Cybercriminalité
Faire du risque un atout !

Même si les données objectives manquent, Internet constitue de plus en plus une source de profit et un moyen d'expression de la criminalité organisée. Selon Vladimir Golubev, seuls 12% des cybercrimes seraient connus des instances de justice, de police et du grand public[1].

Le manque de statistiques officielles provient en partie du fait que les organisations ne souhaitent pas forcément communiquer sur les malveillances subies. Pire, elles ignorent bien souvent qu'elles sont victimes d'une malveillance, lorsqu'elles font l'objet d'attaques passives (détournement transparent de données, de flux, écoutes clandestines, introduction non détectée dans des systèmes...), ou n'en prennent conscience qu'a postériori, lorsque toute action de réaction devient obsolète.

En fait, les organisations ne savent pas non plus gérer les situations de crise. Elles n'ont à l'évidence pas une confiance suffisante dans les instances de justice, de police et dans leur compétence propre pour traiter ce type de problème. Résultats : certaines préfèrent même se faire justice elles-mêmes.

La recherche de profit

Qu'il s'agisse de "téléchargeur" ou "implanteur" (downloader), de "key-loggers", de "bot-robots", de logiciels publicitaires (adware - advertising software), de logiciels espions (spyware - spying software) dont un grand nombre existe sous couvert d'outils d'aide à la navigation, à la personnalisation des services, etc., la présence de programmes indésirables s'exécutant dans l'environnement de l'utilisateur continue à augmenter. Les vecteurs d'introduction de ces logiciels peuvent être des logiciels gratuits ou en démonstration, des sites pornographiques ou de jeux, mais aussi le courrier électronique, le spam, les forums de discussions, etc. Quel que soit leur mode d'introduction, même s'ils sont installés après un consentement initial ou

Solange Ghernaouti Hélie
HEC Lausanne

Les organisations ne peuvent plus négliger les dangers réels qui les menacent.
Elles doivent toutes s'y préparer car la menace cybercriminelle un jour se concrétisera.
Se préparer, c'est faire du risque un levier pour réaliser une sécurité de qualité.

[1] Vladimir Gobulev, Computer crime typology - January 09, 2004 - Computer Crime Research Center http://www.crime- research.org/articles/Golubev1203/

CV Solange GHERNAOUTI HÉLIE

Professeure à l'Ecole des HEC de l'Université de Lausanne. Directrice de l'Institut d'Informatique et Organisation, Vice - Doyenne de l'Ecole des HEC.
Expert international à l'UIT et auteure d'une quinzaine de livres dont *Sécurité informatique et réseaux : cours et exercices corrigés* - Dunod, Février 2006.

avec l'accord implicite de l'utilisateur (ce qui peut être le cas des adware, mais jamais des spyware), leur usage est détourné et ils s'exécutent, le plus souvent, en l'absence de consentement réel des utilisateurs.

Pour la plupart, ces logiciels sont des outils de capture d'informations (vol d'informations, capture de mots de passe, de trafic), d'appropriation de ressources ou d'attaques. Ils permettent notamment de diffuser et de piloter des outils d'attaques en déni de service distribué (DDoS). Plusieurs milliers sont actuellement en circulation. La finalité : le profit financier, en portant par exemple atteinte à des concurrents.

Ces logiciels collectent et transfèrent des données à l'insu de l'utilisateur (observation des habitudes de navigation pour des publicités ciblées) et peuvent servir d'intermédiaires à des activités illégales (relais de spam et de phishing[2], par exemple). En tout état de cause, ils visent à enrichir l'entité qui en est à l'origine.

La détection et la désinstallation de ces logiciels sont parfois difficiles, voire impossibles, par les utilisateurs non experts en informatique. L'internaute possède en effet rarement les compétences ou les outils nécessaires pour les maîtriser.

Ainsi, de nos jours, les virus (vers, chevaux de Troie, bombes logiques) n'ont plus pour objectif principal la destruction massive et gratuite de données, ils sont orientés vers la recherche de gains. Les virus deviennent ainsi les vecteurs de réalisation de la criminalité financière au service, le plus souvent, de la criminalité organisée. Ils constituent des moyens d'enrichissement considérable pour leur auteur et sont des instruments de nuisance et de déstabilisation des organisations et des Etats.

&IS De nos jours, les virus sont orientés vers la recherche de gains.

