L'insécurité informatique : un risque financier majeur

Patrice GUICHARD*
Olivier PASTRÉ**

Hackers, crackers, phreakers, spammers, coderz... : sous ces noms, majoritairement anglais et apparemment inoffensifs (et dont la liste s'allonge chaque année), se cache une réalité de plus en plus inquiétante : la criminalité informatique, ou cybercriminalité, qui se développe de plus en plus rapidement, sans pour cela être mieux comprise, avec des conséquences économiques et organisationnelles dans des domaines de plus en plus variés ; ce qui oblige tous les acteurs concernés par ce phénomène majeur à des questionnements de plus en plus complexes.

UN PHÉNOMÈNE MAJEUR, MAIS MÉCONNU

Quelles que soient les statistiques utilisées, et malgré une présomption très forte de sous-estimation (sur laquelle nous reviendrons), les chiffres de la cybercriminalité explosent véritablement. Pour ne prendre que deux exemples, Symantec, leader mondial du secteur (promoteur de l'antivirus Norton), a recensé dans le monde 1 276 nouvelles failles de sécurité au premier semestre 2004, soit environ 48 nouvelles failles de sécurité par semaine et plus de 4 096 nouveaux virus affectant les plates-formes Windows, nombre qui a été multiplié par 4,5 par rapport au premier semestre 2003, tandis que le CERT (Computer Emergency Response Team), organisme incontournable en matière de sécurité sur Internet, qui comptabilisait 2 340 incidents en 1994, en dénombre 137 529 pour la seule année 2003 avec une progression de + 67 % par rapport à 2002.

Autre « explosion », et c'est rassurant, celle de l'industrie de la sécurité

* Directeur général de Safe Protect.
** Professeur à l'université Paris VIII.

informatique. Une industrie qui croît chaque année, depuis 10 ans, avec un taux de croissance à deux chiffres et avec des perspectives ne laissant prévoir aucun ralentissement à court ou moyen terme. Pour ne prendre que l'Europe, la croissance estimée du marché de la sécurité informatique est ainsi attendue à + 26 % par an pour les cinq prochaines années et devrait atteindre 3,13 milliards de dollars en 2007[1]. Datamonitor, pour sa part, estime le marché mondial de la sécurité des systèmes d'information à 21,2 milliards de dollars en 2005.

Ces perspectives s'expliquent aisément. D'abord, parce que la criminalité progresse et nécessite donc des « gardes » plus relevées : une récente étude du Gartner Group indique que, d'ici à 2005, 70 % des PME gérant leur propre système de sécurité raccordé à Internet feront l'objet d'une attaque réussie, et (ce qui est plus inquiétant) que plus de 60 % d'entre elles ne réaliseront pas qu'elles ont été victimes d'une ou plusieurs attaques. Ensuite, parce que les acteurs concernés déjà sensibilisés prennent, chaque année, mieux conscience des risques que présente cette forme de délits : pour les entreprises françaises ayant déjà investi dans ce domaine, les anticipations d'augmentation des dépenses sur les deux années à venir sont ainsi de 30 % pour les PME et de 59 % pour les grandes entreprises. Enfin, parce que la sécurité informatique gagne chaque année de nouveaux terrains. Les PME (en particulier dans l'industrie) et les collectivités territoriales emboîtent progressivement le pas aux grandes entreprises (qui représentent encore plus de 50 % du marché, en particulier dans les services) et aux administrations centrales.

Sur le diagnostic, il n'y a donc pas « photo ». En apparence au moins, car ce qui frappe le plus lorsque l'on creuse le sujet, c'est la complexité et, plus grave, la méconnaissance générale du phénomène. Cette méconnaissance tient à trois principaux facteurs.

