

La cyber-criminalité en pleine ascension

«Quand le monde virtuel attaque le monde réel»

Sarah Merouani, Risk & Outsourcing Solutions

Résumé

Si Internet a facilité l'accès à d'innombrables informations à des millions de personnes, il a dans le même temps favorisé le développement d'une nouvelle forme de délit: la cyber-criminalité.

Plus rentable que le trafic de stupéfiants, la cyber-criminalité est devenue le nouveau fléau de ce 21^{ème} siècle. Dans la ligne de mire des cyber-criminels, on trouve les entreprises, les organisations étatiques et surtout le simple utilisateur d'Internet. Motivés avant tout par l'appât du gain, ces cyber-criminels cherchent de plus en plus à déstabiliser leurs victimes sur un plan politique. Les armes utilisées pour mener leurs attaques ne cessent d'évoluer en parallèle des moyens de défense mis en œuvre. Les politiques essaient d'harmoniser une réglementation internationale commune pour lutter contre ces actes malveillants. Mais est-il vraiment possible de combattre un ennemi invisible ?

La cyber-criminalité en pleine ascension

Le panorama général

Alors qu'un crime est commis toutes les trois minutes et demi dans les rues de New York, une identité est volée en ligne toutes les trois secondes soit près de 10 512 000 identités chaque année.¹ La cyber-criminalité est devenue un business illégal à part entière, bénéficiant d'un grand anonymat, et se heurtant à peu d'obstacles, ce qui le rend particulièrement rentable. Productrices de richesse économique, les entreprises sont particulièrement ciblées par la cyber-criminalité et concernées par cette problématique.

Définition

Le terme « cyber-criminalité » a été inventé à la fin des années 90, alors qu'Internet se répandait en Amérique du Nord. Il désigne de façon large une activité dans laquelle les systèmes et les réseaux informatiques sont les **outils**, les **cibles** et les **lieux** pour réaliser des activités criminelles.

La cyber-criminalité se caractérise par deux aspects principalement :

- les cas dans lesquels le type de risque est ancien mais son application nouvelle, comme par exemple les tentatives d'escroquerie par Internet
- de nouveaux périls émergents comme par exemple les cas de piratage, d'introduction dans ou d'espionnage des systèmes informatiques d'autres personnes ou organisations.

Les acteurs

Le profil des cyber-criminels dépend largement de leurs motivations et de

leur niveau d'expertise dans le domaine informatique. Ce profil couvre :

- les vandales
- les intrus / voleurs
- les espions

Leurs motivations peuvent être de la simple curiosité, la recherche de la célébrité, l'appât du profit personnel ou encore la recherche d'un gain économique et/ou politique.

Les espions, dont le profil recoupe à la fois la recherche d'intérêts économiques et/ou politiques avec un fort niveau d'expertise dans les systèmes informatiques, représentent la menace la plus dangereuse. En effet, leurs actions peuvent avoir des conséquences particulièrement lourdes, comme déstabiliser l'économie entière d'un pays ou la perte de grandes sommes d'argent en une seule fois.

Compte-tenu de leur force d'action, ces cyber-criminels requièrent les investissements les plus importants en matière de défense.

Les voleurs dont les desseins sont uniquement l'appât d'un gain personnel représentent la menace en plus forte croissance. Leur stratégie consiste très souvent à dérober de petites sommes d'argent à un grand nombre de victimes. Le contexte économique actuel pourrait être un leitmotiv supplémentaire pour certaines personnes afin de maintenir ou accroître leurs revenus. Selon un sondage conduit par le cabinet de conseil et d'audit KPMG, deux professionnels sur trois (66%) estiment que les ingénieurs informatiques victimes de la crise seraient assez enclins à mettre leurs compétences et leurs connaissances au

La crise a un impact négatif sur la lutte contre la cyber-criminalité.

¹http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20090922_03

service de l'économie cyber-criminelle (fraude, vol de documents sensibles).²

Les victimes

Les victimes de cyber-attaques se répartissent en trois catégories :

- Les **citoyens**. Les visiteurs individuels de sites Internet sont une cible privilégiée pour les cyber-criminels. Très souvent, les risques encourus sont ignorés et les moyens pour les prévenir sont très faibles. Ainsi, chaque année, plus de 10 millions d'identités sur Internet seraient volées à travers le monde³ : numéros de sécurité sociale ou de cartes bancaires. Ce phénomène est d'autant plus problématique avec le développement du e-commerce et de l'e-banking qui facilitent la diffusion de ces données personnelles. La fraude et l'escroquerie en ligne prennent de plus en plus d'ampleur. Ainsi, en 2001, des groupes organisés en Ukraine et Russie auraient réussi à détourner les numéros d'au moins un million de cartes de crédit aux Etats-Unis.⁴
- Les **acteurs économiques**. Les entreprises représentent également une cible de choix dès lors qu'elles disposent de renseignements variés, dont le vol peut donner lieu à des chantages ou des diffusions pouvant avoir des conséquences lourdes financièrement ou en terme d'image et aller jusqu'à mettre à mal leur pérennité. Elles sont d'autant plus vulnérables qu'elles peuvent être attaquées de l'extérieur mais aussi de l'intérieur via ses employés ou prestataires. Pour les grands groupes industriels, ces attaques représentent un coût et des risques en termes d'image et de compétitivité prohibitifs. C'est pourquoi certaines entreprises se paient les services de

« hackers » à l'origine d'attaques contre leurs propres systèmes.

