Sécurité informatique

3e édition

Principes et méthodes

Laurent Bloch

Christophe Wolfhugel

Préfaces de Christian Queinnec et d'Hervé Schauer

Avec la contribution de Nat Makarévitch

 ISBN : 978-2-212-13233-5

EYROLLES

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 par exemple le livre de Michel Volle *e-conomie* [140], disponible en ligne, qui explique comment pour une entreprise comme Air-France le SI, 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 différence 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.

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 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 17).

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 démultiplié 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 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 pieds 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, et, 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 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 les sites négationnistes étaient installés aux États-Unis, pays dépourvu d'une législation anti-négationniste, ce qui interdisait 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 ceux-ci n'en pouvaient mais. En effet, ainsi que nous le verrons à la page 266, 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.

Cette question du filtrage de contenu est traitée par le rapport Kahn-Brugidou [29] ; le site `www.legalis.net` [86] 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 [68] et de Lawrence Lessig [87] 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 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 42 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 (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 peut capter (enfin, pas si facilement que cela, heureusement), il est possible à un tiers de la détourner. 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 54), authentifier sans chiffrer laisse la porte ouverte au vol de données.

Empêcher les intrusions

Mais 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 262. La surenchère suivante proclame que si l'on a détecté une intrusion, autant la stopper, et les IDS sont 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 18 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 2011) 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 [11] 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 les comportements sont inadaptés, toutes les mesures techniques seront parfaitement vaines parce que contournées.

Abandonner les utilisateurs inexpérimentés aux requins ?

Un article récent de Marcus J. Ranum [107] (cf. page 256), qui n'est rien moins que l'inventeur du pare-feu et une autorité mondiale du domaine SSI, soutient l'idée paradoxale qu'il serait inutile, voire nuisible, d'éduquer les utilisateurs du SI à la sé-

curité : 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 [136], naufragé reçu comme dieu vivant d'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 spécialisés 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, les phénomènes les plus dangereux ne manqueront pas de proliférer, et de ce moment surgiront les incidents les plus graves.

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 ap-

pliquer 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* [117] 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 clients, 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.

Une machine virtuelle par 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 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 Research Projects Agency)* consécutive à la propagation du ver de Morris, la première attaque, involontaire[1] mais de grande envergure, contre l'Internet. En 2011, 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, le CERT-IST[4] qui s'adresse au monde industriel. En fait,

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/`

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), organisme placé auprès du Premier ministre, dirigée par Patrick Pailloux et rattaché au Secrétariat général de la défense et de la sécurité nationale (SGDN), 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 ceux-ci (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 un 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 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.

5. http://www.cert.org/
6. http://www.ssi.gouv.fr/index.html

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. 297) 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 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

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.*

La présente section sur le management de la sécurité présente des normes et des méthodes que nous n'approuvons pas ; elles ne sont pas inutiles, mais nuisibles. 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.

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*. C'est l'essor de la demande d'audits qui 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 2011) quatre 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 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 [79] 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* » [80], 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)[7], 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. »

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 ;
- 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.

7. http://www.ssi.gouv.fr/fr/confiance/ebiospresentation.html

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[8]. Nous recommandons aussi la lecture du livre qu'Alexandre Fernadez-Toro a consacré au sujet, *Management de la sécurité du système d'information : Implémentation ISO 27001* [57].

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 [76] propose un « Modèle de maturité de capacité » : qui peut traduire ce jargon invraisemblable ?

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

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 est d'une ampleur propre à absorber une énergie considérable, or une fois que l'on connaît par cœur les critères communs et que l'on sait appliquer EBIOS les pieds au mur, on n'a pas mis en place une seule mesure concrète de SSI, on est seulement 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 pour se plier à un tel exercice :

- l'entreprise est dans un environnement qui 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 30), 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, les autres sont encore plus pénibles !

Ce qui frappe le lecteur de ces normes, c'est que la vérification formelle de conformité à leur texte peut presque 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 je tairai 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. Si j'osais, je serais d'accord avec eux, mais je suis trop respectueux des normes et des autorités pour cela. En fait, 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 les grands nigauds nommés Aristote, Descartes, Newton, Kant et Einstein n'y ont pas pensé, ils se seraient épargné bien de la fatigue cérébrale.

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 [26] 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, c'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 [9].

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 est antinomique de toute politique réelle de sécurité. Leur fonction principale ne serait-elle pas de donner du travail aux cabinets de consultants spécialisés, à condition que leur clientèle soit (très) solvable ?

Un projet de certification de sécurité Open Source : OSSTMM

L'*Institute for Security and Open Methodologies* (ISECOM) [10], 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*

9. Le lecteur pourra aussi se reporter avec profit au livre bénéfiquement concis de Scott Barman, *Writing Information Security Policies* [12].

10. `http://www.isecom.org/`

Methodology Manual (OSSTMM)[11]. Ce manuel, disponible librement en ligne, propose donc une méthodologie de vérification de la sûreté des systèmes.

La fonction d'un référentiel, c'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.

D'autre part, 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 partenaires, 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

11. http://www.isecom.org/osstmm/

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 de ces aspects simplement humains : ce sont de certains d'entre eux qu'il sera question ici. 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 bien sûr 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, afin que 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 revendu à temps leurs stock-options pour se retirer sur leur yacht aux îles Cayman... 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, c'est la prolifération des systèmes de contrôle et d'audit que nous avons évoqués à la page 21, 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 2011 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 » [83] 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 [75] 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 XIV^e^ siècle (cf. mon livre [18], ou sur le Web [19]).

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 [48], qui jettent une lumière vive aussi bien sur toutes ces normes relatives aux systèmes de management que sur la mode récente du principe de précaution.

Pour décrire ces systèmes de pensée, Dupuy introduit la notion de « rationalité procédurale », qui procéderait 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 [18], donnent à penser que c'est bien au renoncement 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[12], 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 totalement, que ce soit dans l'entreprise ou dans l'usage privé des ordinateurs et des réseaux.

12. 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.

Richard Feynman à propos de la conduite de projet

Un des derniers écrits du physicien Richard P. Feynman, prix Nobel 1965, fut une annexe [58] 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.