Sciences à la page

MARS 2013

CYBERSÉCURITÉ

Tenter d'assurer la cybersécurité, c'est essayer d'empêcher l'accès non autorisé aux ordinateurs et aux réseaux. Protéger ces systèmes est primordial pour la sécurité du public, du commerce privé et en ligne, de l'infrastructure essentielle et des renseignements personnels.

Les Canadiens dépendent plus que jamais des réseaux d'ordinateurs. Mais, dans une société branchée, la vulnérabilité à la cybercriminalité et à l'espionnage, aux soi-disant cyberattaques, s'accroit.

La cybercriminalité – qui inclut le vol d'identité, la fraude en ligne et les canulars – a des conséquences directes sur la vie des Canadiens. Une étude a estimé que de juillet 2011 à juillet 2012, 8,3 millions de Canadiens adultes ont été victimes d'un délit informatique[1], et même notre gouvernement est « chaque jour, […] témoin de tentatives de pénétration de ses réseaux[2] ».

Une étude réalisée en 2012 a classé le Canada au troisième rang dans le monde pour ce qui est des victimes de la cybercriminalité et au dixième pour le nombre de sites malveillants hébergés (environ 750 000). Les États-Unis sont arrivés premiers dans les deux catégories[3].

Les cybermenaces évoluent rapidement. Les cyberattaques sont en général perpétrées par des « pirates » motivés par l'espionnage, le crime (vol de données, par exemple.) ou l'activisme (« hacktivisme »)[4]. Bien que la recherche effectuée par des Canadiens avance sur plusieurs fronts, le gouvernement doit essayer de suivre le rythme d'un déluge de cyberattaques[5]. En février, le directeur du Service canadien du renseignement de sécurité (SCRS), Richard Fadden a dit au Comité sénatorial permanent de la sécurité nationale et de la défense que, si le nombre d'attaques continue d'augmenter, le Canada pourrait dans les deux prochaines années ne plus parvenir à réprimer les cybermenaces[6].

Source : Phtos.com

1) 2012 Norton Cyb ry/1030295/2012-norton-study-consumer-cybercrime-costs-canadians-c-1-4-billion; http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf
2) Canadian Security Intelligence Service, 2010–2011 Public Report, Message from the Director. http://www.csis-scrs.gc.ca/pblctns/nnlrprt/2010-2011/rprt2010-2011-eng_final.asp

3) Websense 2013 Threat Report. (p. 10, p. 11 [in infographic])http://www.websense.com/assets/reports/websense-2013-threat-report.pdf
4) CSIS commissioned study by Angela Gendron and Martin Rudner, Assessing Cyber Threats to Canadian Infrastructure http://www.csis-scrs.gc.ca/pblctns/cdmctrch/CyberTrheats_AO_Booklet_ENG.pdf [sic]
5) 2012 Fall Report of the Auditor General of Canada, Chapter 3—Protecting Canadian Critical Infrastructure Against Cyber Threats. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html
6) Testimony before the Standing Senate Committee on National Security and Defense. Ottawa, Monday, February 11, 2013.

UNE NOUVELLE MENACE : LES CYBERATTAQUES CONTRE LES APPAREILS MOBILES

Il y a en gros dix milliards d'appareils connectés sur la planète de nos jours, soit plus d'un par personne. Le rapport du groupe de solutions Internet (IBSG) de CISCO prévoit que ce nombre sera de plus de 40 milliards en 2020[1]. Plus de 11 millions de Canadiens ont un téléphone intelligent et leur principale activité sur Internet consiste à utiliser des applications mobiles.

Des chercheurs allemands ont en 2012 examiné 13 500 applis sur la plateforme Android et ont découvert que 8 % d'entre elles étaient vulnérables à des cyberattaques pouvant compromettre la sécurité des renseignements personnels. Ces chercheurs ont pu s'emparer de données ur les utilisateurs d'American Express, de PayPal, de Facebook et de Google, entre autres.

L'an dernier, 16 % des Canadiens adultes ont été victimes de cyberattaques par le truchement de médias sociaux et d'appareils mobiles. Soixante-seize pour cent des utilisateurs de la technologie mobile n'ont pas de logiciel de sécurité pour leurs appareils[2].

