Denis JACOPINI participera au 8e IT-Forum à Abidjan les 2 et 3 juin 2016

Denis JACOPINI participera au 8e IT-Forum à Abidjan les 2 et 3 juin 2016

La 8e édition du IT-Forum (Forum des décideurs et acteurs des Technologies de l'Information) se déroulera les 2 et 3 juin prochain à Abidjan.

IT FORUM 8ème EDITION

Des conférences seront animées en plénières par des spécialistes, des Experts-Consultants et des Universitaires. Ce sera le lieu de faire des exposés, de partager des expériences, de former et d'informer les participants.
Les enjeux de la transformation numérique et plus globalement de l'appropriation des nouvelles technologies modifient considérablement notre mode de vie. La sécurisation des données et des dispositifs de paiement comporte des failles qu'il comporte d'améliorer pour apporter la confiance nécessaire au climat des affaires.
De nombreuses études viennent conforter ce constat et tendent à démontrer le potentiel de croissance du secteur.
En Côte d'Ivoire, les transactions mobiles s'élèvent à 15 milliards de FCFA par jour soit 22,5 millions d'Euros.
Des montants qui donnent le vertige et qui poussent les sites marchands notamment les opérateurs de télécommunications à prendre des mesures de sécurité de plus en plus importantes… mais qui montrent aussi rapidement leurs limites !
Au fil des années, la Côte d'Ivoire s'est imposée comme l'un des leaders naturels dans le domaine des transactions mobiles en Afrique.
En insistant sur la priorité à donner à la protection des données et des transactions (mobile banking, eCommerce),
Devenu un rendez-vous incontournable depuis une décennie, l'IT Forum s'impose aujourd'hui comme l'une des
rencontres les plus importantes.
QUAND
Jeudi 2 juin 2016 à 08:00 – Vendredi 3 juin 2016 à 18:00 (Heure : Côte d'Ivoire) – Ajouter au calendrier
LIEU
Maison de l'entreprise – CGECI (Confédération Générale des Entreprises de Côte d'Ivoire – Patronat ivoirien), Avenue Lamblin, Abidjan, Lagunes, Côte d'Ivoire, Abidjan, Plateau, Cote d'Ivoire –
PROGRAMME
http://www.ciomag-event.com/8eme-edition-it-forum-cote-d-ivoire

---

Réagissez à cet article

Sources :

IT-Forum 2016 – 8e édition du Forum des décideurs et acteurs des Technologies de l'Information

http://it-forum.ci

https://www.eventbrite.fr/e/inscription-it-forum-2016-8eme-edition-24951266911

L'essor du chiffrement inquiète le renseignement anglais | Le Net Expert Informatique

L'essor du chiffrement inquiète le renseignement anglais

Dans une interview à la BBC, le patron du renseignement intérieur britannique (MI5) a exprimé ses inquiétudes à l'égard de l'évolution des technologies de chiffrement. Selon lui, les entreprises technos ont le devoir éthique d'informer les autorités de menaces potentielles.

Le gouvernement britannique n'en démord pas et veut ses backdoors : dans une interview donnée à la BBC, le dirigeant du MI5, les services de sécurité de la Grande-Bretagne, évoque à nouveau le débat autour des technologies de chiffrement qui se développent à destination du grand public.

Pour Andrew Parker, directeur du MI5, les services de police ont de plus en plus de mal à obtenir des informations en ligne et les entreprises du secteur technologique devraient selon lui informer les agences de renseignement des potentielles menaces détectées via leurs outils. Il explique au micro de la BBC que les services de police sont confrontés à la difficulté croissante d'obtenir « les relevés de communications des utilisateurs suspectés d'activités terroristes, et ce même en disposant d'un mandat de justice. »

Haro sur le chiffrement

Une critique déjà entendue fréquemment et qui fait écho au développement d'outils de chiffrement de bout-en-bout, mouvement qui gagne en intensité dans l'industrie des nouvelles technologies et des services en ligne suite aux révélations d'Edward Snowden.

