le marketing s'oppose à la technique ». *MISC*, (21), Octobre 2005. Dans un excellent numéro consacré aux *Limites de la sécurité*.

[70] Nicolas Fischbach. « Sécurité de la VoIP chez un opérateur ». 2006. http://www.ossir.org/jssi/jssi2006/supports/1B.pdf.

[71] Gustave Flaubert. *Bouvard et Pécuchet*. Le Seuil, Paris, 1857. NDA : comme il s'agit, en fin de compte, d'un livre sur la bêtise, sa lecture sera utile à quiconque se préoccupe de sécurité, puisque souvent les failles de sécurité ne sont pas sans lien avec la bêtise.

[72] Laurence Freyt-Caffin. « L'administrateur réseau, un voltigeur sans filet ». Dans *5e journées réseau JRES*, 2003. En ligne ici : http://2003.jres.org/actes/paper.130.pdf.

[73] Simson Garfinkel. *PGP* – Pretty Good Privacy. O'Reilly, Sebastopol, Californie (Paris), 1995. Traduction de Nat Makarévitch.

[74] Simson Garfinkel et Abhi Shelat. « MIT researchers uncover mountains of private data on discarded computers ». *Massachusetts Institute of Technology, News Office*, 15 janvier 2003. http://web.mit.edu/newsoffice/2003/diskdrives.html.

[75] Simson L. Garfinkel. « VoIP and Skype Security ». *Tactical Technology Collective*, Mars 2005. http://www.tacticaltech.org/files/tacticaltech/Skype_Security.pdf.

[76] Solveig Godeluck. *La géopolitique d'Internet*. La Découverte, Paris, 2002. 247 pages.

[77] Fernando Gont. décembre 2011. http://tools.ietf.org/html/draft-gont-6man-stable-privacy-addresses-00.

[78] Fernando Gont. « Results of a Security Assessment of the Internet Protocol version 6 (IPv6) ». septembre 2011. http://www.si6networks.com/presentations/hacklu2011/fgont-hacklu2011-ip-security.pdf.

[79] Fernando Gont. « Recent Advances in IPv6 Security ». avril 2012. http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-fgont-recent-advances-in-ipv6-security.pdf.

[80] Peter Gutmann. *Engineering Security*. University of Auckland, Auckland, Nouvelle-Zélande, 2011. Texte intégral disponible en ligne ici : http://www.cs.auckland.ac.nz/~pgut001/pubs/book.pdf.

[81] José Luis Gómez-Barroso et Claudio Feijóo. « Asymmetries and Shortages of the Network Neutrality Principle ». *CACM*, 54(4) :36–37, Avril 2011.

[82] Katie Hafner et Matthew Lyon. *Where Wizards Stay Up Late – The Origins of the Internet*. Pocket Books, Londres, 1996.

[83] John L. Hennessy et David A. Patterson. *Computer Architecture : a Quantitative Approach*. Morgan Kaufman Publishers (Vuibert pour la traduction française), San Mateo, Calif., USA, 2006. NDA : ce livre donne à la description de l'architecture des ordinateurs une ampleur intellectuelle que peu soupçonnaient. En annexe, une bonne introduction à la représentation des nombres (norme IEEE 754 notamment). La traduction française est recommandable.

[84] Andrew Hodges. *Alan Turing : the Enigma (Alan Turing : l'Énigme de l'intelligence)*. Simon and Schuster (Payot, Paris pour la traduction), New-York, USA, 1983.

[85] Michael Howard et David LeBlanc. *Écrire du code sécurisé*. Microsoft, Redmond, USA, 2003. Traduction de Marc Israël.

[86] G. Dan Hutcheson. « The World Has Changed ». *VLSI Research*, 13 avril 2005. https://www.vlsiresearch.com/public/600203v1.0.pdf.

[87] ISO/IEC. « Information technology – Systems Security Engineering – Capability Maturity Model (SSE-CMM) ». (21827), 2002.

[88] ISO/IEC. « Lignes directrices pour l'audit des systèmes de management de la qualité et/ou de management environnemental ». (19011), 2002.

[89] ISO/IEC. « Common Criteria for Information Technology Security Evaluation ». (15408), 2005.

[90] ISO/IEC. « Information Security Management Systems – Requirements ». (27001), 2005.

[91] ISO/IEC. « Information technology. Code of practice for information security management ». (17799), 2005.

[92] Saad Kadhi. « Le nuage Dropbox vu de la terre ferme ». *MISC*, (60), mars-avril 2011.

[93] Saad Kadhi. « À l'abord de Box ». *MISC*, (64), novembre-décembre 2012.

[94] Poul-Henning Kamp. « The Most Expensive One-byte Mistake ». *ACM Queue*, 9(7), juillet 2011. http://queue.acm.org/detail.cfm?id=2010365.