1) http://www.cisco.com/web/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf
2) Sascha Fahl et al., Why Eve and Mallory Love Android: An Analysis of Android SSL (In)Security, Journal of Computer and Communications Security. http://www2.dcsec.uni-hannover.de/files/android/p50-fahl.pdf, 2012 Norton Cybercrime Report. http://www.newswire.ca/en/story/1030295/2012-norton-study-consumer-cybercrime-costs-canadians-c-1-4-billion; http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf

LES CONSÉQUENCES ÉCONOMIQUES DES CYBERATTAQUES

Les coûts économiques de la cybercriminalité sont difficiles à évaluer, en partie parce que les entreprises ne veulent pas révéler les violations de la cybersécurité et les pertes financières qui en résultent[7]. La perte de droits de propriété intellectuelle et les dommages à la réputation font partie des coûts éventuels[8]. Les enquêtes et les rapports ont différentes définitions de la cybercriminalité. Les données scientifiques de tierces parties objectives et les données décrivant l'étendue des dégâts font défaut et de meilleures données sur ces questions sont nécessaires pour la réalisation de recherches qui pourront éclairer l'élaboration de politiques. Voici des chiffres qui ont été avancés :

- Selon ceux du logiciel antivirus Norton, de juin 2011 à juin 2012, le coût net de la cybercriminalité a été de 1,4 milliard de dollars au Canada[9].
- Une enquête menée en 2011 auprès des professionnels de la sécurité de la TI au Canada a conclu que le coût annuel moyen pour les gouvernements, le public et l'entreprise privée était de 83 000 $, une diminution importante par rapport aux années antérieures, et que le nombre annuel moyen de violations était de sept ou huit[10].
- D'après un article publié en 2008 par des chercheurs de l'Université McMaster, le vol d'identité a coûté en moyenne 150 millions de dollars aux consommateurs canadiens l'année précédente[11].

7) Ponemon Institute, Second Annual Cost of Cyber Crime Study Benchmark Study of U.S. Companies. http://www.hpenterprisesecurity.com/collateral/report/2011_Cost_of_Cyber_Crime_Study_August.pdf CRS Report for Congress, The Economic Impact of Cyber-Attacks.http://www.cisco.com/warp/public/779/govtaffairs/images/CRS_Cyber_Attacks.pdf

8) Benjamin J. Brooker, et al., A Framework for the Evaluation of State Breach Reporting Laws, Risk Analysis. http://www.sys.virginia.edu/sieds07/papers/SIEDS07_0066_Fl.pdf
9) See fn 2. See Public Safety statement fn 1, which estimates the cost of identity theft at $1.9 billion. A few people have questioned the $1.4 billion figure, but it seems to be consistent with the government source.
10) Telus & Rotman School of Management, 2011 Executive Summary, Joint Study on Canadian IT Security Practices.http://business.telus.com/en_CA/content/pdf/whyTELUS/Security_Thought_Leadership/TELUS_Rotman_2011_Results.pdf
11) http://merc.mcmaster.ca/working-papers/23.html

SÉCURITÉ NATIONALE

Le ministre de la Sécurité publique, Vic Toews, a reconnu que des pirates pouvaient « troubler les contrôles électroniques des réseaux de distribution d'électricité, des installations de traitement des eaux et des réseaux de télécommunications », et paralyser ainsi des services vitaux pour la sécurité publique et la sécurité nationale[1]. En 2009, le ver Stuxnet , une sorte de logiciel malveillant, a infiltré les centrifugeuses d'une centrale nucléaire iranienne et les a gravement endommagées en portant la vitesse de fonctionnement au-delà des limites sécuritaires, ce qui les a fait voler en éclats[2].

Dans un rapport récent, la firme de sécurité Mandiant a attribué les attaques contre la branche canadienne du concepteur de systèmes de contrôle industriel Telvent à un groupe de pirates chinois. Telvent développe des logiciels pour le contrôle des réseaux électriques, des oléoducs et d'autres systèmes industriels partout sur le continent. Les pirates ont infiltré Telvent en 2012 et dérobé les données de l'entreprise relatives au fonctionnement de ces systèmes[3].

