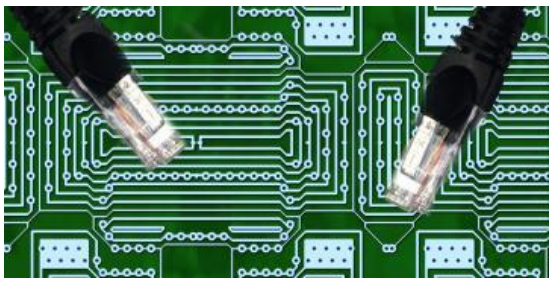
Quand le frigo vole vos données personnelles | Le Net Expert Informatique

	**Quand le frigo vole vos données personnelles**

Des experts en sécurité viennent de démontrer que des pirates, en passant par un réfrigérateur connecté, seraient capables de s'introduire sur les comptes de la messagerie Gmail de Google. Un type d'attaque informatique qui relance le débat sur les failles de sécurité des objets innombrables que nous connectons au web.

Désormais, les lave-linge commandent leur stock de lessive en ligne, les voitures tweetent à leur garagiste et toutes sortes de gadgets communicants nous aident à mieux contrôler notre environnement. L'internet des objets n'en fini plus de nous étonner en permettant d'associer des puces électroniques aux choses qui nous entourent. D'ici à 2020, quelque 200 milliards d'objets reliés à un réseau seront utilisés par les internautes sans intervention spécifique de leur part. Un nouvel eldorado économique pour les industriels de la high tech, mais aussi le paradis des pirates qui s'empresseront de piller cette nouvelle informatique qui ne possède pas un véritable système de sécurité.

Les experts tirent la sonnette d'alarme depuis des années, dénonçant le manque de protection des objets reliés en permanence à la Toile. Récemment, des hackers ont réalisé un coup d'éclat en prenant le contrôle de plus de 100 000 gadgets électroniques en les détournant de leur fonction première comme des téléviseurs, des consoles de jeux, des box internet et même un réfrigérateur connecté. Jusqu'à présent, il était inutile de s'inquiéter de ces attaques spectaculaires sur nos grille-pain, lave-linge ou autres joujoux électroniques en ligne, les cybercriminels se contentaient seulement de les dérégler.

Le problème prend aujourd'hui, une toute autre dimension, une équipe de chercheurs vient d'identifier une faille de sécurité plus inquiétante. Elle offre la possibilité à des pirates de s'introduire sur les comptes de la messagerie de Google Gmail, en passant par les cuisines de particuliers où trône le dernier modèle des réfrigérateurs intelligents de la marque Samsung. L'appareil qui gère la fraicheur de nos denrées alimentaires a été conçu pour télécharger l'agenda de notre boite électronique et de l'afficher automatiquement sur son écran intégré.

Une porte d'entrée idéale, estiment les chercheurs, qui permet aux pirates d'accéder facilement à nos courriels et à nos données confidentielles. Qu'on se rassure, jusqu'à présent, aucune intrusion de ce type n'est à déplorer, s'empressent-ils d'ajouter. La firme Samsung promet de corriger cette anomalie, mais le développement exponentiel de l'internet des objets, sans un système de sécurité pensé à l'avance, a de quoi inquiéter et risque de se métamorphoser bien vite en cyber cauchemar pour consommateurs techno-branchés.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.rfi.fr/emission/20150906-quand-le-frigo-vole-vos-donnees-objets-connectes-internet-cyber-attaque-securite
Par Dominique Desaunay

L'état des lieux de la protection des données

personnelles en Tunisie | Le Net Expert Informatique

L’état des lieux de la protection des données personnelles en Tunisie

Chawki Gaddes, président de l'INPDP explique les missions et ambitions de cette instance chargée de la protection des données personnelles.

Fruit d'un travail juridique entamé en 2002, l'Instance nationale de la protection des données personnelles (INPDP), régie par la loi organique no 2004-63 du 27 juillet 2004, n'a pu être mise en route qu'au début 2009. Et c'est avec la nomination de son 3e président, en la personne du juriste Chawki Gaddes, qui a succédé, le 5 mai 20015, au magistrat Mokhtar Yahiaoui (les présidents et les membres de l'instance sont désignés par décret pour 3 ans), que le travail effectif a réellement démarré.