La banalisation de la cybercriminalité

La cybercriminalité se réalise le plus souvent au travers de délits ordinaires, presque invisibles mais très présents et efficaces grâce à la mise en réseau des ressources et des personnes. Les entreprises, mais surtout leurs ressources informatiques et informationnelles, deviennent ainsi des cibles privilégiées pour les organisations criminelles à la recherche de profits. Il s'agit ici d'une menace stratégique, dans la mesure où l'argent se trouve dorénavant dans les systèmes informatiques, dans les grandes entreprises, dans des fonds de pension, et plus seulement dans les coffres des banques.

De fait, aujourd'hui, les nouvelles technologies facilitent toute sorte de vol, de modification, de sabotage d'informations ou de fraudes. Les phénomènes de chantage, d'extorsion de fonds, de désinformation et de cyberpropagande existent et les ressources informatiques deviennent les otages potentiels des cybercriminels. Les maîtres-chanteurs se sont approprié le cyberespace et tout le monde peut être la cible de leurs actions.

L'explosion du phénomène d'usurpation d'identité depuis 2003 démontre ainsi que les criminels ont bien compris l'avantage qu'ils pouvaient tirer, non seulement des capacités d'anonymisation offertes par Internet, mais aussi de l'appropriation des fausses identités, afin de ne pas être poursuivis ou tenus responsables d'actions criminelles ou terroristes.

Comme tous les criminels qui profitent des infrastructures technologiques mises en place, les "blanchisseurs" de fonds recourent également de plus en plus à Internet, afin de pouvoir utiliser légalement des capitaux générés par des activités criminelles, telles que le trafic de drogue, la vente illégale d'armes, la corruption, le proxénétisme, la pédophilie, la fraude fiscale...

Bien qu'il soit largement sous-déclaré,

2 Phishing : utilisation de la messagerie électronique pour leurrer les internautes afin de les inciter à livrer eux-mêmes, sur un site web, leurs informations sensibles (identifiants, mots de passe, numéros de compte...) qui seront ensuite exploitées à des fins malveillantes.

et le plus souvent méconnu, ce blanchiment d'argent sale via Internet prend, lui aussi, de l'ampleur. Internet offre ainsi un potentiel exceptionnel tant par la dématérialisation (anonymat, monde virtuel, rapidité de transfert) que par la non-territorialité (phénomène transnational, conflits de compétences et de juridictions), caractéristiques largement exploitées par les acteurs traditionnels du blanchiment. Internet permet ainsi, en toute impunité, de réinsérer de l'argent sale dans les circuits économiques par le biais de transferts de flux, d'investissement et de capitalisation.

Les placements boursiers en ligne, les casinos en ligne, l'e-commerce, les ventes de produits et services fictifs contre des paiements réels, génèrent de nombreux bénéfices. De telles activités sont incontrôlables et les poursuites en justice impossibles. L'e-banking, les transactions du foncier et de l'immobilier via le net, la création de sociétés virtuelles "écran", les porte-monnaie électroniques sont aussi utilisés pour effectuer du blanchiment d'argent.

En ayant recours à certains services dématérialisés, l'internaute, peut ainsi sans le savoir favoriser le développement du blanchiment d'argent. Pire, les entreprises peuvent également être fortuitement impliquées dans ces processus et en subir des conséquences judiciaires et commerciales importantes.

Paradis numériques et réglementation internationale

Le fait de pouvoir localiser des serveurs dans des Etats faibles, qui constituent des refuges à des opérations transnationales, ainsi que le manque de régulation internationale et de contrôle d'Internet, offre une couche d'isolation protectrice aux criminels. Ceux-ci tirent ainsi partie de l'aterritorialité de l'Internet, de l'inexistence dans certains Etats de lois réprimant le crime informatique et des juridictions multiples dont relève le réseau des réseaux.

A l'instar des paradis fiscaux, il existe maintenant des paradis numériques, où un malfaiteur peut agir ou héberger des serveurs et des contenus illicites en toute impunité.

A l'heure actuelle, aucune réponse correcte, tant sur le plan juridique que technique, n'est apportée pour maîtriser ces différents délits favorisés par l'Internet.

Certes, une volonté réglementaire existe bien au niveau international. La première réglementation internationale, contribuant à appréhender la dimension internationale de la cybercriminalité, est la Convention sur la cyber-criminalité du Conseil de l'Europe (adoptée à Budapest en novembre 2001, entrée en vigueur en juillet 2004). Ce n'est donc pas forcément l'absence de Lois, ou de principes directeurs (Cf Lignes directrices de l'OCDE régissant la sécurité des systèmes et des réseaux - vers une culture de la sécurité - 2002) qui sont en cause. Ce sont la difficulté et la complexité des moyens à mettre en œuvre pour atteindre les objectifs de lutte contre la cybercrimnalité et le crime organisé, qui font que le cyber-risque informatique d'origine criminelle reste difficilement maîtrisable et que l'Internet est, du coup, très exploité à des fins malveillantes.