- Les **administrations publiques** ne sont pas non plus à l'abri d'une attaque. Ici, très souvent est recherchée la déstabilisation économique et/ou politique en s'attaquant à des symboles forts. Les Etats-Unis en ont fait récemment la douloureuse expérience. Depuis le 4 juillet 2009 – jour de la fête de l'Indépendance – plusieurs agences gouvernementales, dont le Département du Trésor, les services secrets, la *Federal Trade Commission* (chargée d'appliquer le droit de la consommation) et le Département du transport, ont été victimes de cyber-attaques. Dans le même temps, la Corée du Sud a également enregistré une série d'attaques visant notamment la Blue House – la résidence et le bureau principal du Président –, le Ministère de la Défense ou encore l'Assemblée nationale. Ces attaques, si elles ne sont pas rapidement déjouées, peuvent conduire à la paralysie économique d'un État, sans compter l'accès à des informations à caractère hautement stratégique qui peuvent être subtilisées à l'insu des États.

Les chiffres

Il semble quasiment impossible de chiffrer le montant des fraudes causées par la cyber-criminalité. C'est ce que la police appelle le « **chiffre noir** ». ⁵ Ceci s'explique principalement par le fait que les entreprises ou les particuliers victimes de ces attaques ignorent avoir subi ces attaques. A cela, s'ajoute une certaine réticence de la part des entreprises à dénoncer ces délits, de peur de dévoiler des secrets inhérents à leur système informatique. De plus, comme le souligne Eugène Kaspersky, expert international dans la lutte contre la cyber-criminalité et fondateur de Kaspersky Lab⁶, « les activités

² KPMG, e-crime survey 2009, mars 2009. Cette étude réalisée par KPMG en collaboration avec AKJ Associates auprès de 307 collaborateurs issus de différents métiers, a été présentée lors du 7^{ème} congrès international sur la cyber-criminalité qui s'est tenu à Londres les 24 et 25 mars 2009.

³ <http://www.kpmg.fr/fr/news/etude-cybercriminalite-mai09.asp>

⁴ Yves Hulman, *Le Temps*, « Le vol de données sur Internet, un marché en pleine expansion », 10.10.2009.

⁵ <http://www.ladocumentationfrancaise.fr/dossiers/internet-monde/cybercriminalite.shtml>

⁶ http://cybercrime.ifrance.com/cout_cybercrime_print.htm

⁶ Logiciel antivirus

criminelles s'inscrivent toujours dans la mouvance des affaires légales. »⁷

Toutefois, l'éditeur d'antivirus McAfee évalue à USD 1 000 milliards par année les pertes subies par les entreprises, à la suite de pertes de données ou d'actions criminelles, faisant ainsi de la cyber-criminalité une activité bien plus lucrative que le trafic de stupéfiants. Après une étude menée auprès de 800 DSI (directeurs des systèmes d'informations) dans quatre pays industrialisés (Etats-Unis, Royaume-Uni, Allemagne, Japon) et quatre pays émergents (Chine, Inde, Brésil, Dubaï), la société McAfee précise qu'en 2008, ces entreprises ont perdu l'équivalent de USD 4,6 milliards en données informatiques sensibles (données clients, données financières, brevets, etc.). Ces pertes de données auraient entraîné un coût d'USD 600 millions pour « colmater les brèches de sécurité en question »⁸. Ramenées à l'échelle planétaire, on atteint le chiffre d'USD 1 000 milliards. En parallèle, un sondage réalisé conjointement par Information Week Research et le cabinet de conseil PriceWaterhouseCoopers chiffre à 1.600 milliards de dollars le temps perdu (chômage technique, réparation des systèmes impactés) par les entreprises victimes de ces attaques depuis l'an 2000.⁹

Une activité bien organisée

La cyber-criminalité est la réplique exacte de toute forme d'exploitation économique, l'aspect illégal en plus. Comme cette dernière, la cyber-criminalité répond à des critères de rentabilité, de gestion des risques ou encore de facilité d'utilisation des produits.

Une particularité importante de la cyber-criminalité et qui encourage de facto sa forte

croissance est le faible niveau de risques encourus comparé aux chances de réussite pour celui qui a recours à ce type d'activité et contrairement au monde réel où la dimension psychologique est très forte et peut avoir un effet de dissuasion certain. Dans le monde virtuel, les cyber-criminels ont tout le loisir d'agir

anonymement puisqu'ils ne sont pas en contact direct avec leurs victimes. La dimension psychologique de l'acte criminel est alors moins pressante et la culpabilité se fait moins ressentir.