[95] Josh Karlin, Stephanie Forrest, et Jennifer Rexford. « Nation-State Routing : Censorship, Wiretapping, and BGP ». mars 2009. http://arxiv.org/abs/0903.3218.

[96] Kevin Krewell. « A Look Ahead To 2006 ». *Microprocessor Article*, vol. 20 nº 1, janvier 2006. La revue mensuelle avec édition hebdomadaire sur le Web du microprocesseur et de ses évolutions techniques et industrielles. Informée, compétente, beaucoup de détail technique exposé avec clarté : http://www.mpronline.com/mpr/index.html.

[97] Benjamin A. Kuperman, Carla E. Brodley, Hilmi Ozdoganoglu, T.N. Vijaykumar, et Ankit Jalote. « Detection and Prevention of Stack Buffer Overflow Attacks ». *Communications of the ACM (CACM)*, vol. 48 nº 11, novembre 2005.

[98] Augustin Landier et David Thesmar. « Action publique et intelligence collective ». *Commentaire*, 33(131) :713–719, 2010.

[99] James R. Langevin, Michael T. McCaul, Scott Charney, Lt. General Harry Raduege, et James A. Lewis. « Cybersecurity Two Years Later ». janvier 2011. http://csis.org/publication/cybersecurity-two-years-later.

[100] Sophie Le Pallec. « La convergence des identifiants numériques ». Dans *Actes du congrès JRES*, 2005. http://2005.jres.org/slides/70.pdf.

[101] Legalis.net. « Legalis.net ». 2 août 2006. http://www.legalis.net.

[102] Lawrence Lessig. *The future of ideas – The fate of the commons in a connected world*. Random House, New York, 2001. 352 pages.

[103] Steven Levy. *Hackers : Heroes of the Computer Revolution*. Doubleday, USA, 1984.

[104] Cédric Llorens, Laurent Levier, et Denis Valois. *Tableaux de bord de la sécurité réseau*. Eyrolles, Paris, 2006.

[105] Robert Longeon et Jean-Luc Archimbaud. *Guide de la sécurité des systèmes d'information – à l'usage des directeurs*. Centre National de la Recherche Scientifique (CNRS), Paris, 1999.

[106] Michael W. Lucas. *PGP & GPG - Assurer la confidentialité de ses e-mails et de ses fichiers*. Eyrolles (traduit par Daniel Garance), Paris, 2006.

[107] Fabrice Mattatia. *Traitement des données personnelles : le guide juridique*. Eyrolles, Paris, 2013.

[108] Alfred J. Menezes, Paul C. van Oorschot, et Scott A. Vanstone. *Handbook of Applied Cryptography*. CRC Press, Boca Raton, Floride, États-Unis, 1997. Une introduction complète au sujet, disponible en consultation sur le Web : http://www.cacr.math.uwaterloo.ca/hac/.

[109] MISC. « MISC ». *MISC*, 2005. Revue francophone de sécurité informatique : http://www.miscmag.com.

[110] Multicians. « Multics ». 2006. http://www.multicians.org/.

[111] Stéphane Natkin. *Les protocoles de Sécurité d'Internet*. Dunod, Paris, 2002.

[112] Stephen Northcutt et Judy Novak. *Détection d'intrusion de réseau*. Vuibert, Paris, 2002 (2004 pour la traduction). Traduction de Raymond Debonne.

[113] Michael J. O'Donnell. « Separate Handles from Names on the Internet ». *Communications of the ACM*, 48(12) :79–83, Décembre 2005.

[114] Ossir. « Site de l'OSSIR ». *Observatoire de la sécurité des systèmes d'information et des réseaux*, 2005. NDA : cette association est aujourd'hui le meilleur cénacle francophone dans son domaine. http://www.ossir.org.

[115] Loïc Pasquiet. « Déploiement d'une solution de téléphonie sur IP dans un campus ». 2006. http://www.ossir.org/jssi/jssi2006/supports/2A.pdf.

[116] Rob Pegoraro. « Tim Berners-Lee : The Web needs to stay open, but DRM is fine by me ». 10 mars 2013. http://boingboing.net/2013/03/10/tim-berners-lee-the-web-needs.html.

[117] Jacky Pierson et Robert Longeon. « La biométrie (suite) ». *Sécurité Informatique*, Avril 2004. Suite de l'article du bulletin de sécurité informatique du CNRS qui expose clairement les limites de la biométrie : http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num48.pdf.

[118] Kenneth D. Pimple. « Surrounded by Machines ». *CACM*, 54(3) :29–31, Mars 2011.

[119] W. Curtis Preston. *Using SANs and NAS*. O'Reilly, Sebastopol, California, 2002.