L'hétérogénéité du phénomène

Le terme générique d'*hackers*, souvent mal employé par les médias, recouvre des réalités très diverses. En termes de menaces, cela passe de l'espionnage d'un concurrent (menace de niveau 2 sur une échelle de 5, selon une récente enquête de Ernst et Young de 2003) au vol de brevet (2,3), à l'attaque d'un *hacker* amateur (3,7), à l'espionnage par des prestataires (2,9), au blocage d'un système par des requêtes (3,3), plus communément appelé « déni de service » (DOS) et, pour finir, par les virus et les vers (3,6), eux-mêmes, par nature, éminemment diversifiés. À un niveau plus général, on peut regrouper les multiples manifestations de la cybercriminalité selon la récente typologie de l'Organisation de coopération et de développement économiques (OCDE) qui distingue trois grandes familles de délits :

- l'entrée, l'altération, l'effacement ou la suppression de données et de programmes dans l'intention de commettre un transfert illégal de fonds, de commettre un faux, ou d'entraver le fonctionnement du système informatique et/ou de télécommunication ;
- la violation du droit exclusif du détenteur du programme informatique

protégé dans l'intention de l'exploiter commercialement et de le mettre sur le marché ;
- l'accès dans un système informatique, ou de télécom, ou l'interception d'un tel système, fait sciemment et sans l'autorisation du responsable.

Cette typologie, généralement reconnue aujourd'hui, a le mérite de mettre un peu d'ordre. Il n'est pas sûr toutefois qu'elle soit très opérationnelle et, surtout, qu'elle soit pérenne, compte tenu d'une caractéristique consubstantielle de la cybercriminalité, qui est l'évolutivité.

Le caractère évolutif des technologies

Dernière tendance pour l'année 2004, le *phishing* - concaténation du « ph » du jargon des *hackers* (contraction de *phone*) et de *fishing* qui veut dire « pêcher » - est une escroquerie par Internet qui consiste à lancer un filet, le plus souvent via l'envoi massif d'e-mails maquillés et la mise en place de faux sites Web (principalement bancaires), pour aller à la pêche aux données personnelles et financières (accès aux comptes bancaires, aux numéros de cartes de crédit...).

Ce phénomène, qui n'existait qu'à l'état embryonnaire il y a quelques mois, a fait à ce jour plus de 17 millions de victimes aux États-Unis et inquiète désormais tous les industriels de la sécurité. Mais le *phishing* n'est rien à côté des dangers véhiculés par la convergence observée des différentes techniques de piratage (SPAM + *phishing* + vers informatiques + chevaux de Troie), qui est de nature à démultiplier les risques.

D'autre part, les innovations technologiques permanentes, pourtant destinées à améliorer le confort des utilisateurs, rendent la tâche de sécurisation de plus en plus difficile et sont elles-mêmes des facteurs d'accroissement des risques. Ainsi, les réseaux *Wi-Fi*, qui utilisent les technologies sans fil, sont de véritables « passe-murailles » et permettent, certes, à l'entreprise de s'affranchir de câbles, mais donnent également la possibilité aux cybercriminels de s'affranchir des sécurités physiques (portes, murs, systèmes d'alarme) pour s'introduire insidieusement sur les ordinateurs et, qui plus est, même si ceux-ci ne sont pas reliés à Internet. Rien que sur Paris, une récente étude de l'association Paris sans fil a démontré que plus de 40 % des réseaux *Wi-Fi* de la capitale ne disposant d'aucune mesure préventive de sécurisation étaient perméables à des intrusions externes. Le Web a ainsi considérablement élargi l'espace de la cybercriminalité.

Le plus inquiétant, ces dernières années, est la modification du profil des *hackers*. Au départ, on avait principalement affaire à des individus isolés à la recherche de reconnaissance et/ou en guerre idéologique contre *Big Brother*. Aujourd'hui, on doit faire face à des réseaux criminels de mieux en mieux organisés, directement ou indirectement liés à des ramifications mafieuses, pour qui l'Internet est une sorte d'Eldorado du non droit. La sophistication s'est donc accrue, mais surtout l'ampleur des risques financiers a littéralement « explosé ». En 2004, l'exploit technologique s'est effacé devant l'appât du gain devenu la raison principale d'attaques organisées et ciblées.

S'ajoute à cela un autre phénomène : les piratages sont de plus en plus générés à l'intérieur même des entreprises et des organismes, et donc de plus en plus difficiles à détecter et à combattre. Aujourd'hui, plus de la moitié des attaques sont ainsi des attaques « internes ».

Face à cette menace, l'industrie de la sécurité informatique a, certes, réagi, et la palette des protections s'est considérablement enrichie. Par ailleurs, la réactivité des industriels de la sécurité informatique s'est sensiblement accrue. On estime ainsi qu'en matière d'antivirus, le délai de réaction des leaders du marché est passé, ces deux dernières années, de quelques jours à quelques heures.

