SWISS ENGINEERING
Revue Technique Suisse RTS

Cybercriminalité – le vol organisé

L'UNIL offre des conseils stratégiques et des formations en cybersécurité

N° 3 · Mars 2015 · 31ème année · CHF 8.–

www.swissengineering-rts.ch

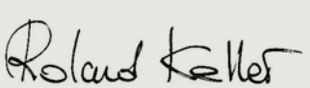
EN COUVERTURE L'époque où les jeunes passionnés d'informatique tentaient désespérément de s'infiltrer via l'internet dans les serveurs vulnérables est bien loin. Aujourd'hui, la cybercriminalité est devenue un métier à part entière.

Roland Keller
Rédacteur responsable
SWISS ENGINEERING
Revue Technique Suisse RTS

Le taux plancher des vaches

Après la décision de la BNS d'abandonner le cours du plancher de l'euro, la nouvelle a eu l'effet d'une bombe dans les milieux économiques. On a même parlé de tsunami financier. Dans l'édition de l'hebdomadaire La Semaine qui a suivi la nouvelle, Rolf Muster, directeur de Schaublin Machines SA, s'est insurgé contre la passivité des politiciens de haut rang en clamant haut et fort que le Conseil fédéral n'est pas digne du peuple suisse. « Personne ne semble véritablement se rendre compte de la gravité de la situation », a-t-il déclaré. Si l'on peut comprendre sa réaction, comme celle de l'institut de recherches conjoncturelles zurichois KOF qui s'attend à voir à une courte récession et une hausse du chômage, on peut aussi adhérer au fait que notre banque centrale n'avait pas le choix.

Le franc suisse continuellement scotché à 1 franc 20 à l'euro n'aurait pas pu se démarquer de son plancher des vaches si envié de notre entourage, d'autant plus qu'entre-temps le dollar à la hausse est venu rééquilibrer la donne sur le marché. Alors, est-ce une aussi grande catastrophe qu'on veut bien nous le faire croire ?



123RF.com

L'hameçonnage, phishing ou filoutage est une technique utilisée par des fraudeurs pour obtenir des renseignements personnels dans le but de perpétrer une usurpation d'identité. Les cyber-criminels ont de plus en plus d'astuces pour nous tromper. On s'y laisserait vite prendre.

La confiance ébranlée

Menacé récemment par un « cybercalifat » se revendiquant proche de l'organisation Etat islamique, le président américain Barack Obama a fait appel aux geeks lors d'un sommet sur la cybersécurité à Palo Alto (Californie). Un peu dépassés par les événements, les politiques ne savent plus à quel saint se vouer. On les comprend … Nous aussi sommes parfois embarrassés, ne serait-ce qu'avec les usurpations d'identité.

Selon Solange Ghernaouti, les origines de la cybercriminalité sont à trouver dans l'usage à des fins criminelles des technologies de l'information et de la communication, notamment Internet. Les criminels ont très rapidement compris la profitabilité qu'ils pouvaient tirer d'Internet pour réaliser leurs actions criminelles traditionnelles (crime économique, escroqueries, trafics de stupéfiants, traite d'êtres humains, espionnage, blanchiment d'argent, etc.). Tous les délits classiques peuvent être optimisés via les technologies du numérique, qui étendent le champ de la criminalité en offrant la possibilité de réaliser de nouveaux délits tels que le vol, la détérioration de ressources informatiques, l'intrusion dans des systèmes informatiques, l'usurpation d'identité numérique, etc. La cybercriminalité est un prolongement de la criminalité classique au travers du cyberspace, ce dernier constituant depuis son origine, un champ d'actions et une source additionnelle d'opportunités criminelles.
C'est en 1983 que l'OCDE (Organisation de coopération et de développement économiques) donne la première définition de la notion d'infraction informatique et c'est en particulier la Convention Européenne sur la Cybercriminalité qui, en 2001, a largement contribué à faire connaitre ce terme reflétant une réalité bien plus ancienne mais méconnue.