[120] Fabien Périgaud. *Conficker.C : de peer en peer !* CERT Lexsi, Paris, 2009. http://www.lexsi-leblog.fr/cert/confickerc-peer-en-peer.html.

[121] Fabien Périgaud. *Conficker.C : la réponse du berger à la bergère*. CERT Lexsi, Paris, 2009. http://www.lexsi-leblog.fr/cert/confickerc-la-reponse-du-berger-a-la-bergere.html.

[122] Christian Queinnec. « Le filtrage : une application de (et pour) Lisp ». 1995. http://pagesperso-systeme.lip6.fr/Christian.Queinnec/Books/LeFiltrage.ps.gz.

[123] Marcus J. Ranum. « The Six Dumbest Ideas in Computer Security ». *Site de Marcus J. Ranum*, Mars 2009. http://www.ranum.com/security/computer_security/editorials/dumb/.

[124] Marcus J. Ranum. « What is *Deep Inspection ?* ». *Site de Marcus J. Ranum*, Mars 2009. http://www.ranum.com/security/computer_security/editorials/deepinspect/.

[125] Yakov Rekhter, Robert G. Moskowitz, Daniel Karrenberg, Geert Jan de Groot, et Eliot Lear. « RFC 1918 – Address Allocation for Private Internets ». Février 1996. Cette RFC remplace les 1597 et 1627 de 1994 ; http://www.ietf.org/rfc/rfc1918.txt.

[126] Ronald Rivest, Adi Shamir, et Leonard Adleman. « A Method for Obtaining Digital Signatures and Public-Key Cryptosystems ». *CACM*, 21(2), Février 1978. L'article fondateur, accessible en ligne ici : http://people.csail.mit.edu/rivest/Rsapaper.pdf.

[127] Michel Rocard. « Vers une société de la connaissance ouverte ». 5 avril 2007. http://www.starinux.org/rapport-libre-rocard.pdf.

[128] J. Rosenberg, R. Mahy, P. Matthews, et D. Wing. « RFC 5389 – Session Traversal Utilities for NAT (STUN) ». Octobre 2008. http://www.ietf.org/rfc/rfc5389.txt.

[129] Mark E. Russinovich. « Sony, Rootkits and Digital Rights Management Gone Too Far ». *Sysinternals*, Octobre 2005. http://blogs.technet.com/b/markrussinovich/archive/2005/10/31/sony-rootkits-and-digital-rights-management-gone-too-far.aspx.

[130] Mark E. Russinovich. *Windows Internals : Windows 2000, Windows XP & Windows Server 2003*. Microsoft Press, Redmond, État de Washington, 2005.

[131] Emmanuel Saint-James. *La Programmation applicative (de Lisp à la machine en passant par le λ-calcul)*. Hermès, Paris, 1993. NDA : avec une préface de Jacques Arsac. Une étude riche et originale avec des aperçus saisissants sur la programmation.

[132] Kavé Salamatian. « Internet et la réinvention de la géographie ». *Nouvelle Revue de Géopolitique*, janvier 2013. http://kave.salamatian.org/wordpress/?p=6.

[133] Kavé Salamatian. « Internet Science : a Manifesto ». *Blog de Kavé Salamatian*, janvier 2013. http://kave.salamatian.org/wordpress/?p=10.

[134] Olivier Salaün. « Introduction aux architectures Web de *Single-Sign On* ». 2003. http://2003.jres.org/actes/paper.116.pdf.

[135] Cliff Saran. « BP turns its back on traditional IT security with Internet access to company systems ». *Computer Weekly*, 3 septembre 2004.

[136] Hervé Schauer. « VoIP et sécurité – Retour d'expérience d'audits de sécurité ». 2006. http://www.hsc.fr/ressources/presentations/tenor06-voip-sec/.

[137] Hervé Schauer. « Site d'Hervé Schauer Consultants ». *Hervé Schauer Consultants*, Février 2008. http://www.hsc.fr/index.html.fr.

[138] Hervé Schauer. « Le marché de la sécurité ». *FIC 2013*, février 2013. http://www.dailymotion.com/video/xx55nb_le-marche-de-la-securite_tech#.USTmLn2sNQI.

[139] Bruce Schneier. « The Internet is a surveillance state ». 16 mars 2013. http://us.cnn.com/2013/03/16/opinion/schneier-internet-surveillance.

[140] Security Focus. « Security Focus ». Février 2009. http://www.securityfocus.com/.

[141] Avi Silberschatz, Peter Galvin, et Greg Gagne. *Principes appliqués des systèmes d'exploitation*. Vuibert (pour la traduction française), Paris, 2001.

[142] Simon Singh. *The Code Book (Histoire des codes secrets)*. J.-C. Lattès (pour la traduction française), Paris, 1999. Un ouvrage de vulgarisation passionnant.