Et la problématique n'est cantonnée Outre-Manche, où David Cameron a annoncé son intention de légiférer sur le sujet. Aux États Unis, on a ainsi pu voir les dirigeants du FBI exprimer une demande similaire, évoquant la possibilité de mettre en place des backdoors connues des seuls services de renseignement afin de pouvoir accéder aux données échangées sur les plateformes de messagerie en ligne. En France, c'est le procureur de la République de Paris qui s'y colle : celui-ci avait signé en août une tribune dans le New York Times déplorant l'essor du chiffrement et l'obstacle que celui-ci constituait dans les enquêtes judiciaires.

Face à cette offensive, les défenseurs de la cryptographie s'inquiètent tout particulièrement des conséquences que pourrait apporter la mise en œuvre d'une telle volonté politique : pour Bruce Schneier, expert américain de la cryptographie, s'appuyer sur ce type de procédé viendrait immanquablement contredire le principe même de la cryptographie, supposé garantir la sécurité des échanges entre les destinataires. De plus, et l'affaire récente des clefs d'accès aux cadenas TSA le rappelle bien : les backdoors ne sauraient garantir que la personne qui les utilise est bien un représentant des forces de l'ordre, laissant la possibilité à des cybercriminels ou à des pays étrangers de les exploiter.

Source :
http://www.zdnet.fr/actualites/le-renseignement-anglais-s-inquiete-lui-aussi-de-l-essor-du-chiffrement-39825120.htm

---

Cyberespace : les USA et la

Chine font la paix | Le Net Expert Informatique

Cyberespace : les USA et la Chine font la paix

L**e New York Times informe qu'un accord de non-agression contre les sites d'infrastructure critique en temps de paix devrait être signé au cours de la visite du président chinois Xi Jinping aux États-Unis la semaine prochaine.**

Plus tôt, le président américain Barack Obama avait parlé du risque d'aggravation des relations bilatérales en cas d'impossibilité de trouver un terrain d'entente. Au printemps, un tel accord avait déjà été signé entre la Russie et la Chine. Un nouveau régime international de conduite des pays dans le cyberespace pourrait ainsi voir le jour progressivement.

Les représentants de la Chine et des USA mènent des négociations sur un accord les engageant mutuellement à ne pas porter d'attaques cybernétiques contre des sites d'infrastructure critique en temps de paix. Cet accord visera à prévenir les attaques contre les centrales électriques, les systèmes bancaires, les réseaux téléphoniques et les hôpitaux. Les sources du NYT auprès de l'administration du président américain soulignent que ce document devrait contenir peu d'aspects concrets. Il impliquera très probablement des engagements sur le respect des principes et des règles de conduite dans le cyberespace adoptés par un groupe d'experts gouvernementaux de l'Onu en juin dernier.

L'accord en question ne devrait pas concerner l'espionnage industriel des sites commerciaux qui, selon les USA, constituent la grande partie des intrusions chinoises. Ces derniers temps, ce problème est devenu central dans les relations bilatérales. « A un certain moment nous commencerons à considérer les cyberattaques comme une menace à la sécurité nationale et nous y réagirons en conséquence », a déclaré le 11 septembre Barack Obama à Fort Meade devant les militaires américains. Le 16 septembre, il déclarait aussi aux représentants de la communauté d'affaires: « Nous avons préparé plusieurs mesures appelées à montrer que si cette question n'était pas réglée, elle compliquerait considérablement les relations bilatérales ».
Les opinions exprimées dans ce contenu n'engagent que la responsabilité de l'auteur.

Source : http://fr.sputniknews.com/presse/20150921/1018285357/cyberespace-usa-chine.html
Par Kommersant

La cybersécurité devrait devenir le point d’orgue de la coopération sino-américaine | Le Net Expert Informatique

La cybersécurité devrait devenir le point d’orgue de la coopération sino-américaine

Dans le cadre de la prochaine visite du président chinois Xi Jinping aux Etats-Unis, il est quasiment certain que la cybersécurité sera un sujet brûlant. En fait, en matière de protection de la cybersécurité, la Chine et les Etats-Unis, deux acteurs importants dans ce domaine, ont beaucoup à gagner à coopérer.