Ces criminels du cyber-espace ont de nombreuses ressources à leur disposition pour aboutir à leurs fins tout en conservant leur anonymat. Les sites de e-commerce ont la part belle dans les cibles visées par ces acteurs. Ainsi comme le met en lumière Eugène Kaspersky, « les sites de e-commerce et les banques en ligne, qui s'efforcent de favoriser les transactions financières jouent sur la corde raide à force de rechercher le meilleur compromis entre la vitesse des prestations et les critères de sécurité. »¹⁰ Les sites de jeu en ligne sont également visés tout comme les services boursiers en ligne en raison de la forte liquidité des actifs échangés sur les marchés boursiers.

Le Web 2.0¹¹ a gagné également ses lettres de noblesse auprès des cyber-criminels, avec tout son cortège de réseaux sociaux, blogs, forums comme Facebook, YouTube et Daylimotion.

Le point commun de tous ces services en ligne, qu'ils soient à but lucratif ou dans un but de divertissement, est la facilité de téléchargement, de publication, d'échange d'informations, rendant nécessairement leurs utilisateurs plus vulnérables à des cyber-attaques.

La cyber-criminalité a généré en 2008 un revenu d'environ un billion (un million de millions) de dollars.

Tribune de Genève, 07.10.2009,

⁷ <http://www.itrnews.com/articles/99055/2010-nouveaux-defis-cybercriminalite-br-eugene-kaspersky.html>

⁸ <http://pro.01net.com/editorial/402185/la-cybercriminalite-ferait-perdre-chaque-annee-1-000-milliards-de-dollars-aux-entreprises/>

⁹ http://cybercrime.ifrance.com/cout_cybercrime_print.htm

¹⁰ Ibid.

¹¹ Le web 2.0 désigne une étape de l'évolution du web dont l'utilisateur et le partage d'information sont la clé de voute. Ce web est notamment caractérisé par l'apparition de nouveaux services multi-supports (ordinateur, pda, téléphone) favorisant l'interaction entre les internautes (blogs, wikis, social networking, partage de photos et de vidéos, réactions).

Les menaces

Si les risques liés à la cyber-criminalité évoluent selon une dynamique propre aux technologies de l'information et de la communication, la responsabilité des hommes est plus directement impliquée dans leur survenance. De plus, avec l'intensification du phénomène Internet qui est un phénomène global (emails, réseaux sociaux), le risque devient global pour les entreprises dès lors qu'il s'insinue au cœur même de celles-ci.

Les menaces internes

Les entreprises ont tendance à se focaliser uniquement sur les risques d'attaques venant de l'extérieur et donc à sous-estimer ceux pouvant venir de l'intérieur même. Pourtant, les opportunités de réaliser de telles attaques sont nombreuses et peuvent engendrer des conséquences bien plus lourdes pour les entreprises.

De manière générale, les entreprises sont relativement dépourvues face aux menaces internes. Il existe différentes situations à risques et le panorama présenté ci-dessous n'est bien entendu pas exhaustif.

La consultation de sites Internet

L'usage d'Internet s'est complètement banalisé dans les entreprises, devenant même un outil de travail à part entière, notamment avec l'usage de la messagerie électronique. De plus, beaucoup d'employés font usage d'Internet à des fins personnelles pendant leurs heures de pause mais également pendant leurs heures de travail.

Ainsi, la simple visite de sites Internet peut laisser s'infiltrer toutes formes de logiciels malveillants. Il n'y a même plus besoin d'ouvrir ou de télécharger des fichiers pour voir son ordinateur contaminé par une forme de « malware »¹². Il y a encore peu, il était possible d'identifier ces menaces grâce au nom que portaient ces virus tel que « Melissa » ou encore « I love you ». Afin de

¹² Logiciel développé dans le but de nuire à un système informatique.

permettre à ces virus de pénétrer le système et les fichiers en toute discrétion sans éveiller les soupçons de l'utilisateur de la machine, très souvent les messages d'avertissement de l'antivirus sont supprimés.

Aujourd'hui la réalité est tout autre. Candid Wüest, spécialiste des menaces informatiques chez Symantec (concepteur des célèbres logiciels Norton) souligne que « quelques 13 000 sites Internet sont infectés chaque jour », ajoutant même que « la plupart d'entre eux sont tout à fait légitimes. »¹³

Beaucoup d'entreprises mettent en place des filtres pour interdire l'accès à certains sites, notamment les sites de messageries personnelles comme Hotmail ou Gmail mais aussi les sites de réseaux sociaux à l'instar de Facebook et Twitter, qui sont très consultés. Mais n'importe quelle page de site peut être concernée, dès lors qu'une faille a pu être exploitée par des programmeurs malveillants. Ainsi, même des sites tout à fait professionnels sont susceptibles de représenter un danger.