Une prise de conscience

La prise de conscience de la fragilité du monde numérique et cette non-maîtrise des technologies de l'information et des solutions de sécurité commercialisées devraient nous alerter sérieusement sur notre dépendance vis-à-vis de technologies que nous ne maîtrisons pas !

Le fait de pouvoir localiser des serveurs dans des Etats faibles offre une couche d'isolation protectrice aux criminels.

Il serait, dans ce domaine, illusoire de penser que des solutions d'ordre technologique ou juridique viendront suppléer les erreurs de conception et de gestion de l'informatique et des télécoms. Du coup, la vraie question consiste à savoir jusqu'où nous désirons être dépendant d'un fournisseur, d'un pays ou d'un administrateur. Combien d'entreprises ont, à leurs dépens, compris leur dépendance excessive vis-à-vis d'un fournisseur ou d'un administrateur système !

Ainsi, les premiers éléments de la maî-

trise du risque cybercriminel passent avant tout par :

• la redéfinition de notre relation aux nouvelles technologies et aux fournisseurs ;

• l'exigence d'une garantie de sécurité ;

• la responsabilité de l'ensemble des acteurs.

Avant de mettre en place des mesures classiques de sécurité par une démarche de prévention - protection - défense, protégeons les ressources sensibles ou critiques d'une organisation en repensant tout d'abord leur relation aux nouvelles technologies.

De plus, exigeons :

• des produits de qualité dont le niveau de sécurité puisse être contrôlable et vérifiable ;

• que la sécurité ne soit plus réalisée dans l'obscurité, qu'elle soit transparente ;

• que la sécurité ne relève plus uniquement de la responsabilité des utilisateurs, mais aussi de celle des intermédiaires techniques ;

• qu'un minimum de sécurité soit intégré en mode natif dans les solutions technologiques.

Revenir aux fondamentaux

Les événements qui marquent l'actualité et la recrudescence des cyberattaques ne modifient pas le champ d'application de la sécurité informatique. Il s'agit toujours d'assurer les mêmes critères de base : la disponibilité, la confidentialité, l'intégrité, la preuve, la non-répudiation, l'authenticité, qu'il s'agisse de données, de services, de transactions, d'infrastructures, de réseaux ou de systèmes. Seul le contexte d'application des technologies de la sécurité change et se complexifie.

La maîtrise des risques technologiques et informationnels passe donc nécessairement par une approche globale et cohérente de la sécurité. Il faut tenir compte de facteurs d'ordre humain, technologique, économique et juridique.

Les besoins de sécurité ne doivent pas faire d'Internet un territoire contrôlé à l'excès, car des dérives portant atteinte aux droits fondamentaux sont alors prévisibles.

Sans cette volonté d'intégrer dans une approche systémique, toutes les composantes d'une démarche sécuritaire, les solutions de sécurité ne pourront protéger correctement une informatique distribuée. Pour autant, les besoins de sécurité ne doivent pas faire d'Internet un territoire contrôlé à l'excès, car des dérives portant atteinte aux droits fondamentaux sont alors prévisibles. En fait, la sécurité, ici aussi, ne peut être que la résultante d'un compromis entre : besoins et solutions de sécurité, facilité d'utilisation et efficacité des solutions de sécurité, délais de disponibilité et coûts de développement et d'intégration des solutions, niveaux de sécurité et coûts des solutions. Ce compromis résultera nécessairement d'un choix consistant à privilégier un facteur au détriment des autres. L'équilibre entre les besoins de sécurité et les dimensions financières et humaines n'est pas évident : respect de l'intimité numérique des individus et possibilité de confondre et de poursuivre des criminels.

Ainsi, la maîtrise des risques technologiques ne se résume plus, loin s'en faut, à la chasse aux hackers, ni à la mise en place de barrières technologiques comme des systèmes pare-feu (firewall). La diffusion d'une certaine culture et d'une approche pluridisciplinaire de la sécurité et de la maîtrise du risque informatique est obligatoire.