Il n'empêche : les risques informatiques sont donc bien réels, de plus en plus importants, mais très largement sous-estimés pour une troisième raison, spécifique à ce nouveau type de risques : le silence des victimes.

L'omerta statistique

On ne lutte efficacement que si l'on connaît son ennemi. Or, il est peu de risques qui sont, à ce jour, plus mal maîtrisés que le risque informatique, et ce, pour trois raisons au moins :

- d'abord parce que ce risque est mal détecté par les victimes elles-mêmes : en France, le nombre d'entreprises qui ne peuvent évaluer les pertes liées à une malveillance interne ou à un virus est de l'ordre de 50 %, et seules 3 % d'entre elles déclarent avoir détecté par elles-mêmes qu'elles avaient fait objet d'une intrusion ;
- ensuite, parce que les victimes, pour des raisons de confidentialité et d'image, ne font que très rarement état des attaques dont elles ont été les victimes ;
- enfin, parce que, si la perception du risque informatique progresse, le « passage à l'acte » pour la mise en place d'un système de sécurité est tributaire des fortes contraintes budgétaires actuelles des entreprises et de l'appréciation floue du risque informatique. Retour à « la poule et l'œuf »...

DES CONSÉQUENCES PROTÉIFORMES ET DE MULTIPLES INTERROGATIONS

Le pessimisme n'a pas sa place ici et le scénario catastrophe du *big bang* informatique avancé par certains spécialistes est bien peu vraisemblable. À toute mutation technologique correspondent des risques nouveaux qu'il est possible de limiter, dès lors que l'on en prend la mesure, et les conséquences de la montée de la cybercriminalité doivent, pour cela, être mesurées avec précision et rigueur.

Les premières conséquences se déchiffrent au niveau microéconomique par une perte d'efficacité et de compétitivité liée aux surcoûts sécuritaires qu'engendrent ces nouvelles menaces ; mais aussi et surtout par les effets indirects des attaques informatiques sur l'organisation même des entreprises. Cela commence à se vérifier dans des secteurs fortement automatisés, comme la banque où l'intensification de l'interconnexion entre les réseaux informatiques augmente considérablement les risques. De manière plus indirecte,

la cybercriminalité pose en termes nouveaux, au travers de vols ou de détournements de fichiers, le problème de la concurrence. Certains métiers, dont l'activité repose sur la gestion de fichiers ou de brevets, sont, dans ce domaine, particulièrement menacés.

Au niveau mésoéconomique, certains secteurs sont plus directement concernés que d'autres. C'est notamment le cas de la banque et de l'assurance, où non seulement l'organisation interne, mais aussi la relation clients, sont directement impactées. Avec, en prime, dans certains cas, une incidence instantanée sur la matière première même de l'entreprise, à savoir l'argent (pour le seul cas du *phishing*, 2 millions de victimes aux États-Unis en 2003, et un préjudice global de 1,2 milliard de dollars[2]).

Dans le secteur de l'assurance se greffe une autre interrogation sur l'assurabilité même de la cyberdélinquance. Jusqu'où peut-on assurer ? Quelles doivent être les clauses suspensives du contrat ? Quel *pricing* mettre en place ? À bien y réfléchir, le métier de l'assurance n'est peut-être pas le plus menacé, mais sûrement le plus globalement impacté dans toutes ses dimensions. Nul doute qu'une réflexion approfondie commune à ce secteur et à l'industrie de la sécurité informatique doit être conduite, pour mieux cerner selon quels critères la frontière du risque informatique est susceptible d'évoluer à l'avenir.

D'une manière plus générale, on peut considérer que la vulnérabilité d'un secteur en matière de cybercriminalité dépendra de quatre critères principaux :
- son intensité informationnelle ;
- son degré d'informatisation ;
- son intensité capitalistique ;
- son intégration organisationnelle.

Ces critères sont classés par ordre d'importance décroissante et sont, pour certains d'entre eux, fortement corrélés. À ce stade, la seule chose que l'on puisse dire est que le secteur du BTP (bâtiments et travaux publics) est à peu près le seul à être organiquement à l'abri de ce nouveau type de risque...