Les messageries électroniques

Les messageries électroniques se sont rapidement imposées comme un outil de travail indispensable au sein des entreprises, permettant une communication rapide et discrète à la fois en interne entre collaborateurs et en externe avec les clients et les partenaires. Dans ces emails, beaucoup d'informations et de documents à la portée plus ou moins confidentielle peuvent être échangés. Ils représentent dès lors une aubaine pour les cyber-criminels qui veulent s'approprier ces informations.

Face au renforcement des défenses informatiques, les hackers recourent de plus en plus aux attaques indirectes, en s'en prenant ainsi directement aux stations de

¹³ Cité in *Le Temps*. « Le vol de données sur Internet, un marché en pleine expansion », 10.10.2009.

travail des collaborateurs au travers de leur messagerie. La technique est simple puisque comme l'indique Marco Ricca, directeur de la société IRIS, il suffit que « des e-mails [soient] envoyés nominativement aux collaborateurs. Selon la sophistication du programme, le seul fait de le recevoir va donner accès au hacker ».¹⁴ Si tel n'est pas le cas, il faudra alors ouvrir le message puis cliquer sur un lien ou une pièce jointe, qui seront accompagnés d'un cheval de Troie. Les sites de réseaux sociaux professionnels tels que LinkedIn ou Viadeo facilitent le travail des hackers. En effet, ces sites demandent très souvent à leurs membres d'indiquer leurs intérêts ou autres hobbies. Dès lors, quoi de plus simple que de pirater une messagerie en personnalisant les e-mails afin de susciter l'intérêt de la victime pour être certain de leur ouverture.

Pour s'introduire dans une messagerie électronique, le hacker peut également se faire passer pour l'administrateur ou une personne en charge de la sécurité du réseau en utilisant un pseudonyme du type « admin.reseau ». L'objectif est d'obtenir le mot de passe de la victime.

Une fois les boîtes mail piratées, il est alors très aisé d'accéder directement au serveur et de récolter toutes les informations voulues.

Les périphériques de stockage

Les entreprises s'exposent également à de grands risques en autorisant, sans aucun contrôle, l'usage de périphériques de stockage comme les clés USB et les disques durs externes. Les risques peuvent être doubles. D'une part, ces matériels peuvent permettre la fuite d'information. D'autre part, ils peuvent importer de nouveaux virus dans le réseau informatique de l'entreprise.

Les ordinateurs personnels des employés ont très souvent une capacité de protection faible contre les cyber-attaques et sont donc en grande majorité porteurs de virus. Ceux-ci sont très facilement importés sur les périphériques qui, connectés ensuite sur le

¹⁴ Ibid.

poste de travail, peuvent infecter l'ensemble du réseau de l'entreprise.

La fuite d'information ("Data leakage")

Ce sont les employés, en partance ou non, qui constituent le premier risque de vol de données. Les entreprises disposent de données vitales pour le développement de leur activité : secrets d'affaires, coordonnées de partenaires commerciaux, données clients, données stratégiques, etc. Il est alors très tentant pour un employé de quitter les locaux en emportant des données, des procédures ou des documents, surtout si la relation de travail se termine mal.

Selon Deloitte, 92% des attaques sont influencées par des événements négatifs relatifs à l'environnement de travail et 97% des acteurs présentent des signes de mécontentement avant de participer à une attaque¹⁵.

Le vol de données peut se faire de différentes manières :

- L'utilisation de **périphériques de stockage**, notamment les clés USB. Discrètes et d'une capacité de stockage de plus en plus importante, ces dernières sont très nuisibles pour les entreprises et très difficiles à contrôler ;
- L'envoi d'**e-mail** à soi-même ou au destinataire de l'information dérobée ;
- L'utilisation de **technologies sans fil** comme le Wifi ou le bluetooth ;
- La duplication de **documents physiques** ;
- La récupération de données dans les **poubelles** de l'entreprise.

Les employés sont bien évidemment les premières personnes à l'origine de ces modes opératoires. Mais il ne faut pas non plus négliger les prestataires de services qui peuvent avoir un droit d'accès très étendu aux données de l'entreprise.

Les menaces externes

¹⁵ Carnegie Mellon University, GFSI Survey 2008.

Les chevaux de Troie

Selon l'étude de KPMG, 68% des sondés considèrent les chevaux de Troie comme la cyber-attaque la plus dangereuse pour leur réseau.¹⁶ Ils font partie des grandes menaces que l'on peut rencontrer sur Internet, parmi les virus et autres vers, à la seule différence néanmoins qu'ils ne se reproduisent pas.

Les chevaux de Troie utilisent une ruse pour agir de façon invisible, le plus souvent en se greffant sur un programme anodin et sain. Ils sont donc très difficiles à repérer, d'où leur dangerosité. Leur objectif est d'ouvrir une porte dérobée ("*backdoor*") sur le système cible, permettant à l'attaquant de revenir par la suite épier, collecter des données, les corrompre, contrôler voire même détruire le système.¹⁷

Dès lors que les chevaux de Troie ne se répliquent pas, ils ne possèdent pas de signature de réplication et donc ne sont pas détectables par les logiciels antivirus. S'il n'est pas possible de détecter leur présence, il peut être en revanche possible d'essayer de détecter leur activité. Un cheval de Troie est en effet obligé d'ouvrir des voies d'accès pour pouvoir communiquer avec l'extérieur. Il suffit de remarquer si des ports¹⁸ de la machine sont habituellement inutilisés.