Pour les organisations et les Etats, posséder une vision stratégique de ces problématiques est devenu une nécessité. En effet, la dépendance aux technologies de traitement de l'information associée à l'interdépendance des infrastructures ainsi que la vulnérabilité des systèmes informatiques, ne peuvent plus être ignorées. Les organisations, et plus globalement la société, doivent se doter de mesures, procédures et outils qui autorisent une gestion efficace des risques technologique et informationnel.

Paradoxalement, les ressources disponibles en matière de sécurité ne manquent pas, et le marché de la sécurité est en pleine expansion. Mais ces ressources sont-elles pour autant adaptées aux besoins, implantées et gérées correctement ? Cela n'est pas certain, d'autant qu'elles s'appliquent à un environnement en perpétuelle mutation, qui comporte aussi une dimension humaine difficilement contrôlable.

On le sait, les dégâts les plus graves ont parfois pour origine une simple négligence, qui peut relever : de l'incompétence des acteurs, de défaillances lors de la conception ou de la mise en œuvre des technologies, des pouvoirs excessifs accordés aux administrateurs systèmes, d'une gestion défectueuse, etc.

Protection et gestion du risque

Les organisations ne peuvent plus négliger les dangers réels qui les menacent et ont un véritable devoir de protection de leurs infrastructures, de leurs flux, de leurs secrets industriels et commerciaux, de leur argent. Elles doivent dès à présent se préparer à la menace cybercriminelle qui un jour ou l'autre se concrétisera.

Aujourd'hui, la plupart des grandes organisations répondent au besoin de maîtrise des risques par l'intégration dans leur management, de la notion de "gouvernement" de la sécurité. Le plus souvent, un responsable de la sécurité, aux fonctions et missions déterminées, doté de moyens d'action, concrétise la volonté directoriale de maîtriser le risque informatique.

Mais la gestion des risques n'est pas seulement l'affaire d'un spécialiste. Elle nécessite l'implication de tous les acteurs de l'organisation et repose : sur la connaissance et la compréhension, la responsabilisation, la capacité à formuler des analyses de risques et à mettre en place des mesures efficaces.Une véritable doctrine de sécurité doit être développée afin d'assurer la sécurité, l'intelligence économique, la veille et la conformité juridique. Il s'agit d'organiser la protection et la défense des valeurs en prenant en considération la menace du risque criminel dans la stratégie d'entreprise.

Bien sûr, il est souvent difficile d'identifier les acteurs de la cybercriminalité, leurs modalités d'action et leur motivation. Mais nous savons par contre que les organisations criminelles agissent généralement de manière opportuniste et s'attaquent plus volontiers aux acteurs vulnérables.

Ne pas devenir une cible prioritaire de la cybercriminalité est possible dans la mesure ou l'organisation protégera efficacement (c'est-à-dire mieux que les autres) son infrastructure informatique et sortira de la logique ou la mise en place de la sécurité se limite à avoir le même niveau d'insécurité que ses concurrents. Le risque cybercriminel est alors transformé en levier pour réaliser une sécurité de qualité.

En revanche si l'organisation est considérée, par les acteurs classiques de la criminalité, comme étant une source de richesse ou un symbole à détruire, elle sera l'objet d'attaques ciblées. La destruction par des actes terroristes est alors à craindre.

Une stratégie de protection et de défense appropriées doit alors être mise en place, sans illusion. Car les outils classiques de l'assurance et de la gestion de risques sont de peu d'efficacité devant le risque d'origine criminelle qui ne peut totalement être évité à moins de ne pas être connecté à Internet.

Pour autant, les entreprises doivent être rentables et compenser le manque à gagner engendré par le risque cybercriminel et le coût des mesures à mettre en place pour le maîtriser. Un modèle économique doit donc être pensé pour supporter de manière optimale le coût de la protection des infrastructures, de la sécurité des systèmes, réseaux, données et services.

Ne pas devenir une cible prioritaire de la cybercriminalité est possible

Face à la synergie et à la convergence du crime organisé, du crime économique et du cybercrime, une réponse complète, multilatérale et transnationale est à apporter.

Il est donc important de sensibiliser l'ensemble des acteurs du monde de l'Internet aux enjeux de la maîtrise de la sécurité et aux mesures élémentaires qui, si elles sont clairement énoncées, définies et mises en œuvre intelligemment, renforceront la confiance des utilisateurs envers les technologies de l'information et diminueront les opportunités criminelles.

Référence

Les Universités de Lausanne, Genève et Neuchâtel offrent un programme de formation continue de longue durée en Management et ingénierie de la sécurité informatique.