Les systèmes du gouvernement canadien ont aussi été violés, et les effets sont durables. Au début de 2011, les comptes utilisateurs d'employés du Conseil du Trésor, de Recherche et développement pour la défense Canada et du ministère des Finances ont été compromis, obligeant ces ministères et organismes à bloquer l'accès de leur personnel à Internet pour résoudre l'atteinte à la sécurité des données. Il a fallu près de huit mois pour que le service Internet soit pleinement rétabli[4]. Si ces attaques deviennent plus fréquentes, comme beaucoup le prévoient, la sécurité nationale reposera de plus en plus sur une solide cyberdéfense.

1) 2012 Norton Cybercrime Report.http://www.newswire.ca/en/story/1030295/2012-norton-study-consumer-cybercrime-costs-canadians-c-1-4-billion; http://now-static.norton.com/now/en/pu/images/Promotions/2012/cybercrimeReport/2012_Norton_Cybercrime_Report_Master_FINAL_050912.pdf
2) Thomas M. Chen, Saeed Abu-Nimeh, Lessons from Stuxnet, IEEE Computer Society, April 2011.
3) Mandiant, APT1 Exposing One of China's Cyber Espionage Units, http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf
4) 2012 Fall Report of the Auditor General of Canada, Chapter 3—Protecting Canadian Critical Infrastructure Against Cyber Threats. http://www.oag-bvg.gc.ca/internet/English/parl_oag_201210_03_e_37347.html
Stephanie Levitz and Jim Bronskill, Hackers had head start breaking into Ottawa computers, documents show, The Globe and Mail/Canadian Press, Monday, Sep. 26 2011. http://www.theglobeandmail.com/news/politics/hackers-had-head-start-breaking-into-ottawa-computers-documents-show/article4256843/

ARAMCO C. SHAMOON : LE COÛT D'UNE CYBERATTAQUE DESTRUCTRICE

À la fin de 2012, des pirates se sont attaqués à la société pétrolière Aramco, propriété de l'État saoudien. L'Arabie saoudite est le plus gros producteur de pétrole au monde, et Aramco gère l'infrastructure pétrolière du pays.

Un groupe appelé « l'épée tranchante de la justice » a revendiqué la responsabilité de l'attaque, qui a gravement endommagé 30 000 ordinateurs. Selon l'information de presse, les pirates ont utilisé un logiciel malveillant (maliciel) appelé Shamoon, qui a rendu les ordinateurs inutilisables et obligé l'entreprise à remplacer leur disque dur[1]. Aramco dit avoir débranché les ordinateurs fragilisés du réseau avant que son infrastructure ne soit touchée[2].

1) Jim Finkle, Exclusive: Insiders suspected in Saudi cyber attack, Reuters, Sept. 7, 2012. http://www.reuters.com/article/2012/09/07/net-us-saudi-aramco-hack-idUSBRE8860CR20120907
2) Saudi Aramco, Saudi Aramco restores network services, Press Release. http://www.saudiaramco.com/content/mobile/en/home/news/latest-news/2012/saudi-aramco-restores-network.html Nicole Perlroth, In Cyberattack on Saudi Firm, U.S. Sees Iran Firing Back, New York Times, October 23, 2012. http://www.nytimes.com/2012/10/24/business/global/cyberattack-on-saudi-oil-firm-disquiets-us.html

Source : ImagesCARWTY8

MOYENS UTILISÉS POUR FRAGILISER LES SYSTÈMES INFORMATIQUES

L'INGÉNIERIE SOCIALE, L'HAMEÇONNAGE CIBLÉ ET GHOSTNET

En 2008 et en 2009, le Laboratoire citoyen, Munk Centre Munk of International Studies, de l'Université de Toronto a fait des recherches sur un « réseau de cyberespionnage » qu'il a appelé GhostNet et qui ciblait les dirigeants tibétains. Les pirates ont amené ces personnes à révéler des renseignements personnels en utilisant l'« hameçonnage ciblé ».

À la différence de l'hameçonnage ordinaire, qui essaie d'amener tout le monde, sans distinction, à dévoiler des renseignements personnels'« hameçonnage ciblé » adapte ses attaques à certaines personnes en particulier.