Les chevaux de Troie peuvent être utilisés à des fins professionnelles. C'est le cas des Help Desk, qui vont prendre en main à distance un ordinateur pour intervenir sur les données à la demande de l'utilisateur. Mais, le plus souvent, ils sont utilisés à des fins d'espionnage ou de déstabilisation. C'est ainsi qu'en octobre 2009, le site du Département fédéral des affaires étrangères

¹⁶ KPMG, p. 22

¹⁷ <http://www.securiteinfo.com/attaques/divers/troie.shtml>

¹⁸ Un port est une "porte virtuelle" sur une machine connectée à un réseau. C'est par cette "porte" que transitent les informations échangées par le réseau. Il est possible d'ouvrir les ports n°1 à 65536. Certains ports sont quasi attirés à certains services (exemple : le port 80 est utilisé pour surfer sur Internet (port http), le port 21 est utilisé pour le téléchargement (port FTP) et les ports 110 et 25 sont utilisés respectivement pour la réception et l'envoi d'email par un serveur POP).
<http://www.clubic.com/article-14181-1-trojan-et-virus-comprendre-et-se-protger.html>

suisse (DFAE) a été victime d'une attaque informatique bloquant ainsi pendant plusieurs jours l'utilisation de la messagerie électronique. Plus récemment, à quelques jours de l'ouverture du sommet de Copenhague sur le climat (7 au 18 décembre 2009), des milliers de courriers électroniques privés et de documents secrets appartenant aux plus prestigieux scientifiques britanniques et américains ont fait leur apparition sur Internet. En piratant l'une des banques de données sur le climat les plus importantes du monde, hébergées par l'Université d'East Anglia, en Grande Bretagne, les hackers sont parvenus à créer la discorde entre ces chercheurs en disqualifiant réciproquement leurs travaux. L'épisode du DFAE n'étonne guère les spécialistes puisque selon Sébastien Fanti, avocat spécialisé dans le droit d'auteur sur Internet, « aujourd'hui, des hackers suisses proposent pour 2 000 francs leurs services pour pirater les e-mails de particuliers ».¹⁹

Les chevaux de Troie deviennent de plus en plus l'apanage d'apprentis hackers en raison de leur facilité d'utilisation et de leur grande efficacité. Ils représentent un phénomène inquiétant car grandissant. Il serait donc inopportun de négliger leur pouvoir de nuisance tant sur le système d'information en lui-même que d'un point de vue d'image de l'entreprise. Il ne faut pas négliger l'impact médiatique entraîné par la découverte d'un cheval de Troie dans le système d'information d'une entreprise : compromission, espionnage industriel, remise en cause de la politique de sécurité.

Le déni de service

Est appelée « attaque par déni de service » toute action malveillante ayant pour résultat la mise hors-ligne d'un serveur. Il s'agit de priver une personne, une entreprise ou une organisation des ressources réseaux dont elle dispose en temps normal.²⁰ Le déni de service va toucher principalement :

¹⁹ Cité in La Tribune de Genève, « L'attaque qui a visé le Département des affaires étrangères est révélatrice de l'évolution des techniques des hackers », 28.10.2009.

²⁰ <http://www.securiteinfo.com/attaques/hacking/dos.shtml>

- le service de messagerie électronique
- l'accès à Internet
- les ressources partagées (pages Web)
- les services à caractère commercial comme Yahoo!, Google ou EBay.

Le hacker souhaitant nuire à une machine ou un système par un déni de service n'a que l'embaras du choix des méthodes à utiliser. En effet, plusieurs types de cyber-attaques – Virus, débordements de tampon (« *buffers overflows* »), attaque par fragmentation (attaque *Teardrop*), etc. – vont engendrer une saturation du système aboutissant à un déni de service. On se souvient ainsi du virus nommé « Blaster » qui, le 14 août 2003, a provoqué la plus grande panne électrique aux Etats-Unis et au Canada. Le but de ce ver était de lancer une attaque en déni de service contre Microsoft, et plus particulièrement contre son serveur de mise à jour *windowsupdate.com*. Plus récemment en été 2009, ce sont Twitter, Google et Facebook qui ont été les victimes d'une attaque en déni de service. Les cyber-criminels semblent être résolus à prendre comme cible les sites en vogue. Si Google et Facebook ont affirmé avoir su gérer la riposte sans encombre, le site de microblogging Twitter a, quant à lui, été inaccessible pendant deux heures. Le groupe américain McAfee prévoit une hausse des tentatives de piratages en 2010 contre les sites de socialisation. Comme l'indique la société « les cyber-criminels vont profiter de l'explosion des applications et services sur Facebook et de la confiance qui règne entre « amis » pour inciter les internautes à cliquer sur des liens dont ils se seraient autrement méfiés. »²¹

Ces cyber-attaques à l'encontre de sites très fréquentés posent inévitablement la question de la protection des données personnelles dès lors que leur objectif est de collecter un certain nombre d'informations sur leurs utilisateurs.