Il y a quelques jours, le représentant spécial de M. Xi, Meng Jianzhu, s'est rendu aux Etats-Unis. Les deux pays ont alors atteint un consensus important pour la lutte contre les crimes sur Internet. Les deux pays peuvent désormais coopérer davantage dans ce domaine.

La Chine et les Etats-Unis sont deux pays dotés de technologies Internet très développées, a indiqué M. Meng, ajoutant que dans le contexte des incidents fréquents et des menaces sécuritaires croissantes dans le cyberespace, il est très important que les deux pays renforcent la confiance mutuelle et la coopération dans la sphère de la cybersécurité.

Le consensus a envoyé un bon message: la cybersécurité peut devenir un domaine de coopération sino-américain au lieu d'une source de frictions.

Mais certaines agences américaines ainsi que certains médias ne cessent de parler des soi-disantes attaques chinoises sur Internet.

Le directeur des Renseignements nationaux américains, James Clapper, a déclaré que la Chine et la Russie représentent les menaces sur Internet les plus sophistiquées et que le cyber-espionnage chinois continue de viser un vaste domaine des intérêts américains. Des médias américains ont même dit que des entreprises et des individus chinois pourraient être sanctionnés pour leurs cyberattaques contre des cibles commerciales américaines.

Il est évident que ces remarques irresponsables et ces accusations sans fondement ne sont pas favorables aux relations bilatérales et empêcheront de trouver des solutions à ce problème.

La Chine ne cesse de dire qu'elle est contre toutes formes de cyberattaques et qu'elle les éliminera, car elle a été pendant longtemps une victime de ces activités illégales.

Face à la cybersécurité, nouveau problème touchant pratiquement le monde entier, la Chine a également prôné la coopération avec la partie américaine et tout autre pays afin de protéger la sécurité et son ordre pacifique.

La Chine a montré qu'elle était prête à exploiter le potentiel de la gouvernance d'Internet avec les autres pays, mais tout progrès majeur dans ce domaine dépend de l'action de Washington.

Si les Etats-Unis pouvaient faire preuve de sincérité et prendre d'autres vraies mesures concrètes pour protéger la cybersécurité aux côtés de la Chine, au lieu de porter des accusations sans fondement contre la Chine, les conséquences pour les relations bilatérales seraient positives et l'Internet serait meilleur.

Source : http://french.xinhuanet.com/2015-09/15/c_134627069.htm

Pourquoi est-il impossible de protéger vos données personnelles contre le piratage | Le Net Expert Informatique

Pourquoi est-il impossible de protéger vos données personnelles contre le piratage

Que ce soit les gouvernements ou les services comme Ashley Madison, aucune entreprise, organisation ou personne n'est à l'abri d'une cyberattaque.

Selon Caleb Barlow, vice-président d'IBM Security, la raison est pourtant simple : alors que la culture du secret fait partie des mœurs du monde des affaires depuis ad vitam æternam, le partage d'information est ce qui permet aux pirates de réaliser des percées en la matière au quotidien.
Alors que la culture du secret fait partie des mœurs du monde des affaires, le partage d'information est ce qui permet aux pirates de réaliser des percées au quotidien.
«Nous sommes confrontés à une pandémie. Elle fait les manchettes tous les jours», a-t-il déclaré au blogue Tech Insider. «Et il nous faut comprendre que ce n'est que la pointe de l'iceberg.»
«80% des attaques [aux États-Unis] ne sont pas perpétrées par des pays étrangers, elles sont le fruit du crime organisé», affirme Barlow. «Des regroupements criminels hautement organisés travaillent dans des cubicules, font du 9 à 5 et profitent de leurs weekends de congés. Ils collaborent entre eux afin de s'aider mutuellement. Comme l'on pourrait collaborer avec d'autres personnes d'une même industrie afin d'apprendre les uns des autres et s'aider mutuellement.»
À son avis, si les entreprises souhaitent réellement se prémunir contre de futures cyberattaques, elles auraient intérêt à faire la même chose. Voilà pourquoi Barlow emploie la métaphore d'une pandémie.
«Si la situation était traitée comme la crise d'Ebola, les médecins collaboreraient activement entre eux à trouver des outils et traitements efficaces contre les infections», croit-il. «Afin de lutter contre le problème, les données de base sur des choses comme le niveau d'infections et les origines de celles-ci doivent être démocratisées. Ce n'est qu'une fois que l'on détermine le traitement efficace, une fois que l'on passe à l'étape de la pharmaceutique, que l'on peut se faire concurrence. Mais ce n'est pas du tout la façon dont la cybersécurité fonctionne aujourd'hui.»
Les plus importantes données concernant de telles cyberattaques et menaces sont généralement conservées par des institutions privées, principalement des entreprises spécialisées en cybersécurité. Cette information n'est pratiquement jamais partagée, et lorsque c'est le cas, c'est généralement parce que les données sont devenues obsolètes.

