LE RISQUE INFORMATIQUE : UNE COMPLEXITÉ CROISSANTE

PATRICE GUICHARD *

Depuis quelques années, la sécurité des systèmes d'information a connu une évolution spectaculaire, étroitement liée à la dynamique d'informatisation des gouvernements et des entreprises. La complexité croissante des systèmes, les coûts de plus en plus élevés des équipements et des logiciels, ainsi que l'élargissement des domaines d'application font que l'informatique est devenue un élément stratégique pour les entreprises, et toute destruction ou altération de leurs données peut compromettre leur compétitivité, leur image et occasionner des pertes souvent élevées. Fin 2004, ces pertes représentaient environ 16,7 Md$, contre 3,3 Md$ en 1997 (Computer Economics, 2004).

Cependant, bien que de plus en plus d'entreprises prennent conscience de ces risques et investissent de plus en plus en personnel et en moyens pour en limiter les conséquences, ce phénomène demeure mal connu et peu maîtrisé par leurs dirigeants.

Il y a encore peu de temps, les efforts des responsables informatiques ou des responsables sécurité se concentraient principalement sur la sécurisation du périmètre autour de leur réseau interne. Et il était finalement rassurant pour eux de disposer d'une image convenue de la menace, celle d'un adolescent génial dont les « bidouilles » informatiques faisaient courir un léger frisson d'angoisse dans les services informatiques, souvent relayé par une presse à sensation tout acquise.

* Docteur en informatique, Directeur R&D, Safe-Protect.

Face à cette menace « externe », la sécurité était donc implémentée en des points de contrôle facilement identifiables qui filtraient les flux passant entre le réseau interne (LAN) et le réseau externe (Internet), grâce à l'implémentation de logiciels ou matériels communément appelés « pare-feu » ou *firewall*.

L'avantage de cette démarche sécuritaire, que nous pourrions qualifier dorénavant de « démarche de base », résidait dans le fait que son administration était facilitée par la centralisation des contrôles entre ces zones ; en complément des « pare-feu » censés filtrer les accès illicites venant de l'extérieur, des logiciels antivirus, et des logiciels de filtrage d'URLs étaient également déployés en entrée-sortie du réseau de confiance.

Cependant, malgré tous ces investissements et une prise de conscience des différents responsables pour sécuriser leur système d'information, le nombre d'attaques n'a cessé d'augmenter. Pour ne citer que quelques exemples, le CERT (Computer Emergency Response Team), organisme incontournable en matière de sécurité sur Internet, qui comptabilisait 2 340 incidents en 1994, dénombrait 137 529 incidents pour la seule année 2003 avec une progression de 67 % par rapport à 2002. Le nombre de failles publié est lui aussi en forte augmentation, passant de 171 failles publiées en 1994, pour culminer, au troisième trimestre 2005, à plus de 4 268 failles, soit une moyenne hebdomadaire de 82 failles (sans compter celles qui ne sont volontairement pas publiées par les pirates, ceci leur garantissant toujours une avance dans le domaine de l'intrusion des systèmes d'information).

Malheureusement, l'évaluation de ces attaques n'est pas toujours bien mesurée. Un constat récent (qui était déjà sorti en France en 2004 via une étude du Clusif) montrait que 30 % des managers IT ne pouvaient chiffrer le nombre d'attaques dont ils avaient été la cible. Plus grave encore, que 22 % d'entre eux affirmaient ne pas être en mesure de donner une estimation du nombre de menaces ayant réussi à franchir les défenses de sécurité de leur entreprise.

Et, pour couronner le tout, même si les entreprises prennent des mesures pour se protéger, elles ne sont pas pour autant à l'abri. Les dernières statistiques dans ce domaine sont pour le moins surprenantes : actuellement 99 % des entreprises utilisent un logiciel antivirus mais 78 % d'entre elles ont quand même subi des préjudices liés aux virus, vers... (CSI/FBI Computer Crime and Security, 2004 ; Rapport sur la sécurité et la délinquance informatique).

Une autre étude portant sur trois millions d'ordinateurs professionnels a recensé 83 millions d'instances de logiciels espions *Spywares*. (Groupe Gartner, septembre 2004).

Le débat est donc ouvert : la mise en place de systèmes de sécurité ne serait-elle qu'un leurre ?

Heureusement tel n'est pas le cas. De nos jours, le « contexte » des entreprises est devenu plus complexe à sécuriser et la notion de périmètre beaucoup plus flou pour ne pas dire obsolète face à la multitude des moyens de communication et de connexion au réseau ainsi qu'à la mobilité des systèmes modernes mis à la disposition des utilisateurs.