En 2008, les auteurs de GhostNet ont envoyé un message électronique à campaigns@freetibet.org, auquel était jointe une pièce intitulée « Translation of Freedom Movement ID Book for Tibetans in Exile.doc » (traduction du livret d'identité, liberté de mouvement pour les Tibétains en exil.doc). Ce document Word, qui semblait authentique, était infecté par un maliciel qui se cachait dans l'ordinateur de la victime lorsque celle ci ouvrait le document. Le maliciel se connectait à GhostNet où les pirates pouvaient, entre autres choses, activer des caméras Web, voir les écrans des moniteurs et avoir accès à l'information confidentielle stockée dans les ordinateurs infectés.

Le Laboratoire citoyen a estimé dans son rapport que près de 1 300 ordinateurs, dont beaucoup croit-on appartenaient à des diplomates et à des ambassades partout dans le monde, ont été fragilisés par GhostNet. Les chercheurs ont découvert l'infection en surveillant de près le trafic réseau sur les ordinateurs du Bureau du dalaï-lama[1].

1) Ronald Deibert, et al., Tracking GhostNet: Investigating a Cyber Espionage Network, Information Warfare Monitor, March 29, 2009. http://www.scribd.com/document_downloads/direct/13731776?extension=pdf&ft=1361195018&lt=1361198628&uahk=lkLqwrJvQLkgGZQj9dFjr//Oc/4

ATTAQUES PAR LE TRUCHEMENT DES NAVIGATEURS

Les attaques par le truchement des navigateurs sont souvent exécutées à l'aide d'un code JavaScript malveillant implanté dans une page Web. Le JavaScript est un langage de programmation couramment utilisé par les sites de nouvelles très consultés, les magasins en ligne et les sites Web des établissements d'enseignement et des gouvernements, par exemple.

Les pirates se servent de JavaScript pour exploiter les faiblesses des navigateurs et de leurs modules d'extension, appelés plugiciels. Lorsqu'il visite un site Web fragilisé, le code malveillant infecte l'utilisateur, puis télécharge et installe un maliciel sur l'ordinateur de la victime. Ces attaques sont appelées téléchargements furtifs[1].

ATTAQUES PAR LE TRUCHEMENT DES POINTS FAIBLES D'UN LOGICIEL

Exploiter les défauts de conception des logiciels – parfois appelés « codage négligé » – est une autre méthode couramment utilisée pour avoir accès à un ordinateur sans y être autorisé. Les pirates peuvent tirer parti de ces failles et créer des programmes afin d'en faire mauvais usage. Ils publient ensuite souvent leurs découvertes en ligne, ce qui amplifie le problème.

Une fois que les attaquants ont accès à un système, ils peuvent installer un maliciel et se servir de l'ordinateur infecté pour de viles activités. Souvent, les points faibles apparaissent « comme ça », avant que le fabricant ait produit un programme de correction pour les régler. On parle alors de « vulnérabilité du jour zéro ».

1) N. Provos, D. McNamee, P. Mavrommatis, K. Wang, and N. Modadugu. The ghost in the browser: Analysis of web-based malware. In Proceedings of USENIX Workshop on Hot Topics in Understanding Botnets (HotBots), April, 2007

POURQUOI LES MALICIELS ET LES RÉSEAUX DE ZOMBIES DEVRAIENT-ILS NOUS INQUIÉTER?

Maliciel : programme malveillant qui attaque les ordinateurs, dérobe de l'information de nature délicate ou perturbe des systèmes. Il peut s'agir de chevaux de Troie, de logiciels espions, de vers ou de virus.

L'infection par un maliciel est souvent la première étape vers l'établissement d'un réseau de zombies, c'est-à-dire un réseau d'ordinateurs infectés qui peuvent agir de concert et sont contrôlés par des « maîtres ». Une fois branché à un réseau de zombies, le maître peut commander à distance à chacun des systèmes fragilisés, ou zombies, d'effectuer diverses tâches. Il peut s'agir de voler des renseignements personnels, d'envoyer des canulars par courriel ou de prendre part à de grandes attaques par déni de service distribué (DDoS) cordonnées avec d'autres zombies[1]. Les DDoS sont une tactique fréquemment employée pour surcharger les systèmes Internet et les faire tomber en panne; on s'en est servi pour attaquer les systèmes de communication et le gouvernement estonien en 2007[2].