Afin de pallier le problème, IBM a récemment lancé X-Force Exchange, une plateforme cherchant à colliger et diffuser ce type de données, gratuitement. La base de données est composée à la fois de données antérieures et de données générées en temps réel. Les utilisateurs peuvent ainsi y observer le déploiement de cyberattaques et de maliciels en direct.

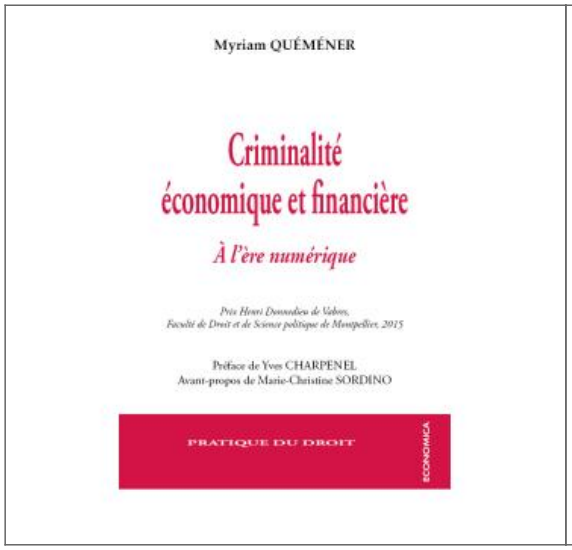
Aux dires d'IBM, les données qu'elle partage ainsi gratuitement représentent 700 téraoctets. Elle met au défi le reste de la communauté spécialisée en cybersécurité d'en faire autant.

X-Force Exchange est consultable sur https://exchange.xforce.ibmcloud.com/

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://branchez-vous.com/2015/08/25/pourquoi-il-impossible-de-proteger-vos-donnees-personnelles-le-piratage/
Par Laurent LaSalle

La criminalité économique et financière à l’ère numérique | Le Net Expert Informatique



La criminalité économique et financière à l’ère numérique

Les banques, les compagnies d'assurances, les sites gouvernementaux, les compagnies pétrolières et, maintenant, l'industrie aéronautique avec la cyberattaque de la compagnie polonaise LOT : le cybercrime cible des secteurs de plus en plus sensibles, sources de dégâts humains majeurs. Au-delà des pertes financières, c'est le cœur du système politique, économique et juridique qui est aujourd'hui menacé par ce fléau.

Que fait l'État, la justice, pour enrayer ces comportements ? Fabriquer des lois en série est-elle « la » solution face à l'existence de cyberparadis, d'une cyberéconomie souterraine de plus en plus puissante, et à la volatilité des preuves ? Le Point.fr a interrogé Myriam Quemener, magistrate, auteur d'un ouvrage de référence sur le sujet : La criminalité économique et financière à l'ère numérique*.