Parallèlement à cette multiplicité des moyens de communication, les fonctionnalités applicatives ont, elles aussi, continué à se sophistiquer, tant pour l'entreprise que pour les systèmes personnels, ce qui expose d'autant plus les réseaux d'entreprises à des menaces qui étaient inconnues jusque-là. L'intégration directe des systèmes d'entreprise avec ceux de leurs partenaires (B to B) et de leurs clients (B to C) amène la définition et l'application de politiques de sécurité à un niveau de défi multidimensionnel.

Le simple concept d'origine de « périmètre », qui offrait l'avantage de centraliser l'application des règles de sécurité en un certain nombre de points de contrôle, s'est grandement complexifié ces dernières années.

Aux multiples systèmes d'exploitation « *open source* ou non » (dont des systèmes personnels qui sont en plein essor), s'est ajouté le développement d'une grande variété de plates-formes de traitement de l'information. Celles-ci vont des appareils portatifs PDA, aux téléphones portables, ordinateurs portables, bornes publiques, périphériques amovibles (type clé USB), baladeur MP3, disques dur externes... Les méthodes de connexion de ces systèmes à l'entreprise se sont également diversifiées. L'émergence de produits « réseau à large bande passante » a accru le niveau de sophistication des informations accessibles à l'utilisateur final et aux bureaux personnels, connexion qui, par le passé, était exclusivement réservée aux centres de calculs. Les réseaux privés virtuels (VPN), quant à eux, permettent dorénavant, même aux particuliers, d'avoir accès au cœur même de l'entreprise, et cela avec un niveau de performance qui ne se trouvait auparavant qu'au sein du réseau local (LAN) de l'entreprise.

Les technologies sans fil (WI-FI, Bluetooth, EDGE, 3G...) étendent cette disponibilité et accroissent la complexité de la gestion du réseau. Ces innovations technologiques permanentes, pourtant destinées à améliorer le confort des utilisateurs, rendent la tâche de sécurisation de plus en plus difficile et sont des facteurs d'accroissement des risques. Ainsi, les réseaux WI-FI qui utilisent les technologies sans fil, sont de véritables « passe-murailles » et s'ils permettent à l'entreprise de s'affranchir de câbles, donnent également la possibilité aux cybercriminels de s'affranchir des sécurités physiques (portes, murs, systèmes d'alarme) pour s'introduire insidieusement dans les ordinateurs même si ceux-ci

ne sont pas reliés à Internet. Rien que sur Paris, une récente étude de l'association Paris sans fil a ainsi démontré que plus de 40 % des réseaux WI-FI de la capitale ne disposaient d'aucune mesure préventive de sécurisation et étaient donc perméables à des intrusions externes.

De par ces développements techniques, les terminaisons réseau peuvent se retrouver partout. Le cœur du centre de données de l'entreprise peut ainsi être le point d'entrée d'environnements d'utilisateurs distants. Cette capacité de se connecter au réseau de confiance depuis n'importe quel lieu, à tout moment, a transformé le périmètre de sécurité traditionnel en le dotant de multiples dimensions qui n'existaient pas auparavant. Le travail de sécurisation de l'entreprise n'en est devenu que plus ardu.

De plus, la mise en conformité des systèmes d'information avec les dernières réglementations générales (Code de la propriété intellectuelle, CNIL, responsabilité juridique pour les dirigeants, responsables et cadres de l'organisation) ou plus spécifiques (Bâle II, Sarbane-Oxley, HIPAA...) est devenue un enjeu central pour certaines entreprises. Ceci a conduit à dépasser les limites traditionnelles pour attester de l'implémentation d'une politique efficiente de sécurité du réseau.

Le défi de la sécurité des entreprises ne se limite donc plus à une complexité technologique croissante.

Un nombre grandissant de décisions réglementaires implique dorénavant que l'entreprise se dote de moyens adaptés pour faire face à des besoins toujours plus nombreux pour contrôler étroitement son système d'information. Les sanctions encourues en cas de non conformité sont l'une des motivations principales des entreprises. Ainsi, les dirigeants, coupables de produire des certificats frauduleux de conformité sont, avec la Loi Sarbanes-Oxley, qui touche toutes les entreprises cotées aux États-Unis, passibles d'années d'emprisonnement et de plusieurs millions de dollars d'amendes. De même, le non respect de la confidentialité des informations de la Sécurité Sociale américaine imposée par la Loi Insurance Portability and Accountability Act (HIPAA) peut être sanctionné par des amendes à six chiffres chaque année. Si des lois comme Sarbanes-Oxley portent sur toutes les entreprises cotées, des règlements spécifiques à certains métiers ajoutent un fardeau disproportionné aux entreprises des secteurs concernés. Parmi ceux-ci, le secteur financier est sans doute le plus réglementé de tous. Dans son cas une seule non-conformité, peut déboucher sur plusieurs pénalités en application de lois qui s'interfèrent les unes avec les autres. Les systèmes d'information financiers sont ainsi devenus les environnements informatiques les plus sensibles aux réglementations.