«Il faut commencer par sensibiliser, vulgariser et expliquer aux Tunisiens ces notions de données personnelles et leur importance aux échelles individuelle et collective dans tout le pays», insiste Chawki Gaddes.

Les données sensibles

Le président de l'INPDP précise, dans ce contexte, que la donnée personnelle est toute information qui permet d'identifier ou de rendre identifiable une personne (articles 4 et 5 de la loi de 2004). En d'autres termes, toute information qui permet à remonter à la personne concernée : nom et prénom, date de naissance, adresse aussi bien physique qu'électronique, numéro de téléphone, plaque minéralogique de la voiture, numéro d'identification, empreintes digitale ou rétinienne, photo, code génétique, état de santé, opérations bancaires, traces informatiques… «Et la liste n'est pas close, car la science et les techniques évoluent et élargissent davantage le champ de définition de cette notion», ajoute M. Gaddes.

Il y a, en effet, aussi, des données que l'on a pris l'habitude de qualifier de «sensibles»: origine raciale ou génétique, convictions religieuses, opinions politiques, antécédents judiciaires… «Ces données sont, par principe, interdites de traitement», souligne le président de l'INPDP. Et on entend par traitement toutes les opérations réalisées de manière automatique ou manuelle sur les données personnelles. Elles touchent à tout le cycle de la vie d'une information, de sa naissance jusqu'à sa mort : la collecte, l'enregistrement, la conservation, l'organisation, la modification, l'exploitation l'expédition…

Des règles à respecter

Toutes ces opérations doivent respecter les règles définies par la loi qui stipule dans son article premier que toute action sur les données personnelles doit se faire «dans le cadre de la transparence, la loyauté et le respect de la dignité humaine».

L'opération de traitement doit être connue de la personne concernée et de l'instance de contrôle. Aucun fichier n'est créé ni géré dans le secret, et l'INPDP mettra en ligne sur son site la base de données relatives à tout traitement sur le territoire national. Cela permet au citoyen (et à tout résident) de savoir où les données sont collectées et auprès de qui il peut y accéder et éventuellement s'y opposer. Il s'agit d'éthique, de confiance et d'honnêteté de sorte que la finalité du traitement soit définie à l'avance sans être détournée vers d'autres buts

En définitive, traiter les données personnelles c'est se mettre à l'esprit que l'on gère des êtres humains et non des choses. Il y va donc de la dignité humaine. Le citoyen, de par l'article 24 de la Constitution, a le droit à la préservation de sa vie privée contre toute intrusion qui, de nos jours, est mise à rude épreuve eu égard au recours intensif aux technologies de l'information et de la communication.

La Convention 108

Dans un monde sans frontières, la question n'a pas été laissée au hasard. En effet, les premiers pas dans le domaine de la protection des données personnelles remontent à 1974, en France, avec l'institution d'un identifiant unique, un projet en cours de réalisation en Tunisie.

L'idée a, depuis, fait beaucoup de chemin, malgré l'opposition d'une commission parlementaire française qui considère qu'il s'agit, bel et bien, d'une atteinte aux libertés des individus. C'est ainsi que la loi «Informatique et Liberté» a vu le jour en 1978 pour instituer les règles essentielles en la matière qui ont servi de support à la Convention 108 du Conseil de l'Europe.

La Tunisie, soucieuse de se conformer aux pratiques internationalement reconnues en matière de respect des droits humains, a demandé, en juillet dernier, à adhérer à cette convention en vue d'instaurer un climat de confiance aussi bien vis-à-vis de ses citoyens que des intervenants étrangers. Elle sera le 5e Etat non-européen à adhérer à cette convention, après l'Uruguay, l'Ile Maurice, le Maroc et le Sénégal.

La Tunisie sera, ainsi, labellisée «espace de confiance» dans le monde et pourra faire partie des marchés de traitement des données personnelles (ou offshoring) «qui contribuera à la création de 50.000 postes d'emploi et à une rentrée de devises de pas moins de 2000 millions de dinars. Encore faut-il qu'elle réussisse sa bataille contre la violation des données personnelles», tient à affirmer le président de l'INPDP

L'Europe a fortement besoin d'externaliser le traitement des données personnelles, compte tenu des coûts assez élevés de cette opération dans l'espace européen, et la Tunisie est appelée à saisir cette opportunité, à l'instar de l'Inde ou de la Roumanie, qui profitent déjà de ce filon.