Le Point.fr : « Certaines formes de cybercriminalité sont le fait de réseaux mafieux structurés issus de pays n'ayant pas de législation dédiée à ce phénomène », écrivez-vous. Le décalage entre les législations étatiques est-il surmontable et à quelle échéance ? Que font les autorités françaises en attendant une prise en charge globale et harmonisée de cette délinquance ?
Myriam Quemener : Les pays européens ont harmonisé leurs législations et la coopération internationale se renforce en permanence. La Convention de Budapest, seul traité relatif à la lutte contre la cybercriminalité, a déjà été signée par 46 pays, et d'autres États sont actuellement en négociation pour y adhérer. Pour ce qui concerne la France, notre pays dispose d'un arsenal ancien, en particulier la loi de 1988 dite « loi Godfrain » qui permet de réprimer les piratages informatiques et les cybermenaces. Cet arsenal s'est progressivement enrichi et perfectionné pour permettre le recours à des procédures adaptées à l'univers numérique. De nouvelles structures sont nées, comme l'Anssi, qui met en œuvre la stratégie gouvernementale en matière de cybersécurité, mais aussi une nouvelle sous-direction de lutte contre la cybercriminalité et un pôle numérique au parquet de Paris qui a vocation à s'étoffer. On a aussi créé le procureur de la République financier à compétence nationale exclusive en matière de délits boursiers et pour les affaires économiques et financières complexes qui sont aussi souvent à dimension internationale.

Quels sont les nouveaux moyens d'investigation des enquêteurs pour déjouer les attaques ?
Sur le plan procédural, le législateur a transposé le régime des interceptions téléphoniques à Internet. Il a aussi innové en prévoyant l'infiltration numérique, qui est une enquête sous pseudonyme. Elle permet à l'enquêteur d'utiliser un nom d'emprunt pour entrer plus facilement en contact avec le cyberdélinquant. Depuis la loi du 13 novembre 2014, l'enquête sous pseudonyme jusqu'alors utilisée en matière de pédopornographie et de contrefaçon s'applique à l'ensemble des procédures de criminalité organisée.

Les données personnelles sont considérées comme « l'or noir du XXIe siècle ». La semaine dernière, une importante base de données américaine abritant les coordonnées, données de santé et autres informations personnelles d'environ 20 millions de fonctionnaires a été piratée. Quel usage les cyberdélinquants font-ils des données récupérées, et à quoi peut-on s'attendre dans les années qui viennent ?
Ils récupèrent ces données et les revendent sur les marchés noirs du Web (Darknet) qui sont des réseaux parallèles aux réseaux ouverts du type Google. Cela permet par exemple de faire des achats sous de fausses identités ou d'obtenir des virements en se faisant passer pour une entreprise connue. Les données personnelles servent aussi à créer de faux profils, et tout cela se répercute sur l'e-réputation des entreprises. L'usurpation d'adresses IP (spoofing) qui permet de commettre des fraudes à la téléphonie mobile se développe aussi de manière considérable.

Quels sont les prochains défis de la criminalité astucieuse sur Internet ?
En cette période où le terrorisme frappe de façon dramatique, il est important de s'attaquer avec vigueur au financement du terrorisme, et cette lutte passe par une politique publique pragmatique et déterminée contre des phénomènes comme le cyberblanchiment ou les escroqueries aux faux ordres de virement.
Il faut par ailleurs être attentif et vigilant face à des outils numériques comme le crowdfunding (financement participatif) ou les crédits à la consommation. Les sommes obtenues au travers de ces formes de prêt peuvent en effet servir à financer des activités illicites. Il en est de même du « trading haute fréquence » qui permet d'envoyer des ordres d'achat à une vitesse de l'ordre de la nanoseconde, grâce à des algorithmes superpuissants, permettant des manipulations de cours. Le courtage à haute fréquence a aussi ses dérives : un courtier londonien a récemment été arrêté pour une manipulation sur le marché des contrats à terme électroniques aux États-Unis, qui avait contribué au mini-krach de mai 2010 à Wall Street.
Il faut aussi suivre avec attention le développement de ces fameuses « monnaies virtuelles » qui contournent le système bancaire et permettent d'échapper à tout contrôle étatique en raison de l'absence de traçabilité. Les objets connectés, qui favorisent l'usurpation de profils complets, et le cloud computing qui contient des données sensibles à valeur commerciale sont aussi des cibles potentielles de cyberattaques. D'autant que de nombreuses failles de sécurité existent et peuvent être exploitées par les cybercriminels.