Un métier à part entière

Depuis la diffusion sur la toile de nouveaux services et outils internet destinés à une population mondiale favorable à leur utilisation ainsi que la globalisation des réseaux, les infractions pénales sur internet se sont rapidement accrues. L'époque où les jeunes passionnés d'informatique tentaient désespérément de s'infiltrer via l'internet dans les serveurs vulnérables est bien loin. Aujourd'hui, la cybercriminalité est devenue un métier à part entière.
En cette période de crise affectant le système économique mondial, les attaques cybercriminelles ne cessent de croitre. Les entreprises victimes affirment que ces attaques causent une baisse de croissance et de compétitivité. En effet, elles ont pour conséquence une perte de confiance de la part des partenaires et des clients, pouvant entraîner jusqu'à la réduction à moyen terme des effectifs. « Face à de tels dangers, les actions de lutte contre cette tendance se multiplient mais les spécialistes sont encore loin de pouvoir l'éradiquer ou de réduire le taux d'infractions criminelles perpétrées », estime le site internet Anti-cybercriminalite.fr
Selon cette plateforme, il existe plusieurs obstacles juridiques et non-juridiques à la lutte contre le phénomène de la cybercriminalité. Tout d'abord, il faut tenir en compte l'ampleur des réseaux informatiques, la rapidité de la réalisation des infractions et la complexité des enquêtes judiciaires (rassemblement de preuves, investigations…). Sur le plan juridique, la cybercriminalité n'est pas encore considérée comme une infraction dans nombreux pays, ce qui rend difficile sa poursuite par les divers organes de lutte.

> Dans nombreux pays, la cybercriminalité n'est pas encore considérée comme une infraction, ce qui rend difficile sa poursuite par les divers organes de lutte

Lausanne : timides conseils

Sur son site web, la ville de Lausanne (www.lausanne.ch) consacre une page à ce sujet en insistant notamment sur la pédopornographie et les piratages de cartes bancaires. La prévention étant bonne conseillère, Lausanne.ch fournit quelques recommandations et règles élémentaires en cas d'agression, par exemple : ne pas hésiter à annoncer un tel cas à la police, conserver les emails et surtout ne pas donner suite à ceux-ci.
Selon le très sérieux magazine Slate.fr, « il y aurait seulement environ une centaine de criminels purs et durs derrière la cybercriminalité sur l'ensemble de la planète, expliquait récemment à la BBC Troels Oerting, le chef du centre d'Europol sur la cybercriminalité ».
Selon ce dernier, « il ne s'agit pas d'un nombre fixe et il va malheureusement augmenter. Nous pouvons encore faire face, mais les criminels ont plus de ressources et ne rencontrent pas d'obstacles. Ils sont menés par l'appât du gain et produisent des programmes de virus et de chevaux de Troie avec une rapidité que nous avons du mal à suivre ».
Mais le phénomène a pris une telle ampleur ces derniers jours que le président Barack Obama a récemment demandé l'aide de la Silicon Valley. Un peu dépassés par les événements, les politiques font ainsi appel aux geeks. Menacé récemment par un « cybercalifat » se revendiquant proche de l'organisation Etat islamique, le président américain a exhorté la Silicon Valley – lors d'un sommet sur la cybersécurité à Palo Alto (Californie) – à coopérer avec les autorités fédérales pour protéger les Etats-Unis des menaces terroristes, pirates informatiques et espions. « Cela doit forcément être une mission conjointe », a lancé Obama devant un millier de personnes issues des entreprises du secteur, d'universités, d'associations de défense des libertés sur internet et des forces de l'ordre.

MELANI et SCOCI veillent

Mais dans un récent rapport publié par la société spécialisée Kaspersky Lab, une vague de cyberattaques d'un genre nouveau vise depuis 2013 des banques mondiales, dont des russes – et au moins une suisse.
Comme la Centrale suisse d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) n'en a pas eu connaissance, c'est le Service national de coordination de la lutte contre la criminalité sur Internet (SCOCI) qui a pris la relève de l'enquête. Ce centre de compétence pour le public, les administrations et les fournisseurs d'accès Internet offre des services juridique pour toutes questions relatives à la criminalité sur Internet. En sa qualité de service national de coordination, le SCOCI se définit aussi comme un interlocuteur privilégié pour les services étrangers qui exercent la même fonction. Normal, la cybercriminalité n'a pas de frontières. (rke)

Le visible et l'invisible de la criminalité numérique

Chaque technologie est porteuse de potentialités criminelles. Les vulnérabilités techniques, organisationnelles, juridiques comme la maîtrise insuffisante des technologies, le sentiment des criminels de pouvoir agir en toute impunité, sont des composantes de l'insécurité générée par l'usage extensif des technologies du numérique. Solange Ghernaouti décortique pour nous les tenants et aboutissants de ce nouveau phénomène de société.