Pour autant, les dirigeants des petites entreprises ne doivent pas se réjouir. Le simple fait de mettre à disposition de l'un de ses employés

un ordinateur, engage sa responsabilité. Pour ne citer que quelques exemples :
- un employé qui télécharge des images pédophiles grâce à l'ordinateur mis à sa disposition par l'entreprise peut se voir infliger, selon l'article 227-3 du Code pénal, une peine de trois ans de prison et 75 000 € d'amende et l'entreprise se voir reprocher des actes de complicité par fournitures de moyens. Et, sur le plan civil, c'est-à-dire sur le plan d'un éventuel dédommagement des victimes, l'article 1384 alinéa 5 du Code civil précise que : « les maîtres et les commettant [sont responsables] du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés » ;
- lorsqu'un employé télécharge des fichiers musicaux sans l'autorisation de leurs auteurs, celui-ci se rend coupable du délit de contrefaçon. Selon l'article L335-2 du Code de la propriété intellectuelle, ce téléchargement « illicite » est passible de peines maximales de trois ans d'emprisonnement et de 300 000 € d'amende (peines aggravées par la Loi Perben II). Le délit et les peines associées s'appliquent également à celui ou celle qui a mis le fichier en partage, c'est-à-dire celui qui a offert un fichier piraté au téléchargement des internautes, et cela vaut pour tous les types d'œuvres (vidéo, photo, logiciel...) ;
- dans le cas où une base de données client serait pillée par des tiers étrangers à l'entreprise, les responsables doivent prendre « toutes les précautions utiles », c'est-à-dire agir selon l'état de l'art dans le domaine de la sécurité sur le réseau. Cela implique, pour eux, de protéger ce type de contenus et de se doter de moyens adéquats. À défaut, l'employeur s'expose notamment aux peines prévues à l'article 226-22 du Code pénal punissant de cinq ans d'emprisonnement et de 300 000 € d'amende « le fait, par toute personne qui a recueilli, à l'occasion de leur enregistrement, de leur classement, de leur transmission ou d'une autre forme de traitement, des données à caractère personnel dont la divulgation aurait pour effet de porter atteinte à la considération de l'intéressé ou à l'intimité de sa vie privée, de porter, sans autorisation de l'intéressé, ces données à la connaissance d'un tiers qui n'a pas qualité pour les recevoir ». Ce délit étant non intentionnel, l'employeur pourrait être tenu responsable de l'imprudence ou de la négligence ayant permis la divulgation d'une donnée à caractère personnel, même à son insu (dans l'hypothèse d'une imprudence ou d'une négligence, les peines maximales étant ramenées à trois ans d'emprisonnement et 100 000 € d'amende) ;
- l'employé qui utilise des copies illicites de logiciels sur son poste de travail professionnel doit savoir que, aux termes de l'article L.122-4 du Code de la propriété intellectuelle, « toute représentation ou reproduction intégrale ou partielle [d'une œuvre de l'esprit donc d'un logiciel]

faite sans le consentement de l'auteur (...) est illicite ». La jurisprudence considère que l'entreprise qui a fourni les moyens techniques et technologiques de la copie est susceptible d'être tenue responsable pénalement.

La responsabilité juridique de l'employeur sera donc mise en jeu, par application de l'article 1384 alinéa 5 du Code civil qui dispose que « les maîtres et les commettants [sont responsables] du dommage causé par leurs domestiques et préposés dans les fonctions auxquelles ils les ont employés ».

Cette disposition signifie que tout fait commis par un employé dans l'exercice de ses fonctions et qui cause un dommage à autrui engage systématiquement la responsabilité civile de son employeur. L'employeur viendra, dans ces conditions, répondre civilement des fautes de son préposé d'autant que, d'une part, il sera souvent le propriétaire des ordinateurs ayant stocké la contrefaçon, d'autre part, c'est l'entreprise qui sera tenue responsable d'avoir profité directement de cette contrefaçon.

