SÉLECTION

L'économie souterraine induite du cybercrime

SOLANGE GHERNAOUTI-HÉLIE

«La majorité des acteurs Internet sont à la fois victimes et bénéficiaires de la cybercriminalité»

La criminalité par Internet touche la société, les individus, les organisations, les Etats, par manipulations d'opinion, espionnage, terrorisme, harcèlement, escroqueries et fraudes financières. Dans son ouvre «La cybercriminalité. Le visible et l'invisible», Solange Ghernaouti-Hélie, professeure à HEC Lausanne et à l'Université de Genève, experte internationale en sécurité, identifie les motivations et méthodes des criminels qui ont pénétré l'espace virtuel. Du panorama des risques, dans l'activité quotidienne des internautes, le livre passe aux guerres de l'information et aux attaques majeures sur le Net. Le propos s'élève par des réflexions sur le numérique dans la société contemporaine et pose des questions fondamentales. Qui est finalement responsable de la sécurité informatique? Qui contrôle tout le système? Que peut faire l'individu pour que sa dignité et les données intimes sur sa vie soient protégées?

De nos jours, les virus se professionnalisent et sont des vecteurs de la criminalité économique, contribuant à réaliser des profits. Quelle que soit la charge de nocivité véhiculée par les programmes malveillants, ils sont désormais orientés vers la recherche de gains financiers. Ils sont terriblement sophistiqués, de moins en moins visibles, de plus en plus profitables et difficilement détectables. Les réseaux constitués de machines «zombies», infectées par un programme malveillant et pilotées à distance par un pirate, sont des botnets. Ils contribuent à la diffusion du spam et en même temps, les botnets s'étendent grâce au spam. (...)
La production et la diffusion de programmes malveillants (malware ou maliciels: virus, cheval de Troie, porte dérobée (backdoor), renifleur de clavier, botnets, etc.) ainsi que les outils de piratage, autorisent le développement d'une véritable économie souterraine autour d'un marché très profitable. Cela contribue simultanément à alimenter la chaîne de valeurs liées aux technologies de l'information pour les entreprises licites. Citons deux exemples. Le marché des virus, porté par le monde criminel, favorise celui des antivirus. Il profite à l'enrichissement des fournisseurs et vendeurs d'antivirus et conseillers en sécurité qui, eux, réalisent des affaires en toute légalité. Le spam quant à lui, contribue à la profitabilité des:
- fournisseurs de solutions antispam;
- fournisseurs d'accès Internet;
- opérateurs de télécommunication;
- entreprises qui utilisent le spam comme outils de marketing et de publicité que certains considèrent comme agressive sans pour autant être illégale, mais auxquelles les internautes se sont adressés pour réaliser un achat suite à un message de spam reçu ;
- entités illégales qui ont, par le spam, pris le contrôle de la machine de l'utilisateur, installé des programmes malveillants, dérobé des données personnelles, usurpé l'identité de l'internaute pour réaliser d'autres méfaits, etc.

Il existe un véritable paradoxe dans la mesure où la majorité des acteurs de la chaîne Internet peuvent profiter, à divers degrés, des flux malveillants tout en étant victimes de la criminalité.
Force est de constater que la cybercriminalité peut générer des coûts et être une source de bénéfices pour certaines entreprises tout à fait légales. Ainsi, la cybercriminalité qu'elle passe par la diffusion de programmes malveillants ou l'introduction non autorisée dans des ordinateurs, par des attaques visant à nuire à la concurrence ou par de l'espionnage économique, entraîne des coûts de protection, de réaction et de répression. Cela développe une véritable économie autour:
- du conseil en sécurité, du conseil juridique;
- de l'audit et de l'évaluation de la sécurité informatique;
- du développement et de la vente de solutions de sécurité (matériels, logiciels spécialisés, détection d'intrusion, système pare-feu (firewall), tests de pénétration, chiffrement, etc.);
- du développement et de la vente de solutions, matériels, logiciels spécialisés en matière d'investigation informatique (outil de surveillance, de collecte et d'analyse de traces numériques, etc.);
- de la formation en sécurité, en droit, en sciences criminelles;
- de la recherche publique et privée dans des disciplines comme celles précédemment citées mais aussi en sciences humaines et sociales ou en informatique par exemple.