Qu'est-ce qui dissuade vraiment les délinquants, qu'ils soient isolés ou membres d'organisations criminelles ?
La mise en place d'une stratégie globale au niveau des services de l'État est de nature à dissuader les cyberdélinquants, de même que les condamnations et démantèlements de réseaux de cybercriminels qui ne cessent d'augmenter grâce aux moyens d'investigation et à l'expertise de plus en plus pointue des enquêteurs dédiés.

Pensez-vous que l'Internet a démultiplié les risques, ou les a-t-il seulement déplacés ?
L'absence de confrontation physique auteur-victime, propre à Internet, facilite le passage à l'acte. Le système des rencontres virtuelles attire des personnes mal intentionnées qui peuvent plus facilement extorquer de l'argent, notamment via des sites de vente entre particuliers. Aujourd'hui, la cybercriminalité s'industrialise et s'organise sous forme de structures hiérarchisées allant de la main-d'œuvre de base qui récupère des données jusqu'aux têtes de réseau qui donnent les ordres.

Ces phénomènes sont-ils, comme le changement climatique, irréversibles ?
Je ne le pense pas, car, actuellement, il y a une mobilisation importante, du secteur tant public que privé, pour lutter contre ces phénomènes. Il est indispensable de multiplier les actions de formation pluridisciplinaire des acteurs publics et privés qui concourent à la lutte contre ces attaques. Cependant, il ne faut pas perdre de vue que ce type de délinquance lance un défi au temps judiciaire, c'est même une course contre la montre !

L'ouvrage en vente ici

Source : http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/cybercrime-un-defi-lance-au-temps-judiciaire-13-07-2015-1943938_56.php

---

La mise en place de la riposte contre la cybercriminalité | Le Net Expert Informatique

La mise en place de la riposte contre la cybercriminalité

Le 08 juillet 2015, c'est-à-dire le mercredi dernier, l'Observateur permanent du Canada au Conseil de l'Europe, Alan Bowman, a déposé l'instrument de ratification de la Convention de Budapest sur la cybercriminalité, faisant ainsi de ce pays le 47ème Etat partie à ce mécanisme international de lutte contre la cybercriminalité.

Au dernier décompte, 07 autres États ont signé la Convention et 12 ont été invités à y adhérer, ce qui porte à 66 le nombre des États Parties ou qui se sont officiellement engagés à devenir Parties au traité.
« La Convention sur la cybercriminalité, aussi connue comme la Convention de Budapest sur la cybercriminalité ou Convention de Budapest, est le premier traité international qui tente d'aborder les crimes informatiques et les crimes dans Internet en harmonisant certaines lois nationales, en améliorant les techniques d'enquêtes et en augmentant la coopération entre les nations. Il a été rédigé par le Conseil de l'Europe avec la participation active d'observateurs délégués du Canada, du Japon et de la Chine.

Qu'est ce que la cybercriminalité ?
À la fin d'août 2011, plusieurs pays européens avaient signé le traité ». Selon une revue de la littérature disponible sur la question, la cybercriminalité reste encore un concept difficile à appréhender. En France, un rapport du groupe de travail interministériel sur la lutte contre la cybercriminalité datant de février 2014 appréhende la question dans toute sa complexité. Au regard de cette complexité, le rapport note que la Commission européenne a du s'en expliquer dans une communication au Parlement européen en date du 22 mai 2007 en ces termes : "Faute d'une définition communément admise de la criminalité dans le cyberespace, les termes 'cybercriminalité', 'criminalité informatique' ou 'criminalité liée à la haute technologie' sont souvent utilisés indifféremment".
La question préoccupe aussi l'OCDE selon laquelle « la cybercriminalité renvoie à tout comportement illégal contraire à l'éthique ou non autorisé qui concerne le traitement automatique de données et/ou de transmissions de données ».