Les cyberattaquants conçoivent les maliciels non seulement pour se servir des ordinateurs des victimes à des fins criminelles, mais aussi de manière à éviter d'être repérés. Les pirates cachent les maliciels dans les fichiers système et le matériel dont les ordinateurs ont besoin pour fonctionner, ce qui rend l'infection difficile à repérer et parfois impossible à résoudre. Dans les cas extrêmes, le seul moyen d'enlever efficacement le maliciel est de remplacer tout l'ordinateur[3].

1) C. Wüest. Current advances in banking trojans. In Proceedings of 22nd Virus Bulletin International Conference September 2012.
2) Joshua Davis, Hackers Take Down the Most Wired Country in Europe, Wired Magazine, August 21, 2007 http://www.buec.udel.edu/wraggej/MISY850-09S/Estonia.pdf
3) Interview with José Fernandez, Assistant Professor, Department of Computer Engineering, February 14, 2013.

Source : imagesC.OBC

ÉTUDE DE CAS : ATTÉNUATION DE LA MENACE REPRÉSENTÉE PAR UN RÉSEAU DE ZOMBIES ET DESTRUCTION DE WALEDAC

Waledac était un important réseau de zombies source de pourriels et de maliciels qui est apparu en novembre 2008.

Une équipe de chercheurs de l'École Polytechnique de Montréal a aidé à découvrir la structure et le fonctionnement de Waledac, et a repéré des faiblesses pouvant être utilisées pour le démanteler. Les chercheurs ont élaboré des mécanismes d'atténuation contre Waledac et ont recréé un réseau Waledac opérationnel sur un groupe isolé d'ordinateurs se trouvant dans leur laboratoire. Ils se sont servis du réseau reconstitué pour montrer que Waledac réagissait à leur mécanisme d'atténuation. Microsoft a utilisé la recherche pour désactiver Waledac en 2010. Malheureusement , il semble que Waledac soit réapparu récemment sous une nouvelle forme et qu'on s'en serve de nouveau pour commettre des délits informatiques[1].

1) Joan Calvet, et al., The case for in-the-lab botnet experimentation: creating and taking down a 3000-node botnet, Proceedings of Annual Computer Security Applications Conference (ACSAC 2010), December 2010. Fahmida Y. Rashid, Waledac Botnet Reappears as New Password Stealing Variant, eWeek, February 15, 2012. http://www.eweek.com/c/a/Security/Waledac-Botnet-Reappears-as-New-Password-Stealing-Variant-882729/

TECHNOLOGIES D'ATTÉNUATION DES CYBERATTAQUES

Les logiciels antivirus et la surveillance des réseaux peuvent atténuer les cybermenaces. Lorsqu'une défense est en place, toutefois, les pirates conçoivent des attaques pour contourner cette protection. Le jeu du chat et de la souris que sont les cyberconflits signifie que les méthodes et les technologies doivent constamment s'adapter à l'évolution des attaques[1].

1) Interview with José Fernandez, Assistant Professor, Department of Computer Engineering, February 14, 2013.

LA VIE PRIVÉE ET LA LÉGISLATION RELATIVE À LA CYBERSÉCURITÉ

Des activités législatives visant à assurer la cybersécurité et à contrer la cybercriminalité ont eu lieu récemment, mais ont fait l'objet de dures critiques. Le projet de loi C-30 est mort au feuilleton en février après le tollé général soulevé par le fait de donner aux autorités la possibilité d'avoir accès à l'information relative aux abonnés d'Internet et de surveiller les communications sans mandat.

Il a depuis été remplacé par le projet de loi C-55, qui accorderait des pouvoirs semblables dans les situations considérées comme des urgences[1]. Le gouvernement examine en ce moment la règlementation applicable à *la loi canadienne anti-pourriel de 2010*. Cette loi régira en partie la capacité des tierces parties d'installer des logiciels sur un ordinateur sans le consentement de la personne à qui il appartient[2].