Au final, le déni de service est un type d'attaque qui peut réellement coûter très cher dès lors qu'il interrompt le cours normal

des transactions pour une entreprise. Les sommes et les enjeux étant considérables, ils ne cesseront de susciter l'intérêt des hackers.

Le phishing

Le terme anglais *phishing* est une variante orthographique du mot *ishing*, c'est-à-dire aller à la pêche et plus précisément dans le cas présent, aller à la pêche aux informations personnelles.

Le phishing est un type de falsification qui a pour but de voler une identité.²² Un hacker tente d'obtenir des informations telles que numéros de carte de crédit, mots de passe, numéros de compte ou autres informations confidentielles, sous de faux prétextes.

Ce type d'attaque se produit généralement par l'intermédiaire de messages électroniques non sollicités ou de fenêtres contextuelles. Plus concrètement, un cyber-criminel envoie des millions de messages falsifiés (spam) qui semblent provenir de sites de confiance ou sites Web connus à l'instar de ceux de sa banque ou de son gestionnaire de cartes de crédit. L'adresse électronique utilisée, proche du site Web officiel, renvoie vers un site falsifié qui récoltera toutes les informations personnelles transmises par la victime. Celles-ci pourront ensuite être utilisées par le hacker pour acheter des biens en ligne, demander une nouvelle carte de crédit ou voler l'identité de l'internaute. Personne n'est à l'abri d'un vol d'identité puisque même le Président français Nicolas Sarkozy en a fait les frais à l'automne 2008. Son compte bancaire a en effet été piraté suite au vol de ses données confidentielles. Les deniers délestés étaient relativement peu importants puisque les comptes de M. Sarkozy n'ont permis que l'achat de quelques biens en ligne et la souscription à un abonnement de téléphonie mobile.²³ Président ou simple citoyen, personne n'est à l'abri des desseins d'un cyber-criminel.

²¹ <http://technaute.cyberpresse.ca/nouvelles/internet/200912/30/01-935115-facebook-et-twitter-cibles-de-choix-des-pirates-en-2010.php>

²² <http://www.microsoft.com/switzerland/athome/fr/security/email/phishing.msp>

²³ <http://www.lejdd.fr/Societe/Actualite/Compte-Sarkozy-Escrocs-mais-pas-trop-16243/>

Les attaques par phishing sont donc le plus souvent dirigées vers les sites sensibles tels que les sites bancaires. Mais on voit apparaître de plus en plus d'attaques à

l'encontre des sites de réseaux sociaux, du fait que les profils des utilisateurs de ces réseaux sociaux contiennent de nombreux éléments privés.

Les dommages causés par les attaques virales

	Spam	Virus	Spyware	Phishing
Incidence	1 pers. sur 2 est touchée par le spam massif	1 pers. sur 5 a rencontré un problème majeur, voir coûteux	1 pers. sur 11 a rencontré un problème majeur, voir coûteux	1 pers. sur 81 a perdu de l'argent sur un compte
Coût en moyenne	-	100 \$	100 \$	200 \$
Coût total	-	3,3 milliards \$	1,7 milliards \$	2,1 milliards \$

Source : Consumer Reports National Research Center / 2007

Le traitement de la cyber-criminalité

Des réponses normatives

ISO 27000

L'Organisation internationale de normalisation (ISO) a édicté une série de normes dédiées au pilotage de la sécurité de l'information au travers de la série ISO/IEC 27000. Certaines de ces normes ont déjà fait l'état d'une publication alors que d'autres sont encore au stade de projet.

Publié en octobre 2005, le standard **ISO 27001** est la base des règles de certification ISO 27000. Il s'adresse à tous les types d'organismes (entreprises commerciales, administrations,...) et décrit les exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI) dont l'objectif est de garantir la protection des actifs informationnels. Le SMSI s'adapte à chaque organisme. Les informations étant protégées de toute perte ou intrusion, les parties prenantes seront plus confiantes.

Les autres normes de la série ISO 27000 énoncent d'une part les mesures destinées à la mise en place d'un SMSI. Ces mesures diffèrent en fonction du secteur d'activité de

l'entreprise souhaitant implanter un SMSI. D'autre part, elles posent les exigences requises pour obtenir la certification du SMSI.

La norme ISO 27000 est devenue un réel enjeu pour les entreprises. En s'assurant de disposer d'un système informatique capable de résister au mieux à des cyber-attaques, elles peuvent espérer assurer leur pérennité auprès de leurs fournisseurs et de leurs clients. Ainsi, de plus en plus d'entreprises recherchent cette certification en vue d'éviter le nombre d'audits externes commandités par leurs partenaires ou clients.