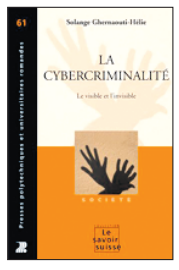
Sans évoquer la médiatisation des affaires cybercriminelles et la récupération politique pour alimenter le discours de l'insécurité et favoriser l'adoption de nouveaux textes de lois ou des techniques et des procédures de surveillance et de contrôle, force est de constater qu'une économie légale de l'insécurité et de la sécurité informatique existe et profite

> LA PRODUCTION ET LA DIFFUSION DE PROGRAMMES MALVEILLANTS ET LES OUTILS DE PIRATAGE AUTORISENT LE DÉVELOPPEMENT D'UNE VÉRITABLE ÉCONOMIE SOUTERRAINE AUTOUR D'UN MARCHÉ TRÈS PROFITABLE. CELA CONTRIBUE À ALIMENTER LA CHAÎNE DE VALEURS LIÉES AUX TECHNOLOGIES DE L'INFORMATION POUR LES ENTREPRISES LICITES.

à certains acteurs. Elle répond à l'économie souterraine de la cybercriminalité qui enrichit des entités au détriment de la société tout entière. En effet, les coûts engendrés par la cybercriminalité, qu'ils soient directement liés au fonctionnement des instances de justice et police ou qu'ils soient indirects du fait de la défiance des acteurs et des dysfonctionnements des organisations victimes, par exemple, sont supportés par la société.
Ceux qui créent des programmes malveillants, ceux qui les diffusent, les vendent ou les mettent en œuvre, sont extrêmement bien organisés. En effet, ils sont le plus souvent hyperspécialisés. De plus, la répartition des tâches et des risques ainsi que la distribution des responsabilités criminelles sont tellement efficaces, qu'il devient difficile, voire impossible, d'identifier et de localiser un criminel lorsqu'un acte illégal est observé. L'organisation du travail est en effet suffisamment optimisée en fonction de tâches spécifiques (création de logiciels malveillants, location ou vente de botnets, usurpation d'identité ou création de fausses identités, ventes d'identités usurpées ou de fausses identités, vols de numéros de cartes de crédits, fabrication de fausses cartes de crédits, vente, diffusion du spam, intermédiaires de toutes sortes, etc.), pour que le monde criminel soit efficace et efficient tout en étant extrêmement dynamique, mobile et flexible, pour s'adapter rapidement aux cibles et échapper aux contre-attaques et investigations policières.
Le risque criminel possède une dimension globale qui touche dans son intégralité une organisation (actionnaires, dirigeants, personnel, outil de production, etc.). Celle-ci doit savoir préserver son intégrité face au risque criminel, comme elle se protège d'ailleurs des risques de corruption par exemple. Elle doit être rentable et compenser le manque à gagner engendré par le risque cybercriminel par le coût des mesures à mettre en place pour le maîtriser. Un modèle économique doit alors être pensé pour supporter de manière optimale le coût de la protection des infrastructures, de la sécurité des systèmes, réseaux, données, services et personnes, bref de tout ce qui constitue le patrimoine de l'entreprise ou d'une administration. Ce modèle, qui a inévitablement un impact sur le coût de production, veillera à préserver le développement de l'activité, par une redistribution des valeurs créées par l'organisation.
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 et de leur trésorerie. Elles doivent se préparer à la menace cybercriminelle qui un jour ou l'autre se concrétisera.
La diffusion d'une certaine culture et d'une approche pluridisciplinaire de la sécurité et de la maîtrise du risque informatique d'origine criminelle est obligatoire. En effet, pour les organisations comme pour les Etats, leur dépendance aux technologies de traitement de l'information associée à l'interdépendance des infrastructures ainsi qu'à la vulnérabilité des systèmes informatiques, requiert une vision stratégique et globale de cette problématique. Les organisations et plus largement la société, doivent se doter de mesures, procédures et outils qui permettent une gestion efficace des risques technologique et informationnel.
Les ressources disponibles en matière de sécurité ne manquent pas. Le marché de la sécurité se porte plutôt bien, il est en pleine expansion. Mais les offres sont-elles pour autant adaptées aux besoins ? Sont-elles implantées et gérées correctement ? Ce n'est pas certain, d'autant qu'elles s'appliquent à un environnement en perpétuelle mutation, qui comporte une dimension humaine difficilement contrôlable. Les dégâts les plus graves ont parfois pour origine par exemple, une gestion défectueuse, une simple négligence (le mot de passe est sur un post-it collé dans un coin de l'écran), l'incompétence (erreurs lors de la conception ou de la mise en œuvre des technologies) ou encore l'attribution de pouvoirs excessifs accordés à des administrateurs système. De plus, une entité commerciale (fournisseurs, distributeurs, etc.) évitera d'avoir à supporter le coût de la sécurité. Il est en effet plus rentable, pour certains acteurs économiques qui ne sont pas contraints par la loi de fournir des solutions sécurisées, que les coûts soient imputés aux consommateurs (achats supplémentaires de produits, frais de formation, remplacement du matériel infecté, etc.) ou à la société. C'est notamment le cas lorsqu'une entreprise licencie des personnes suite à sa mise en faillite du fait d'un défaut de sécurité ou d'une attaque informatique.
Au-delà du discours politiquement correct que constitue l'engagement du secteur privé à lutter contre la cybercriminalité, allant jusqu'à l'octroi de primes parfois faramineuses pour inciter à livrer des informations permettant de capturer un cybercriminel (notion de cyberfar-west), ces mêmes acteurs continuent à commercialiser des solutions informatiques comportant des failles de sécurité. De plus, les solutions de sécurité elles mêmes, puisqu'elles sont aussi informatiques, n'ont pas de solidité garantie et sont porteuses de vulnérabilités exploitables. (…)
Dans la mesure où Internet est devenu, à juste titre ou non, un élément incontournable de l'économie nationale voire planétaire, ne constitue-t-il pas une infrastructure critique, au même titre que le sont les systèmes de distribution électrique? En effet, la capacité des entreprises à produire de la richesse et à développer des services est de plus en plus liée aux technologies et services de l'Internet.
Par ailleurs, les infrastructures informatiques et de télécommunications appartiennent de manière que très partielle à ceux qui en dépendent. Même les infrastructures dites publiques appartiennent pour une large part à des sociétés privées. Dans ce contexte de dépendance et d'interdépendance des infrastructures informatiques et électriques, des infrastructures privées et publiques, qui est donc responsable de la sécurité? Est-il plus judicieux de parler de sécurité informatique ou de sécurité des infrastructures critiques? Est-ce uniquement une question de terminologie ou s'agit-il d'un déplacement des enjeux, du marché et du champ d'application de la sécurité? Difficile en premier lieu de répondre et d'identifier dans ce glissement sémantique les défis que doivent relever les dirigeants en matière de sécurité et de maîtrise des risques informatiques. La tentation est grande de changer l'objet de l'étude sans pour autant répondre à la question fondamentale inhérente à toute démarche sécurité, à savoir : qui contrôle la sécurité?
Cette question nécessite d'apporter entre autres des réponses concrètes aux interrogations suivantes : Comment garantir la sécurité? Quelle confiance accorder à des outils et services de sécurité produits par des tiers? Comment couvrir le risque informatique par une assurance? Quels sont les outils, méthodologies et compétences nécessaires à l'appréciation du risque informatique afin de mettre en place des mesures efficaces et cohérentes de sécurité qui permettent de le maîtriser ou de transformer ce risque en opportunité d'affaires? Autant de questions ouvertes qui dépassent la dimension purement technologique d'Internet et de sa sécurité. Elles méritent un véritable débat de société. (...)