Avec Internet, le crime économique n'est pas uniquement réservé à la criminalité organisée car les outils informatiques et télécoms le mettent à la portée d'individus isolés, qui peuvent se constituer ou non en groupes plus ou moins importants.

Quelles sont les motivations et les méthodes des criminels qui pénètrent l'espace virtuel ?
Caché derrière un écran et agissant à distance à travers de multiples intermédiaires technique, le criminel est le plus souvent mu par un besoin d'enrichissement, par un désir de nuisance, de déstabilisation, de prise de pouvoir ou encore de reconnaissance ou de divertissement
Il est parfois difficile de deviner la motivation des auteurs qui se cachent derrière une cyberattaque s'ils ne la revendiquent pas eux-mêmes. Certains sont de véritables criminels à la recherche de profits, d'autres trouvent leur motivation dans des revendications politiques ou religieuses, d'autres enfin voient dans la cybercriminalité le moyen de travailler, de s'exprimer, d'exister, d'apprendre…
Avec Internet, le crime économique n'est pas uniquement réservé à la criminalité organisée car les outils informatiques et télécoms le mettent à la portée d'individus isolés, qui peuvent se constituer ou non en groupe plus ou moins important.

Quelles sont les principales attaques majeures sur le Net ?
Difficile de répondre à cette question sans définir par ce que l'on entend par majeures. S'agit il de l'amplitude, du nombre de victimes, des impacts, du nombre d'attaques, de celles qui induisent des morts, qui portent atteinte au fonctionnement des infrastructures critiques d'un pays ?

L'ère du numérique dans la société contemporaine a-t-elle accru la criminalité ?
Chaque technologie est porteuse de potentialités criminelles et offre des opportunités pour réaliser des activités illicites. Internet et le cyberespace n'échappent pas à cette règle et le monde criminel a investi celui des ordinateurs et des réseaux pour réaliser des profits tout en prenant un minimum de risques.
Les vulnérabilités techniques, organisationnelles, juridiques comme la maîtrise insuffisante des technologies, le sentiment

des criminels de pouvoir agir en toute impunité sont des composantes de l'insécurité générée par l'usage extensif des technologies du numérique. Cela constitue de nouvelles menaces souvent invisibles mais redoutables, car susceptibles de frapper n'importe quel système informatique, n'importe quelle organisation, n'importe quel pays, n'importe quand. En fait, plus un pays est connecté, plus son taux de pénétration de l'Internet est élevé, plus il est dépendant de l'informatique et des télécoms, plus il est vulnérable à la cybercriminalité. Le risque informatique d'origine criminel est un risque structurel et omniprésent.

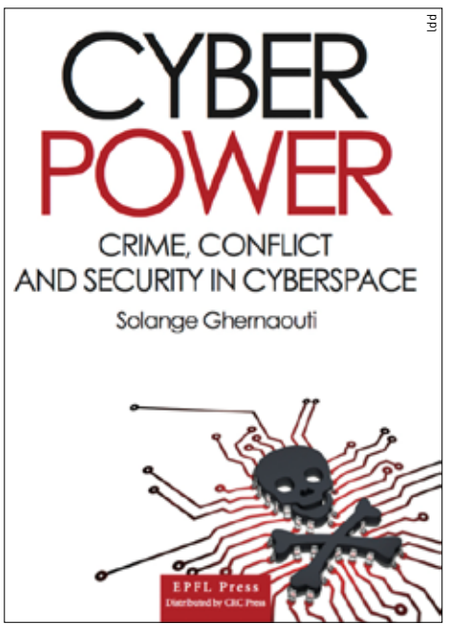
Quels sont les moyens de la police helvétique – romande en particulier – pour repérer et pister les cybercriminels ?
Les moyens sont largement insuffisants au regard de la réalité criminelle à laquelle sont confrontées la population et les entreprises. Une majorité ne sait pas comment et à qui dénoncer un cybercrime. En fait, il faut aussi mettre en place des mesures efficaces de prévention, d'accompagnement des victimes et de répression du cybercrime.
Faute de ressources, de compétences et d'organisation ad hoc des services de police et justice aux niveaux cantonal et fédéral, seule une poignée de cas dénoncés font l'objet d'une investigation, et peu sont résolus.