Heureusement, pour faire face à cette quantité étourdissante de défis en matière de sécurité et de mise en conformité des systèmes d'information, les éditeurs de logiciels de sécurité ont mis au point une quantité toute aussi impressionnante de solutions qui, malheureusement, peuvent s'avérer tout aussi complexes que les problèmes qu'elles sont censées résoudre. Selon les estimations de Enterprise Managment Associates Inc (EMA), il existerait actuellement plus de 2000 sociétés éditrices de logiciels spécialisés en sécurité informatique, qui chacune offre une ou plusieurs solutions dans divers domaines. Ce qui n'a fait qu'alourdir le fardeau des entreprises, qui doivent s'équiper, tant pour leur infrastructure, que pour leur personnel, avec la bonne panoplie de solutions et d'expertise pour répondre aux besoins. En l'absence d'outils capables de simplifier la définition d'une politique cohérente et applicable dans toute l'entreprise, les solutions informatiques elles-mêmes peuvent du fait de leur complexité générer des risques aussi importants que ceux qu'elles sont censées éliminer. Ce risque est aggravé par le fait que seulement 15 % des entreprises disposent de personnel formé à la sécurité (Clusif).

Les « pare-feu » et les antivirus actuels sont de plus en plus distribués, leur mode de fonctionnement s'est également sophistiqué et s'avère donc de plus en plus difficile à appréhender pour des non spécialistes en sécurité.

D'autre part, le mal est souvent là où on s'y attend le moins. Une récente étude menée par ICM Research démontre ainsi que le comportement de la plupart des utilisateurs crée une menace pour la sécurité informatique des entreprises à l'intérieur même de celle-ci.

Parmi les enseignements de ce sondage, on notera en particulier que :

- 21 % des utilisateurs laissent des membres de leur famille ou des amis utiliser leur ordinateur professionnel pour accéder à l'Internet ;
- 51 % connectent toutes sortes de périphériques personnels à leur ordinateur professionnel et un quart d'entre eux le font quotidiennement ;
- 60 % stockent sur le disque dur de leur ordinateur professionnel des données personnelles ;
- 10 % téléchargent des contenus illicites à partir de leur ordinateur professionnel ;
- 62 % admettent n'avoir qu'une connaissance très limitée des principes de sécurité informatique ;
- 52 % ne savent pas comment mettre à jour la protection antivirale de leur PC ;
- 5 % des personnes interrogées reconnaissent avoir accédé à des données confidentielles de l'entreprise sans y avoir été autorisés.

Dès lors, les questions sont les suivantes : que faire ; quelle politique de défense faut-il instaurer ?

Il n'est malheureusement pas possible de donner une solution globale permettant de relever tous ces défis. La seule certitude dans ce domaine est que ce sujet concerne tout le monde dans l'entreprise, les dirigeants aussi bien que les cadres et les employés, que ce soit dans le secteur privé ou public. La seule solution viable à mes yeux est celle qui consiste à protéger en profondeur le réseau interne. La mise en place de cette défense implique plusieurs technologies et une organisation qui relie ces technologies entre elles. Pour cela, le système d'information doit être protégé de l'intérieur en plusieurs endroits :

- il doit être protégé au cœur même du réseau ;
- il doit ensuite être protégé au niveau des routeurs/*switch* qui permettent l'acheminement des données ;
- le poste de travail utilisateur, doit être lui-même sécurisé et cela à plusieurs niveaux, au niveau des logiciels qui peuvent être utilisés par l'utilisateur, au niveau des flux et des protocoles lui servant à communiquer et au niveau des périphériques pouvant être installés ;
- enfin, il faut que les applicatifs et les accès distants, permis par le télétravail soient protégés et que la politique de sécurité de l'entreprise soit toujours activée même lorsque l'utilisateur est en dehors de son lieu de travail.

La notion de sécurité doit être présente au cœur même du système d'information de l'entreprise et si elle bien comprise et bien maîtrisée, l'entreprise retrouvera un niveau de sécurité optimal. En complément de toutes ces technologies, il serait peut-être judicieux d'obliger les entreprises connectées au réseau Internet à faire auditer trimestriellement leur système d'information par des sociétés

spécialisées préalablement certifiées par une Agence nationale de sécurité informatique. Pourquoi ne pas ouvrir en parallèle le débat avec les compagnies d'assurance et proposer une cotisation d'assurance proportionnelle au niveau de sécurité du système d'information de l'entreprise ? Le prix de notre compétitivité économique est peut-être à ce prix ...