Les abus et des sanctions

La loi qui garantit tous les droits en matière d'usage des données personnelles a prévu aussi des sanctions qui vont de l'amende, légère ou lourde (pouvant atteindre 50.000 dinars), jusqu'à la peine de 2 à 5 ans de prison lorsqu'il s'agit de communication ou de transfert de données vers l'étranger

Pour se rendre compte de l'acuité de cette problématique et de ses retombées sur la vie de tous les jours, il faut parcourir la liste des infractions possibles et qui pourraient passer inaperçues, telle l'installation des vidéo-surveillance dans les lieux autres que ceux ouverts au public, ainsi que la liste des peines et des pénalités encourues.

Bref, c'est tout un chantier qui est ouvert devant l'INPDP, qui se donne pour mission d'inculquer et divulguer la culture de la préservation des données personnelles et sensibiliser le citoyen sur ses droits dans ce domaine.

Quand on sait que jusqu'au mois de mai 2015, aucun dossier se rapportant à un abus commis dans ce domaine n'a encore été traité et qu'aucun rapport d'activité n'a été ni élaboré ni présenté, on mesure le chemin qui reste à faire dans ce domaine. «Nous comptons sur la société civile et sur les médias pour nous aider dans cet effort de communication en faveur de la préservation des données personnelles», conclue Chawki Gaddes.

Source : http://kapitalis.com/tunisie/2015/09/06/chawki-gaddes-letat-des-lieux-de-la-protection-des-donnees-personnelles-en-tunisie/
Propos recueillis par Wajdi Msaed

Un nouveau Virus vise les iPhones et l’iPads | Le Net Expert Informatique

	Un nouveau Virus vise les iPhones et l’iPads

Cette nouvelle #famille de virus, baptisée « #KeyRaider« , s'attaque à des iPhone et iPad débloqués pour y installer des applications non approuvées par Apple.

« Nous pensons que c'est le plus grand vol connu de comptes Apple causé par un virus », indique la société de sécurité informatique américaine Palo Alto Networks.©CAROLINE SEIDEL

Des chercheurs en sécurité informatique affirment avoir identifié une nouvelle famille de virus, baptisée « KeyRaider », qui s'attaque à des iPhone et iPad débloqués pour pouvoir y installer des applications non approuvées par Apple. « Nous pensons que c'est le plus grand vol connu de comptes Apple causé par un virus », indique la société de sécurité informatique américaine Palo Alto Networks sur son site internet, où elle résume les résultats d'une enquête réalisée avec WeipTech, un groupe technique amateur réunissant des fans d'Apple en Chine.

« KeyRaider a ainsi déjà réussi à voler plus de 225 000 comptes Apple valides » avec leurs mots de passe, qui ont été retrouvés stockés sur un serveur, ainsi que « des milliers de certificats, clés privées et tickets d'achats », précise Palo Alto Networks. Le virus fonctionne en interceptant les communications de l'appareil avec iTunes, la boutique de musique en ligne d'Apple. Il vole et partage des informations d'achats à l'intérieur d'applications et désactive la fonction de déblocage locale ou à distance de l'iPhone ou de l'iPad.

Dix-huit pays touchés

Certaines des victimes ont constaté des achats anormaux, d'autres ont vu leur appareil bloqué par des pirates qui leur ont demandé une rançon, indique encore la société de sécurité informatique. KeyRaider s'attaque aux appareils utilisant iOS, le système d'exploitation mobile d'Apple, qui ont été débloqués et est distribué en Chine par l'intermédiaire de Cydia, une application non officielle pour iOS donnant accès à des applications non validées par Apple.

Palo Alto Research estime au total que des consommateurs de 18 pays ont été touchés, dont la Chine mais aussi la France, la Russie, le Japon, le Royaume-Uni, les États-Unis, le Canada, l'Allemagne, l'Australie, Israël, l'Italie, l'Espagne, Singapour et la Corée du Sud.

Un porte-parole d'Apple a souligné dans un courriel que « le problème ne touche que ceux qui non seulement ont débloqué leurs appareils (pour permettre des utilisations non utilisées par le fabricant, NDLR) mais ont aussi téléchargé le virus depuis des sources non fiables ».