Que dit l'ONU ?
Pour l'organisation mondiale, tombe sous le coup de la cybercriminalité « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent ». Pour autant qu'elle offre des outils juridiques susceptibles d'aider les pays à enquêter sur la criminalité informatique et de poursuivre en justice les auteurs de ce crime, la Convention de Budapest est un instrument qui mérite une large vulgarisation surtout en ces temps de guerre asymétrique à l'échelle planétaire.
C'est une simple question de bon sens quand on sait que seule la coopération entre Etats est susceptible de porter un coup d'arrêt à cette nouvelle forme de criminalité aux conséquences imprévisibles. Mais un survol rapide de la liste des Etats parties ou qui s'apprêtent à y adhérer permet de réaliser, là aussi, que l'Afrique est encore à la traine. Alors qu'on arrête de geindre si les autres réfléchissent à notre place et nous imposent leurs quatre volontés.

Source : http://malijet.com/la_societe_malienne_aujourdhui/132840-chronique-du-web-la-riposte-contre-la-cybercriminalite-se-met-en.html

Le Canada adhère à la Convention de Budapest – Conseil de l’Europe | Le Net Expert Informatique

Le Canada adhère à la Convention de Budapest – Conseil de l’Europe

L’Observateur permanent du Canada au Conseil de l’Europe, Alan Bowman, a déposé ce matin l’instrument de ratification de la Convention de Budapest sur la cybercriminalité.
Ainsi, le nombre de Parties atteint 47. Sept autres États ont signé la Convention et douze autres pays ont été invités à y adhérer. Actuellement, 66 États sont des Parties ou se sont officiellement engagés à devenir Parties à ce traité.

Liste des signatures, ratifications et adhésions à la Convention de Budapest

---

Source : http://www.coe.int/fr/web/cybercrime/-/canada-joins-budapest-convention

Une convention internationale pour lutter contre le cybercrime | Le Net Expert Informatique

	Une convention internationale pour lutter contre le cybercrime

En avril 2015, la société Symantec spécialisée dans la sécurité informatique présentait son rapport annuel. Selon ses dires, en 2014, 317 millions de nouveaux programmes malveillants auraient été crées au niveau mondial. Enfin, faut-il rappeler ce qui est arrivé à nos amis de TV5 Monde, il y a de cela quelques semaines ? Ecran noir pour la chaîne les 8 et 9 avril 2015. Sans que pour le moment on sache d'où vient l'attaque.

C'est une évidence, la cybercriminalité est en pleine croissance. Multiforme, mondialisée, l'œuvre d'un petit génie malfaisant, ou d'organisations criminelles quand il ne s'agit pas d'une nouvelle arme d'Etat. Une pieuvre, Octopus…

La Convention de Budapest

Pour le moment, le seul grand texte international existant dans le cadre de la lutte contre ce type de criminalité est l'œuvre du Conseil de l'Europe. Signée à Budapest en novembre 2001, la convention traite des infractions possibles à l'égard des droits d'auteur, de la sécurité des réseaux informatique, des fraudes en général et aussi à la lutte contre la pornographie enfantine. Un texte unique en son genre, qui dépasse le seul cadre du Conseil de l'Europe. Puisque déjà 66 pays du monde entier ont adhéré. Dernier en date, il y a de cela quelques jours le Sri Lanka.

Que ce soit le Conseil de l'Europe qui est en pointe dans ce combat ne paraît pas illogique. Comme le rappelle le spécialiste de cette lutte au sein du Conseil de l'Europe, Alexander Seger, ce sont les droits de l'Homme et la démocratie qui sont en danger.

Ce texte permet avant tout de mener la bataille du droit. Il n'a pas de rapport avec les lois en cours sur le renseignement et qui font beaucoup la Une dans de nombreux pays dont la France. En revanche, devant la croissance de ce type de criminalité et le développement toujours plus rapide de la technique, ce texte doit constamment évoluer de même que les pratiques des autorités. Ainsi le Conseil de l'Europe vient-il de créer à Bucarest un bureau destiné à encadrer et à proposer une aide technique aux juristes ou aux politiques lancés dans ce combat.