Qui doit être responsable de la sécurité informatique dans une entreprise afin d'être protégé avec efficience ?
Il est difficile de répondre catégoriquement à cette question, car cela dépend fortement de l'entreprise, de son secteur d'activité, de sa taille, de son niveau de maturité par rapport à l'appréciation des risques cybernétiques. De manière générale, une personne connaissant bien les valeurs à protéger et le fonctionnement de son entreprise, ayant la confiance et le soutien de sa direction générale, étant bon gestionnaire avec le sens du dialogue et pouvant s'appuyer sur des collaborateurs disposant de compétences légales et techniques… cette personne-là est un élément clé de la définition de la politique de sécurité et de sa mise en œuvre opérationnelle.

Jusqu'à quand les criminels pourront-ils user du monde cybernétique ? Celui-ci sera-t-il toujours un Eldorado pour eux ou un phénomène de société indélébile ?
Tant que le monde cyber leur offrira une couche d'isolation protectrice, une source d'enrichissement, des cibles et des victimes potentielles facilement attaquables… La complexité, le coût et le retard pris dans la lutte contre la cybercriminalité associés à l'ingéniosité des criminels, à l'emprise de la criminalité organisée sur nos sociétés connectés et aux moyens dont elle dispose, le fait que nos infrastructures sont toujours trop vulnérables, qu'aucune entité ne veut supporter le coût de la sécurité et le défaut de responsabilité de certains acteurs font que la cybercriminalité est structurellement et intrinsèquement liée au développement de nos activités numériques.

> « Faute de ressources, de compétences et d'organisation ad hoc des services de police et justice aux niveaux cantonal et fédéral, seule une poignée de cas dénoncés font l'objet d'une investigation, et peu sont résolus » Solange Ghernaouti

Et vous ? Avez-vous déjà été piratée ?
Non, espérons que cela sera toujours le cas à l'avenir ! Je suis bien consciente que je ne suis pas à l'abri de malveillance, ni d'une défaillance technique ou de celle d'un fournisseur de services dont je dépends. Tout environnement, toute technologie sont porteurs d'opportunités criminelles et nous pouvons tous être la cible de cyberagressions.



ppl

Cyber Power, par Solange Ghernaouti aux éditions www.ppur.org

Interview : Roland Keller
Rédacteur responsable
SWISS ENGINEERING RTS

regard sur

Solange Ghernaouti

Solange Ghernaouti est professeure à l'Université de Lausanne, directrice de recherche du Swiss Cybersecurity Advisory and Research Group. Avant d'intégrer le monde académique, elle a travaillé en France en tant qu'architecte de réseaux, experte en normalisation internationale (Groupe Bull) et cheffe de produit marketing (Rank Xerox). Titulaire d'un doctorat en informatique et télécommunication de l'Université Paris VI, ancienne auditrice de l'Institut des Hautes Etudes de Défense Nationale.
Experte internationale en cybersécurité et cyberdéfense auprès d'instances onusiennes, gouvernementales et d'institutions privées, Solange Ghernaouti est une conférencière très sollicitée tant en Suisse qu'à l'international. Elle publie de nombreux articles scientifiques et de vulgarisation, et intervient régulièrement dans les médias sur des questions de gestion de risques et de crises, de gouvernance, de stratégie, de lutte contre la cybercriminalité ou de cyberdéfense. Elle est l'auteure d'une trentaine de livres écrits en français ou en anglais – certains ayant été traduits en plusieurs langues dont l'arabe, le chinois, le russe et l'espagnol, « Cyberpower : crime, conflict and security in cyberspace », EPFL Press 2013 ; « Sécurité informatique et réseaux: cours et exercices corrigés», Dunod 2014 ; « La cybercriminalité: le visible et l'invisibles», Le Savoir suisse, 2009.
Ses distinctions :

- Chevalier de la Légion d'Honneur
- Membre de l'Académie Suisse des Sciences Techniques
- Classée par la presse suisse parmi Les 20 femmes qui font la Suisse (Bilan 2012), Les 100 femmes les plus puissantes de Suisse (Women in Businnes 2012), Les 300 personnalités les plus influentes de Suisse (Bilan 2011) et Les 100 personnalités qui font la Suisse romande (L'Hebdo 2011).