La commissaire à la protection de la vie privée, Jennifer Stoddart, a critiqué le projet de loi C-12, qui concerne les responsabilités des sociétés privées lorsque survient une atteinte à la sécurité des données, disant qu'il ne va pas assez loin pour protéger l'information personnelle. Selon elle, l'état actuel de la législation sur la protection des données privées est « inacceptable »[3]. Le Canada n'a en particulier pas de loi exigeant que les renseignements personnels soient encodés lorsqu'ils sont stockés sur des appareils mobiles ou transmis sur des réseaux ouverts, à la différence du Massachusetts, par exemple. Ces lois peuvent contribuer à la protection des renseignements personnels en cas de cyberattaques ou de vol de matériel et de perte d'appareils mobiles.

1) Michael Geist, Lawful Access is Dead (For Now): Government Kills Bill C-30, michaelgeist.ca, February 12, 2013. http://www.michaelgeist.ca/content/view/6782/125/
2) Canada's Anti-Spam Legislation, Fast Facts, http://fightspam.gc.ca/eic/site/030.nsf/eng/h_00039.html
3) Jennifer Stoddart, Testimony before Information & Ethics Committee, Ottawa, December 11th, 2012 http://openparliament.ca/committees/ethics/41-1/59/jennifer-stoddart-34/

POLITIQUE VISANT À ASSURER LA CYBERSÉCURITÉ

Il faudra pour se protéger contre les cyberattaques un mélange d'activités éducatives pour les citoyens, de mise au point de technologies et de règlementation qui établit des protocoles de sécurité pour l'industrie et le gouvernement[1]. Le Canada a signé la Convention sur la cybercriminalité (ou Convention de Budapest) du Conseil de l'Europe. Cette convention fournit un cadre pour la législation permettant de procéder à des enquêtes sur les cybercriminels, et de les poursuivre, et exige notamment que les États établissent des « réseau[x] 24/7 » fonctionnant en tout temps afin que toutes les autres parties puissent communiquer avec eux pour échanger de l'information sur la cybercriminalité[2].

Pour résoudre les problèmes systémiques, l'Union européenne et les États-Unis ont tous deux, en février 2013, diffusé une stratégie visant à améliorer la cybersécurité. L'UE a recommandé d'obliger le secteur privé à communiquer l'information sur les cyberattaques aux organismes gouvernementaux, alors que les États-Unis s'attaquent au même problème par un décret-loi encourageant les propriétaires d'une infrastructure essentielle à participer à l'élaboration de pratiques exemplaires sur la cybersécurité[3]. Tous deux considèrent que l'échange de renseignements est important pour comprendre les cybermenaces. Dans des pays comme la Finlande, Israël et la Suède, où la cybersécurité fait l'objet d'éloges, la collaboration est étroite entre le gouvernement, les forces militaires, le milieu universitaire et le secteur privé[4].

1) Ross Fraser, comments aires sur ce document.
2) Convention on Cybercrime CETS No.: 185, Signatorieshttp://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG
Convention on Cybercrime, Budapest, November 21, 2001 (Art. 35)
http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

3) Convention on Cybercrime CETS No.: 185, Signatorieshttp://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=1&DF=&CL=ENG Convention on Cybercrime, Budapest, November 21, 2001 (Art. 35) http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

4) Brigid Grauman, Cyber-security: The vexed question of global rules, Security & Defence Agenda, February, 2012. http://www.securitydefenceagenda.org/Portals/14/Documents/Publications/SDA_Cyber_report_FINAL.pdf

Sécurité publique Canada a formulé des propositions semblables pour l'échange d'information entre le gouvernement et le secteur privé, ainsi que pour l'élaboration de normes pour la cybersécurité, mais bon nombre n'ont pas encore été pleinement mises en œuvre, selon le vérificateur général[1].

La politique sur la cybersécurité est dans l'enfance et exige une approche nuancée. Par exemple, les défis auxquels sont confrontés les systèmes industriels diffèrent beaucoup de ceux auxquels les réseaux gouvernementaux ou commerciaux font face, bien que les dommages occasionnés à l'un ou à l'autre puissent mettre la sécurité publique en péril. Le dialogue entre tous les secteurs permettra de circonscrire le problème et de le régler[2].

Les experts soulignent que ces initiatives sont nécessaires pour lutter contre les menaces nationales – et parfois mondiales – ; les critiques souvent formulées sont toutefois que ces politiques n'ont pas d'orientation concrète et que, si la collaboration internationale n'est pas élargie, les cybercriminels poursuivront leurs activités en dehors des limites de ces accords[3].