De même, tous les 18 mois, une grande réunion internationale se tient avec tous les acteurs concernés. C'est cette réunion qui répond au doux nom d'Octopus. La dernière se tient à Strasbourg ces jours-ci. Ces conférences permettent de faire le point sur de nouvelles pratiques problématiques qui apparaissent. Ainsi sur le droit des victimes passablement oubliées pour le moment ou bien encore, et ce sera le thème principal des travaux, sur la difficulté pour la justice de trouver des preuves informatiques. Dans quel disque dur les trouver, quel nuage explorer ? En rappelant à nouveau qu'il ne s'agit là que d'un texte portant sur le judiciaire.

Il y a quelques semaines, à La Haye, s'est tenu également une Conférence mondiale sur le Cyber espace 2015. Cette rencontre qui prend en compte les extraordinaires possibilités qu'offre internet avait pris en compte également la question de la sécurité qui doit régner dans le cyberespace. La prise de conscience est donc bien là, il faut espérer que les techniques des criminels quels qu'ils soient n'aillent pas en se développant plus vite que les solutions. Or, et l'on revient à l'étude annuelle de Symantec, il faut désormais aux éditeurs de logiciels beaucoup plus de temps pour créer et déployer des correctifs en cas de faille sécuritaire.

Et s'il fallait vous convaincre du problème, un dernier exemple, celui des « rançongiciels ». Ils prennent le contrôle de vos PC et vous piquent littéralement vos données rendues plus tard contre rançon. Une entreprise française s'est vu réclamer ainsi 90.000 euros.

Et vous, si vous êtes amateurs de pizzas, vous risquez gros…

Lire la suite….

Source : http://geopolis.francetvinfo.fr/une-convention-internationale-pour-lutter-contre-le-cybercrime-65027

La lutte de la Cybercriminalité passe par la coopération et la formation des enquêteurs (Octopus 2015) | Le Net Expert Informatique

	Cybercriminalité: la lutte passe par la coopération et la formation des enquêteurs (Octopus 2015)

Une coopération internationale renforcée en matière de cybercriminalité et des enquêteurs mieux formés permettraient aux Etats de mieux lutter contre ce fléau, ont conclu vendredi des experts réunis à Strasbourg au Conseil de l'Europe.

Experts internationaux, juges, policiers, responsables gouvernementaux: réunis depuis mercredi à Strasbourg (est de la France), 300 participants à la conférence sur la cybercriminalité Octopus 2015 ont avancé plusieurs pistes de travail.
Parmi les domaines d'actions jugés prioritaires, une coopération internationale plus efficace, des outils et des capacités de lutte renforcés permettraient aux Etats d'être mieux armés pour poursuivre et faire condamner les auteurs d'infractions dans le cyberespace, a affirmé Gabriella Battaini-Dragoni, vice-présidente du Conseil de l'Europe, qui présentait les conclusions des participants à la conférence.
Le Conseil de l'Europe a annoncé qu'il allait « démultiplier » ses efforts pour aider les Etats qui le souhaitent à organiser un programme de formation pour juges et procureurs internationaux, a indiqué Mme Battaini-Dragoni.
L'organisation paneuropéenne, qui compte 47 Etats-membres, veut notamment aider les enquêteurs à se servir du « cloud-data », ces traces informatiques qui permettent d'identifier et de poursuivre les criminels.
Elle proposera dans un premier temps un « Guide des preuves électroniques », sous forme de glossaire informatique.
L'idée est aussi de permettre aux enquêteurs de « parler la même langue », selon Alexander Seger, chef de la division de la lutte contre la cybercriminalité au Conseil de l'Europe.
Selon M. Seger, les « territorialités » et les frontières continuent en effet de faire obstacle en matière de coopération entre enquêteurs, qui peuvent avoir besoin de trouver des éléments de preuve hébergés sur des serveurs informatiques à l'étranger.
Selon le Conseil de l'Europe, depuis 2001, 66 pays dont la France ont signé, ratifié la Convention de Budapest sur la cybercriminalité, ou ont été invités à y adhérer.
Plus de 120 pays au total coopérent avec le Conseil de l'Europe pour renforcer leur législation et leur capacité de lutte contre la cybercriminalité.

Source : http://www.notretemps.com/internet/cybercriminalite-la-lutte-passe-par-la,i88427