Les moyens politiques pour dissuader les cybercriminels

La Faculté des Hautes écoles commerciales (HEC) de l'UNIL dispose du Swiss Cybersecurity Advisory & Research Group créé et dirigé par Solange Ghernaouti. S'il contribue à l'enseignement et à la recherche dans le domaine de la sécurité de l'information, les moyens réels mis en place pour lutter dans le domaine de la cybercriminalité sont plutôt dérisoires dans notre pays.

Dissuader les criminels c'est leur faire prendre davantage de risques d'être identifiés et poursuivis, leur faire comprendre qu'ils ne peuvent plus agir en toute impunité.

Les moyens et les recherches dans le domaine de la lutte contre la cybercriminalité sont plutôt dérisoires dans notre pays. Néanmoins, la Faculté des HEC de l'UNIL, grâce au Swiss Cybersecurity Advisory & Research Group créé et dirigé par Solange Ghernaouti, contribue à l'enseignement et à la recherche dans le domaine de la sécurité de l'information. Première femme professeure de la Faculté des HEC en 1987, elle fut une pionnière en matière d'approche interdisciplinaire de la maîtrise des risques, de la sécurité et de la criminalité, liés aux technologies de l'information, pour répondre aux besoins des états, des organisations et des individus. Ses travaux de recherche s'inscrivent dans un cadre de réflexion systémique et global qui intègre les dimensions politique, socio-économique, humaine, juridique, managériale et technologique de la cybersécurité et de la lutte contre la cybercriminalité.

A ce jour, il n'existe pas, au sein de la Faculté ou de l'UNIL, de soutien particulier aux activités de recherche dédiées à la cybersécurité et à la lutte contre la cybercriminalité, ce qui semble être aussi le cas au national. Solange Ghernaouti considère que c'est un frein majeur au développement des ressources nécessaires à la Suisse pour la mise en œuvre de stratégies de cybersécurité et de politiques de lutte contre la cybercriminalité: « Je pallie à ce manque de moyens institutionnels et aussi pour être en phase avec la réalité du terrain, en collaborant directement avec des instances de justice et police au niveau national et international, et en participant à des projets de recherche européens comme E-Crime, dont un des partenaires est Interpol, qui étudie les impacts économiques de la cybercriminalité ».

> « Il est impératif de développer les capacités techniques, organisationnelles et humaines des instances dédiées à la lutte contre la cybercriminalité » Solange Ghernaouti

Pas de politique de sensibilisation

Solange Ghernaouti regrette le manque de politique nationale de la recherche en matière de sécurité informatique, de cybersécurité et de cyberdéfense, soutendue par une politique industrielle cohérente de soutien aux entreprises qui innovent dans ces domaines. Elle constate le défaut d'existence d'une politique de sensibilisation de tous les acteurs de notre société. « Cela comprend notamment toutes les couches de la population, du plus jeune au plus âgé, tous les acteurs, sans oublier les dirigeants politiques et économiques, les personnes en charge du système de justice et police, mais aussi celle d'une politique de formation relative aux risques et à la cybersécurité à tous les niveaux d'enseignement (école, collège, gymnase, université, formation continue) et ce, quelles que soient les disciplines enseignées (médecine, droit, sciences sociales, etc.) ».

Pour elle, nos dirigeants politiques doivent comprendre que la cybercriminalité est un fléau de société et qu'il est urgent d'agir pour tenter de freiner l'expansion de la cybercriminalité et protéger notre économie ainsi que la population. « Il faut limiter les pertes économiques, voire les pertes d'emploi consécutives à l'affaiblissement ou la perte de compétitivité économique des entreprises piratées et limiter également la montée en puissance des acteurs criminels, diminuer le nombre de victimes. Et surtout faire respecter notre état de droit, protéger et faire prospérer nos biens et nos valeurs », insiste-t-elle.