« L'iOS est conçu pour être fiable et sûr à partir du moment où on allume l'appareil. Pour protéger nos utilisateurs des virus, nous surveillons le contenu de l'App Store et nous assurons que toutes les applications dans l'App Store adhèrent aux lignes directrices fixées pour nos développeurs », a-t-il rappelé. Il a toutefois assuré qu'Apple avait pris « des mesures pour protéger ceux affectés par le problème en aidant les propriétaires à réinitialiser leurs comptes (en ligne) iCloud avec un nouveau mot de passe ».

Lire la suite….

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://www.lepoint.fr/high-tech-internet/piratage-informatique-l-iphone-et-l-ipad-vises-par-un-nouveau-virus-02-09-2015-1961181_47.php

---

Conférence internationale sur la protection des données personnelles au Maroc| Le Net

Expert Informatique

	**Conférence internationale sur la protection des données personnelles au Maroc**

Le Maroc abritera en 2016 la 38ème édition de la Conférence internationale des commissaires à la protection des données et à la vie privée (CICPDVP).

Cette décision consolide le modèle marocain en matière de protection des données personnelles au sein de son aire géographique et culturelle, relève un communiqué de la Commission nationale de contrôle de la protection des données à caractère personnel (CNDP) parvenu à la MAP.
Le choix du Maroc a été décidé à la suite de la recommandation du Comité exécutif de la Conférence, qui a examiné les dossiers de candidature de quatre Autorités en lice pour accueillir cette importante manifestation internationale, relève-t-on de même source, ajoutant que le dossier de candidature du Maroc, préparé et défendu par la CNDP a été considéré comme prometteur et sérieux, selon les critères établis par le Comité exécutif.
La CICPDVP est la principale organisation internationale œuvrant dans le domaine de la protection des données personnelles et de la vie privée, rappelle la CNDP, précisant qu'elle compte 101 membres et 17 observateurs, représentant les instances spécialisées dans ce domaine.
Depuis 1978, la CICPDVP tient une conférence annuelle à laquelle assistent des représentants des gouvernements, des organisations internationales, des entreprises privées, des organismes de la société civile et du monde universitaire.
Ce rendez-vous annuel permet aux différents spécialistes et experts de partager leur expertise et leur expérience et de s'informer sur les sujets d'actualité affectant la protection de la vie privée et des données personnelles.
Il contribue aussi au renforcement de la coopération au sein de la communauté internationale de la protection de la vie privée.

Source : http://www.libe.ma/Conference-internationale-sur-la-protection-des-donnees-personnelles_a65532.html

Votre frappe au clavier vous identifie tout aussi efficacement qu’une écriture à la main | Le Net Expert Informatique

	Votre frappe au clavier vous identifie tout aussi efficacement qu’une écriture à la main

Des chercheurs français ont mis au point un logiciel capable de reconnaître avec précision un utilisateur qui tape au clavier d'ordinateur. Une possibilité qui permet de sécuriser des opérations mais qui supprime aussi l'anonymat sur Internet.

Webcam débranchée, pare-feu, IP masquée, VPN… Les internautes aguerris et concernés par leur anonymat sur internet connaissent le minimum requis pour se fondre dans les méandres du web. Qu'ils soient honnêtes ou malhonnêtes, ils pourront bientôt être identifiés et cela n'a plus rien à avoir avec un quelconque logiciel de pistage. Ce qui va trahir les internautes, ce sont leurs doigts. Ou plutôt la façon dont ils vont les utiliser sur leur clavier. Des chercheurs français du Groupe de recherche en informatique image automatique et instrumentation de Caen (Greyc) ont ainsi développé un petit logiciel pilote qui permet de différencier avec une grande précision les différents internautes qui tapent sur leur clavier.
Pour cela, le programme repère la pression exercée sur les touches, le temps d'appui et surtout les délais, très courts, entre chaque touche. Telle une graphologie moderne, tous ces critères s'avèrent très différents en fonction des personnes et permet de donner un profil précis.
« Ce n'est pas nouveau » remarque Jean-Paul Pinte, docteur en information scientifique et technique et maître de conférences à l'Université Catholique de Lille. « Avant l'arrivée des claviers, pendant la Seconde Guerre Mondiale, les opérateurs de renseignement britanniques écoutaient les opérateurs de code morse allemands. La vitesse de code, les erreurs de frappe permettait de différencier les opérateurs. »
Au cours des années 2000, avec l'avènement d'internet, la « frappologie » a été de plus en plus étudiée, dans le même esprit que la graphologie, censée apporter des informations sur la personnalité d'une personne. « C'est surtout dans l'espionnage que cette biométrie dite douce a pris racine mais elle est de plus en plus pratiquée dans le monde du recrutement » souligne Jean-Paul Pinte. Sauf que les techniques se sont largement améliorées et les recherches du Greyc et d'autres chercheurs dépassent le cadre du simple profiling de personnes.