La convention sur la cyber-criminalité

Le caractère transfrontalier de la cyber-criminalité exclut un traitement individuel et exige de facto un renforcement de la coopération et de la coordination internationale. Prenant conscience du problème, les pays membres du Conseil de l'Europe et leurs partenaires (Etats-Unis, Canada, Japon, Afrique du Sud) ont adopté le 23 novembre 2001 à Budapest une **Convention sur la cyber-criminalité**. Cette dernière constitue la première convention pénale à

vocation universelle destinée à lutter contre le cyber-crime. Il s'agit d'une réponse globale aux crimes commis sur et à travers les réseaux informatiques.

Cette convention poursuit trois objectifs :

- harmoniser les législations des États signataires en matière de cyber-criminalité
- compléter ces législations, notamment en matière procédurale
- améliorer la coopération internationale, notamment en matière d'extradition et d'entraide répressive.

Un protocole additionnel à la Convention sur la cyber-criminalité a été ouvert à la signature en janvier 2003. Celui-ci étend le champ d'application de la Convention puisqu'il demande aux États de criminaliser la diffusion de matériel raciste et xénophobe par le biais de systèmes informatiques.

A la fin de l'année 2007, sur les 42 États signataires de la Convention sur la cyber-criminalité, seul un tiers a procédé à sa ratification.

La Suisse fait partie des mauvais élèves puisqu'à ce jour, elle n'a toujours pas ratifié la Convention du Conseil de l'Europe sur la cyber-criminalité. Elle se justifie en arguant que la réglementation générale actuelle de la responsabilité pénale des prestataires est suffisante pour lutter efficacement contre la cyber-criminalité. Toutefois, le Conseil fédéral n'est pas hostile à cette ratification et demande à ce que celle-ci puisse avoir lieu prochainement. Cette demande est d'autant plus pertinente que le droit suisse satisfait dans une large mesure aux exigences posées par la Convention en matière de lutte contre les infractions commises par le canal des médias électroniques.

L'assurabilité des cyber-attaques

Le risque pour les entreprises étant particulièrement élevé – 8 entreprises sur 10 seront concernées – et les dommages potentiellement considérables, la question de l'assurabilité des cyber-risques est fondamentale. Née du développement d'Internet,

les produits d'assurance cyber-risques ont fait leur apparition il y a quelques années aux Etats-Unis. Or, seulement 2% des pertes liées à la cyber-criminalité sont couvertes par l'assurance. Et en dépit du fait que le patrimoine le plus exposé de l'entreprise, à savoir son système d'information, moins de 30% des entreprises s'assurent contre les cyber-risques.

En Europe, la question de l'assurabilité des cyber-risques n'en est qu'à ses balbutiements. Si les pays scandinaves, l'Allemagne ou encore le Royaume-Uni prennent conscience de l'importance réelle à accorder au marché de la cyber-assurance, d'autres pays comme la France affichent un retard important.

La Suisse, quant à elle, commence à prendre le problème très au sérieux et à mettre en place des mesures. Ainsi, les autorités helvétiques soucieuses de protéger les infrastructures d'information et de communication du pays (y compris le réseau Internet) contre les piratages, les défaillances et les attaques, ont mandaté le DFF (Département Fédéral des Finances) de mettre en place une centrale d'enregistrement et d'analyse pour la sûreté de l'information : MELANI (www.melani.admin.ch). L'offre de MELANI est avant tout destinée aux PME et aux particuliers, et est opérationnelle depuis le 1^{er} octobre 2004. Elle se décompose en trois volets :

- des informations rappelant les dangers liés à l'utilisation des technologies nouvelles, notamment Internet et l'e-banking
- des rapports commentant les tendances du secteur IT et portant sur la criminalité informatique dans le monde et en Suisse
- un formulaire d'annonce qui permet de signaler les problèmes qu'ont pu rencontrer les utilisateurs.

En parallèle à l'offre MELANI, des dispositifs davantage techniques sont proposés aux entreprises pour se prémunir contre les cyber-risques. L'objectif est de transférer in fine le risque résiduel auprès d'une assurance. Ainsi, la société IRIS a développé un dispositif à destination des

PME. Le produit IRIS est un boîtier qui est installé en amont de l'infrastructure et il analyse tous les flux entrants et sortants. Les informations recueillies permettent d'identifier la présence d'une attaque contre le système. 95% du risque est ainsi couvert par la partie technique de la solution et les 5% restant sont transférés via une couverture d'assurance. L'assurance du risque résiduel permet de financer les moyens de remise en état du système ou encore de rembourser les préjudices comme les demandes de rançon.

En dépit des solutions techniques actuellement offertes aux entreprises, force est de constater qu'il ne leur est encore pas possible de totalement se couvrir contre ce genre de risque par des produits d'assurance. En effet, l'atypisme des cyber-risques (évolution rapide, peu de statistiques et d'expérience permettant une cotation, caractère systémique de certains périls IT) rend leur assurabilité fortement limitée par rapport aux autres branches d'assurance, tout du moins par les méthodes actuarielles traditionnelles, c'est-à-dire par la mutualisation. En effet, pour qu'une assurance accepte de couvrir un risque, celui-ci doit être ou devenir acceptable. Il faut donc tout d'abord l'évaluer, puis si besoin le réduire, pour qu'il devienne transférable à l'assureur. Or l'évolution permanente des technologies et la transformation continue des dangers limitent dans le temps la validité d'une quantification des cyber-risques. De plus, le caractère transfrontalier de la cyber-criminalité rend imparfaite toute diversification géographique par la ré-assurance. Dès lors, comment évaluer un risque en évolution constante et complètement diffus sur l'ensemble de la planète ?