La professeure pense que la lutte contre la cybercriminalité et les usages abusifs ou déviants des technologies doit s'inscrire dans un projet politique plus large dont les objectifs finaux sont de produire de la sécurité, de contribuer au développement et à la stabilité économique de notre pays, d'assurer sa souveraineté digitale et de développer une société de l'information viable et fiable.

Agir en amont

Dissuader les criminels, c'est leur faire prendre davantage de risques d'être identifiés et poursuivis, leur faire comprendre qu'ils ne peuvent plus agir en toute impunité. Cela suppose entre autre d'agir en amont en proposant des services électronique et des infrastructures informationnelles robustes qui intègrent des mécanismes de sécurité performants. Cela nécessite également un renforcement du dispositif légal et des dispositifs liés à l'entraide judicaire, que cela soit au niveau cantonal, national ou international : « Il est impératif de développer les capacités techniques, organisationnelles et humaines des instances dédiées à la lutte contre la cybercriminalité et d'accorder des moyens supplémentaires aux forces de police et à la justice, ainsi qu'à tous les acteurs de la formation dans ce domaine, y compris en formation continue ».

Selon Solange Ghernaouti, appréhender de manière holistique la problématique de la sécurité et de la résilience de notre société hyperconnectée nous oblige à penser également en terme de lutte contre la prédation systématique et, à grande échelle, de nos ressources informationnelles, du pillage non seulement de données mais aussi de savoir-faire et de connaissances. Car Internet est également une arme de la guerre économique que se livrent les organisations et les Etats.

La manipulation de l'information et de la communication d'influence

Ainsi la manipulation d'information, la communication d'influence, le cyberespionnage sont également des fléaux de sociétés et ne relèvent pas forcément d'entités criminelles, au sens classique du terme. Cette vision globale ne peut pas faire l'économie d'une réflexion en profondeur et de l'attribution des moyens nécessaires à une approche complémentaire et cohérente des problématiques civile et militaire de la cybersécurité et à la cyberdéfense à la hauteur des enjeux que ces deux disciplines représentent pour notre pays. N'oublions pas que le sommet de l'OTAN de septembre 2014 a considéré les cyberattaques massives comme un acte de guerre auquel il pouvait être répondu militairement et qu'un pays membre victime était une atteinte à l'ensemble de ses membres. « L'expression des conflits se décline dans le cyberespace via le plus souvent des cyberattaques sur des infrastructures informatiques civiles et militaires qui font appel aux mêmes boîtes à outils et savoir-faire que ceux utilisées dans le cadre de la cybercriminalité. Renforcer nos compétences en matière de lutte contre la cybercriminalité c'est aussi contribuer à la défense de nos intérêts nationaux et à notre sécurité ». (rke)

Info : www.ecrime-project.eu

à savoir

Le SCOCI à l'action

Le Service national de Coordination de la lutte contre la Criminalité sur Internet (SCOCI) est un centre de compétence pour le public, les administrations et les fournisseurs d'accès Internet pour toutes questions de nature juridique, technique et criminelle relative à la criminalité sur Internet. En sa qualité de service national de coordination, il se définit comme l'interlocuteur privilégié pour les services étrangers qui exercent la même fonction.

Concrètement, après un premier examen et une sauvegarde des données, le SCOCI transmet les informations reçues aux autorités de poursuite pénale compétentes en Suisse et à l'étranger. Il répond également aux questions des annonceurs. Le service de coordination est en outre chargé de rechercher des contenus illicites sur Internet. Enfin, il procède à des analyses approfondies dans le domaine de la criminalité sur Internet.

Par contenus illicites sur internet ayant une importance pénale, sont notamment compris :

- La pornographie dure (actes d'ordre sexuel avec des enfants, des animaux, des excréments humains ou des actes de violence)
- La pornographie légale, lorsqu'elle est librement accessible aux mineurs sans contrôle d'âge
- La représentation de la violence
- La discrimination raciale et l'extrémisme
- Les infractions contre l'honneur, les menaces
- Les escroqueries, la criminalité économique
- L'accès indu à un système informatique, la propagation de virus informatiques, la détérioration de données

Info : www.fedpol.admin.ch