> UN MODÈLE ÉCONOMIQUE DOIT ÊTRE PENSÉ POUR SUPPORTER DE MANIÈRE OPTIMALE LE COÛT DE LA PROTECTION DES INFRASTRUCTURES, DE LA SÉCURITÉ DES SYSTÈMES, RÉSEAUX, DONNÉES, SERVICES ET PERSONNES. BREF DE TOUT CE QUI CONSTITUE LE PATRIMOINE DE L'ENTREPRISE OU D'UNE ADMINISTRATION.

Solange Ghernaouti-Hélie est docteure en informatique de l'Université Paris VI. Professeur à l'Ecole des HEC de Lausanne, elle est également professeur invité au département de sociologie de l'Université de Genève pour un cours de Master «Internet et Société». Experte en sécurité du numérique auprès d'instances onusiennes, gouvernementales et institutions privées, elle est l'auteure d'une vingtaine d'ouvrages.Elle donnera le 3 décembre une conférence «Le défi de la protection des droits de l'Homme et du citoyen dans un contexte de filature numérique et de sécurité informatique globalisée». Uni de Lausanne, bâtiment Internef, auditoire 27, dès 14h30. Infos: www.hec.unil.ch/sgh



SOLANGE GHERNAOUTI-HÉLIE
«La cybercriminalité. Le visible et l'invisible»
Presses polytechniques et universitaires romandes», vol 61, automne 2009, 128 pages.

TOP 5 DES VENTES ÉCONOMIE-FINANCE

PAYOT LIBRAIRE

Cinq meilleures ventes de la semaine dernière dans l'ensemble du réseau

1. **Survivre aux crises**
   J. Attali
   Fayard
2. **La face cachée des banques**
   E. Laurent
   Plon
3. **La prospérité du vice: une introduction (inquiète) à l'économie**
   D. Cohen
   Albin Michel/Documents
4. **Confessions d'un banquier pourri**
   Crésus (Pseudo)
   Le Livre de Poche
4. **UBS: les dessous d'un scandale**
   M. Zaki
   Favre