Le but est avant tout de toujours mieux crypter les données. Ainsi, même en connaissant le mot de passe de sa victime, un usurpateur ne passerait pas entre les mailles du filet sécuritaire puisque sa façon de taper le mot magique serait forcément différente de celle du véritable utilisateur.

Mais ce système offre aussi des perspectives plus sombres car il permet d'identifier une personne à coup sûr, malgré tous ses efforts pour rester anonymes.

Il suffit que plusieurs gros sites s'y mettent et les voilà en possession de toutes les pages visitées par une même personne, identifiée par son clavier. Dans ce cas, l'adresse IP n'aurait plus vraiment d'enjeu. Et ce ne sont pas les réseaux masqués, comme le célèbre TOR qui empêcheront cela. Runa Sandvik, un chercheur indépendant interrogé par le site Arstechnica, a tenté l'expérience et s'est rendu compte que le système chargé normalement de le maintenir anonyme, n'a pas pu lutter. « Aujourd'hui, tout est possible même avec TOR » souligne Jean-Paul Pinte. « La recherche évolue dans le domaine car il faut savoir que l'anonymat n'existe pas vraiment sur la toile. »

L'entreprise suédoise BehavioSec met d'ailleurs à disposition un site d'essai pour évaluer l'efficacité du système pour un site de vente en ligne. Au bout de 3 formulaires (similaires) remplis, le programme était capable de retrouver l'utilisateur dans 75% des cas ultérieurs… Cela concerne les internautes attachés à leur anonymat mais aussi les dissidents politiques de certains pays qui surveillent la toile.

Mais d'ores et déjà, la riposte s'organise. Les chercheurs Per Thorsheim et Paul Moore ont développé un petit plugin pour le navigateur de Google Chrome qui permet de crypter les informations liées au clavier. Si le programme est encore en phase de test, il pourrait être une nouvelle protection à ajouter pour qu'internet reste un espace de liberté.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.atlantico.fr/decryptage/comment-maniere-dont-tapez-votre-clavier-identifie-tout-aussi-efficacement-qu-ecriture-main-2268834.html
Illustration : On peut désormais vous identifier à la manière dont vous tapez sur le clavier de votre ordinateur. Crédit Reuters

---

Pour une politique européenne

du traitement massif des données | Le Net Expert Informatique

	Pour une politique européenne du traitement massif des données

En matière de vie privée et de données personnelles, les régimes juridiques et surtout la perception culturelle des enjeux sont très différents outre-Atlantique et en Europe. Logiquement, il en résulte des législations et des comportements eux-mêmes différents, avec une liberté d'action plus encadrée en Europe.

Ces écarts ont abouti, tout récemment, à la mise en œuvre du fameux « droit à l'oubli », qui ne s'applique qu'en Europe et dont les Américains craignent et refusent la globalisation, avec un argumentaire au moins autant culturel que juridique. Ce qui est reproché à l'Europe, ce n'est pas tant d'avoir sa propre conception de la vie privée que de chercher à en imposer l'application au monde entier.

Un droit à l'oubli très relatif

Ce droit à l'oubli est d'ailleurs très relatif, puisqu'il est possible de le contourner en effectuant ses recherches sur le moteur dédié à un pays hors-Union européenne. Mais bien peu d'entre nous vont au-delà des résultats affichés sur la première page, dans notre langue natale, par notre moteur de recherche préféré.

L'importance du problème va se démultiplier avec le développement des algorithmes prédictifs et de l'intelligence artificielle, qui s'attaquent à l'existence même de la frontière entre données personnelles ou vie privée et informations publiques.

De nouveaux outils aux marges de la loi

Ces outils requièrent de moins en moins de données personnelles ou d'intrusions caractérisées dans la sphère privée, au sens de la loi, pour identifier les personnes et leur comportement car ils se fondent sur l'analyse des « signaux faibles ».