Des solutions techniques

La mise en place de normes internationales ou de produits d'assurances est nécessaire pour contrer les desseins des cyber-criminels. Mais ces solutions trouvent leurs limites dans le fait qu'elles n'interviennent qu'une fois l'attaque réalisée et les dommages survenus. Il faut donc agir de

façon préventive et éviter que l'attaque même ne se réalise. Des solutions davantage techniques existent et les exemples donnés ci-dessous ne constituent pas une liste exhaustive.

Les mesures de réduction type pare-feu et antivirus sont une première réponse à la problématique des cyber-attaques. Mais elles ne permettent pas d'identifier et d'éviter celles-ci.

- Un **pare-feu** (appelé aussi *Firewall* en anglais) est un système permettant de protéger un ordinateur des intrusions provenant d'un réseau tiers (notamment Internet). La mission du pare-feu est de filtrer les paquets de données échangées entre la machine du réseau interne et la machine extérieure, c'est-à-dire de reconnaître les adresses IP de la machine émettrice et de la machine réceptrice.

La sécurité offerte par le système pare-feu n'est évidemment pas absolue. En effet, pour obtenir une protection optimum, il est nécessaire que l'ensemble des communications vers l'extérieur transite systématiquement par l'intermédiaire du pare-feu et qu'il soit correctement configuré. Ainsi, les accès au réseau par contournement du pare-feu sont autant de faille de sécurité.

- Un **antivirus** est un logiciel conçu pour détecter les logiciels malveillants (dont les virus ne sont qu'un exemple) en analysant les fichiers sur le disque dur et les courriers électroniques, et pour les empêcher de nuire. La détection virale se fait principalement au niveau de la signature du virus. Une fois la signature du virus reconnue, celui-ci va être en principe détruit.

En dépit d'une mise à jour fréquente de la base de signatures, un nouveau virus peut quand même passer inaperçu. Par conséquent, aucun antivirus n'est parfait. Il ne peut pas en effet complètement palier la négligence humaine ou les logiciels Internet non sécurisés.

Enfin, certaines sociétés informatiques se sont spécialisées dans les procédures

d'**Ethical Hacking**. L'objectif est ici de simuler des attaques réelles sur le système pour découvrir et recenser les vulnérabilités techniques de l'entreprise. Cette méthode

permet de dresser une cartographie des risques et de proposer des mesures de réduction à mettre en place.

Conclusion

Les cyber-risques ne sont pas une menace que les entreprises peuvent prétendre résoudre uniquement par la *compliance* ou en développant de nouvelles technologies. Gérer la sécurité de son patrimoine le plus précieux, à savoir son système d'information, est un véritable challenge à relever pour chaque entreprise. Malheureusement, peu d'entre elles prennent conscience de cette nécessité quant bien même elles considèrent que les cyber-attaques représentent leur risque le plus important. De fait peu de moyens sont alloués pour y faire face – en y accordant du temps, des moyens financiers et des ressources – mettant ainsi en exergue tout le paradoxe d'une bonne stratégie d'entreprise. La crise économique actuelle ne favorise pas l'implémentation de solutions pour lutter contre la cyber-criminalité, les investissements étant plus ciblés. L'étude de KPMG révèle que seuls 14% des entreprises

inter-rogées estiment qu'il faille davantage investir dans la sécurité.

La cyber-criminalité est et demeurera encore pour longtemps une activité à part :

- tout d'abord, parce que les méthodes utilisées par les cyber-criminels évolueront toujours en parallèle des moyens de défense déployés
- ensuite, parce qu'il n'est pas nécessaire que les armes soient sophistiquées pour atteindre son but. Il suffit juste que la victime ignore qu'elle soit exposée à un risque
- enfin, parce que la cible privilégiée des cyber-criminels demeurera toujours le simple consommateur qui fait ses achats, consulte son compte bancaire ou « boursicote » en ligne.

“Pour être certain de prendre ce que vous attaquez, attaquez là où l'ennemi ne peut se défendre.”

Sun Tzu, L'Art de la Guerre

Pour plus d'informations, veuillez contacter :

Sarah Merouani (Auteur)
Risk & Outsourcing Solutions
Project Manager Junior
smerouani@unirisc.ch

Elisabeth André-Raecke
Spécialiste risques financiers
eandre@unirisc.ch

UNIRISC Group
Rte de Florissant 81
Case postale 145
1211 Genève 17
Tél. : +41 22 839 85 85
Fax : +41 22 839 85 86
www.unirisc.ch