Pour conclure (de manière très provisoire), nous constatons que les conséquences de la cybercriminalité ne se font pas encore sentir au plan macroéconomique. De même que la tendance à la sous-évaluation des risques informatiques n'a plus sa place aujourd'hui, les projections apocalyptiques de certains consultants paraissent totalement déplacées. Néanmoins, compte tenu de la croissance exponentielle du phénomène, on ne peut, dès à présent, faire l'économie d'une réflexion sur le caractère systémique que pourrait, à l'avenir, revêtir le risque informatique.

Si l'on en vient maintenant au cadre réglementaire, le lecteur ne sera pas étonné d'apprendre que le débat sur ce sujet est significativement plus intense aux États-Unis qu'en Europe. Depuis le *Computer Fraud and Abuse Act* de 1984, de nombreuses lois nouvelles intègrent ainsi un volet sur la sécurité informatique. C'est le cas notamment de la loi Sarbanes-Oxley sur la sécurité financière post-Enron (obligation d'information sur les procédures de contrôle interne) ou de la loi Gramm-Leach-Bliley sur la protection des données financières. De même, ont été votées de nombreuses lois s'appliquant à certaines formes spécifiques de cybercriminalité, comme l'*Anti-phishing Act* de juin 2004 (5 ans de prison pour l'envoi d'e-mails non sollicités).

En Europe en général et en France en particulier (loi Godfrain de 1988 sur la fraude informatique et loi sur la confiance dans l'économie numérique de 2004), le législateur est plus mesuré et moins « innovant ». S'oppose ici une vision juridique considérant la cybercriminalité comme un ensemble d'infractions classiques (telles que l'escroquerie, l'usurpation d'identité, la collecte illicite de données personnelles, ou la contrefaçon des droits d'auteur), commises à l'aide de dispositifs nouveaux, à une autre vision, qui prévaut aujourd'hui aux États-Unis, où la cybercriminalité est considérée comme une forme totalement nouvelle de criminalité nécessitant un dispositif législatif spécifique.

Sans trancher sur ce débat, que l'évolution même de la technologie va nourrir et faire évoluer (plutôt, semble-t-il, dans la direction choisie par les États-Unis), mentionnons deux autres aspects, et non des moindres, du problème réglementaire. Le premier concerne l'application de telles lois. La sophistication même des techniques employées rend l'analyse du délit et du préjudice toujours plus délicate. Mais s'ajoute à cela un problème de territorialité de plus en plus inextricable, les *hackers* menant de plus en plus leurs attaques de l'étranger et, généralement, de lieux de « non droit » (avec une préférence marquée, semble-t-il, pour des plates-formes pétrolières réaménagées et immergées dans les eaux territoriales de paradis fiscaux ou des républiques de l'ex-URSS). Deuxième problème : l'interférence des dispositifs de garantie de la sécurité informatique avec la défense des libertés individuelles. Car pour mieux protéger, il faut rentrer au cœur du système et cela pose de nouveaux problèmes, que la Commission informatique et libertés (Cnil) en France devra, à l'avenir, résoudre.

QUE FAIRE ?

Il n'est pas possible de conclure de manière définitive sur un sujet intrinsèquement aussi mouvant. Nous espérons avoir convaincu le lecteur de la pertinence de nos interrogations et de la nécessité de sortir d'une attitude qui se résume aujourd'hui, dans bien des circonstances, à : « Circulez ! Il n'y a rien à voir ! ». Seule certitude dans ce domaine : ce sujet concerne tout le monde : les entreprises et les professions aussi bien que les pouvoirs publics. S'il fallait dresser une liste de priorités à ce stade, cela commencerait tout simplement par une meilleure mesure de l'ampleur du phénomène. Clairement, l'opacité dans ce domaine nous paraît une parade dérisoire et presque... criminelle.

Par ailleurs, un important effort de recherche doit être accompli, au plan national et européen, pour rester dans la « course » à la sécurité informatique et, là, les pouvoirs publics doivent prendre conscience du rôle stratégique de cette industrie nouvelle, dominée à ce jour par les États-Unis et Israël.

Enfin, une réflexion sur le cadre législatif doit être menée (y compris dans le cadre des réglementations en cours d'adoption, comme par exemple Bâle II dans le secteur bancaire), et, là,

le secteur privé, principale victime et meilleur connaisseur des réalités de terrain, doit participer activement aux débats. Car s'il est bien un domaine où la frontière entre le public et le privé n'a pas de sens, c'est bien celui-là...

Notes

1. Source : Frost & Sullivan.
2. Étude du cabinet Gartner, juin 2004.