À l'échelle individuelle, les chercheurs et les gouvernements insistent sur l'importance de l'éducation. En septembre 2012, le gouvernement a lancé le Mois de la sensibilisation à la cybersécurité[4] ainsi que son site Web[5], qui offre des conseils précieux aux groupes les plus à risque, dont les personnes âgées, les étudiants et les enfants. Cette information pratique non seulement aide tous les utilisateurs d'Internet à assurer leur propre protection, mais elle renforce aussi la cybersécurité au bénéfice de tous en protégeant les grands réseaux auxquels ils se branchent.

1) Evidence, Comité du sécurité national et de la défense du Sénat , le 11 février 2013.
2) Entrevue avec Eric Byres, CTO and VP Engineering, Tofino Security, le 14 février 2013.
3) Marc Hall, Storm cloud emerges from EU cybersecurity strategy, EurActv.com, February 8, 2013 http://www.euractiv.com/infosociety/stormcloud-emerges-cloud-safety-news-517658
Lisa Vaas, Infosec pros give verdict on EU's new cybersecurity strategy: "Nice try", NakedSecurity, February 8, 2013 http://nakedsecurity.sophos.com/2013/02/08/eu-cybersecurity-strategy/
Chengxi Wang, Obama's Cybersecurity Executive Order: Heart In The Right Place But There Is Little Teeth, Forbes.Com, February 14, 2013. http://www.forbes.com/sites/forrester/2013/02/14/obamas-cybersecurity-executive-order-heart-in-the-right-place-but-there-is-little-teeth/
Gerry Smith, Obama's Cybersecurity Order Weaker Than Previous Proposals, HuffingtonPost.com, February 12, 2013. http://www.huffingtonpost.com/2013/02/12/obama-cybersecurity-state-of-the-union_n_2669941.html Ron Deibert, Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace, Canadian Defence & Foreign Affairs Institute, August 2012. https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf

4) Ministry of Public Safety, Government of Canada Launches Cyber Security Awareness Month with New Public Awareness Campaign Partnership, September 27, 2012. http://www.publicsafety.gc.ca/media/nr/2012/nr20120927-1-eng.aspx
5) Get Cyber Safe. http://www.getcybersafe.gc.ca/index-eng.aspx

Autres lectures :

1. Ron Deibert, Distributed Security as Cyber Strategy: Outlining a Comprehensive Approach for Canada in Cyberspace, Canadian Defence & Foreign Affairs Institute, août 2012. https://citizenlab.org/wp-content/uploads/2012/08/CDFAI-Distributed-Security-as-Cyber-Strategy_-outlining-a-comprehensive-approach-for-Canada-in-Cyber.pdf
2. Canada's Cyber Security Strategy: http://www.securitepublique.gc.ca/prg/ns/cybr-scrty/ccss-scc-fra.aspx
3. Assessing Cyber Threats to Canadian Infrastructure, report prepared for CSIS, Angela Gendron and Martin Rudner, March 2012 - https://www.csis.gc.ca/pblctns/cdmctrch/20121001_ccsnlpprs-fra.asp

Au sujet de Sciences à la page

Sciences à la page (www.sciencepages.ca) est une initiative du Partenariat en faveur des sciences et de la technologie (www.pagse.org) réalisée en collaboration avec le Centre canadien sciences et médias.

Sciences à la page vise à favoriser la discussion sur des sujets d'actualité centrés sur les sciences et le génie, et résume pour ce faire l'état actuel des connaissances et des politiques. Chaque numéro de ce bulletin gratuit est rédigé et examiné par une équipe multidisciplinaire.

Il a été préparé par Carlton Davis, Tomas Urbina, Simon Liem.

Ce numéro a bénéficié de l'appui du Conseil de recherches en sciences naturelles et en génie (CRSNG) et de la Fondation canadienne pour l'innovation (FCI), ainsi que de l'aide du Secrétariat de la collectivité fédérale en S-T.

Pour obtenir plus d'information : info@sciencepages.ca.

Ce document avec références est disponible au www.sciencepages.ca