[143] Sophos. « Rapport 2013 sur les menaces de sécurité ». 2013. http://www.sophos.com/fr-fr/security-news-trends/reports/security-threat-report.aspx.

[144] Pyda Srisuresh et Kjeld Borch Egevang. « RFC 3022 – Traditional IP Network Address Translator (Traditional NAT) ». Janvier 2001. http://www.ietf.org/rfc/rfc3022.txt.

[145] Richard M. Stallman. « Pouvez-vous faire confiance à votre ordinateur ? ». *Logiciel libre, société libre : articles choisis de Richard M. Stallman*, 2002. http://www.gnu.org/philosophy/can-you-trust.fr.html.

[146] Ross Stapleton-Gray et William Woodcock. « National Internet Defense – Small States on the Skirmish Line ». *CACM*, 54(3) :50–55, Mars 2011.

[147] Symantec. « W32 :Stuxnet ». *Symantec.com*, juillet 2010. http://www.symantec.com/security_response/writeup.jsp?docid=2010-071400-3123-99.

[148] Michael Szydlo. « SHA-1 Collisions can be Found in 2^{63} Operations ». *RSA Laboratories*, Janvier 2011. http://www.rsasecurity.com/rsalabs/node.asp?id=2927.

[149] Andrew S. Tanenbaum. *Réseaux*. Pearson Education (pour la traduction française), Paris, 2003.

[150] Eneken Tikk, Kadri Kaska, et Liis Vihul. *International Cyber Incidents : Legal Considerations*. NATO Cooperative Cyber Defence Centre of Excellence, Tallinn, Estonie, 2011. http://www.ccdcoe.org/231.html.

[151] Isabelle N. Tisserand. *Hacking à cœur – Les enfants du numérique*. Éditions e/dite, Paris, 2002.

[152] Roland Topor. *Le sacré livre de Prouto*. Syros, Paris, 1990.

[153] Daniel Ventre. « Guerre de l'information et cyberguerre : les deux Corées face à face ». *MISC*, (55) :62–71, mai-juin 2011.

[154] Daniel Ventre. « Stuxnet : interprétations ». *MISC*, (53) :53–63, janvier-février 2011.

[155] Vernor Vinge. *True Names*. Tor Books, USA, 1981.

[156] Michel Volle. *e-conomie*. Economica, Paris, 2000. Une analyse économique informée et pénétrante des nouvelles technologies par un maître de l'économétrie et de la statistique, disponible en ligne ici : http://www.volle.com/ouvrages/e-conomie/table.htm.

[157] Michel Volle. *De l'informatique*. Economica, Paris, 2006.

[158] Michel Volle. « Histoire d'un *datawarehouse* ». Février 2009. http://www.volle.com/travaux/dwh.htm.

[159] Michel Volle. « Histoire d'un tableau de bord ». Février 2009. http://www.volle.com/travaux/tdb.htm.

[160] Xiaoyun Wang, Andrew Yao, et Frances Yao. « New Collision search for SHA-1 ». Dans *Crypto'05*, 2005.

[161] Xiaoyun Wang, Yiqun Lisa Yin, et Hongbo Yu. « Finding Collisions in the Full SHA-1 ». Dans *Advances in Cryptology – Crypto'05*, 2005. http://people.csail.mit.edu/yiqun/SHA1AttackProceedingVersion.pdf.

[162] Pierre Wassef. *Arithmétique - Application aux codes correcteurs et à la cryptographie*. Vuibert, Paris, 2008. 218 p – ISBN 978-2-7117-2083-5.

[163] Gerald M. Weinberg. *The Psychology of Computer Programming*. Van Nostrand Reinhold, New York, 1971.

[164] Wikipédia. « Débordement de tampon ». *Wikipédia*, Janvier 2011. http://fr.wikipedia.org/wiki/Buffer_overflow.

[165] Wikipédia. « Network address translation ». *Wikipédia*, Janvier 2011. http://fr.wikipedia.org/wiki/NAT.

[166] Wikipédia. « Pair à pair ». *Wikipédia*, Janvier 2011. http://fr.wikipedia.org/wiki/P2p.

[167] Wikipédia. « SHA-1 ». *Wikipédia*, Janvier 2011. http://fr.wikipedia.org/wiki/SHA-1.

[168] Wikipédia. « SHA-2 ». *Wikipédia*, Avril 2011. http://en.wikipedia.org/wiki/SHA-2.

[169] Philippe Wolf. « De l'authentification biométrique ». *Sécurité Informatique*, octobre 2003. NDA : cet article du bulletin de sécurité informatique du CNRS expose clairement les limites de la biométrie : http://www.sg.cnrs.fr/FSD/securite-systemes/revues-pdf/num46.pdf.