Les législations actuelles nécessitent quant à elles, pour être mises en œuvre, l'identification de l'usage de données personnelles ou des « actes » portant atteinte à la frontière de la vie privée. Donc les atteintes aux données personnelles ou à la vie privée qui sont inévitables pour la mise en œuvre des nouveaux services auront de moins en moins à passer par ce que les législations utilisent pour les qualifier ; qu'il s'agisse d'analyses des réseaux sociaux pour vous accorder un prêt ou de celle du contenu de votre mobile pour vous proposer des recommandations musicales.

Une réforme déjà dépassée ?

Quelle que soit sa pertinence pour les technologies actuelles, la réforme du droit européen des données personnelles pourrait donc être rapidement dépassée, et même l'introduction d'une obligation de privacy by design manquera son but s'il n'est pas plus largement débattu de ce sur quoi elle doit porter.

La réflexion ne doit plus porter sur les données utilisées mais sur les objectifs des services, quelles que soient les données utilisées ou les méthodes employées pour les traiter. L'analyse doit s'effectuer sur les coûts et avantages de chacun des services : lesquels les Européens accepteront d'intégrer dans leur quotidien ? desquels préféreront-ils se priver ?

Ainsi le défi européen est de définir une véritable politique du traitement des données, de leurs utilisations et surtout des objectifs de ces utilisations, au travers une typologie des buts poursuivis, non uniquement de la nature des données utilisées, qui seront toujours plus diluées dans la masse et donc toujours plus incontrôlables. L'argumentaire des défenseurs de la loi sur le renseignement n'était-il pas : « Nous ne nous regardons pas le contenu des messages, nous n'analysons que les métadonnées » ?

Le véritable enjeu : quels objectifs, quelles méthodes, quels usages ?

Dans ces conditions, le débat sur le traitement massif des données, s'il ne s'intéresse qu'aux données personnelles ou à la vie privée stricto sensu, relève du combat d'arrière-garde.

Certes, le progrès technique peut difficilement être interrompu ; mais l'usage qui en est fait doit générer de vrais débats de société, afin que ces évolutions soient acceptées et non subies. Et l'échelon européen offre le cadre juridique, politique et philosophique naturel de ces débats.

Si ces enjeux devaient être escamotés, c'est toute la conception européenne de la vie privée et de la protection des données personnelles qui sera débordée, tôt ou tard, par l'évolution des technologies – en douceur certes, mais irrévocablement et sans que les législations actuelles ne puissent rien empêcher.

Source : http://blogs.lexpress.fr/passe-droits/europe-donnees/
Par Rubin

Le Summer Camp de la NSA, école de cybersécurité | Le Net Expert Informatique

Le Summer Camp de la NSA, école de cybersécurité

29 universités ont accueilli cet été des jeunes pour les initier aux rudiments de la sécurité informatique. Le tout financé par l'agence américaine de renseignement.

Comprendre les écoutes des présidents français par la NSA

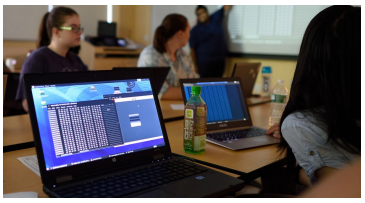
Un été entre ados dans de grands espaces bucoliques, avec canoë et camping au coin du feu ? Pas cette fois. Cet été, 1.400 collégiens et lycéens américains ont été accueillis dans 29 universités pour des « summers camps » qui ne ressemblent pas au traditionnel camp de vacances.

Au fond d'universités aux allures d'hôpitaux, ils ont passé l'essentiel de leur temps dans des salles de classes jaunies, éclairées aux néons, le nez rivé sur un écran d'ordinateur. Normal : ils ont participé au programme GenCyber, pour « Inspirer la nouvelle GENération de professionnels du CYBERespace ». Plus simplement, les « stagiaires » sont venus apprendre à bidouiller dans le code d'ordinateurs. Et devinez qui est le mécène de ces cours d'été pour apprentis-hackers ? La NSA.

Oui, la « No Such Agency », longtemps considérée comme l'agence de renseignement la plus secrète du monde, mais dont les pratiques d'espionnage massif des Américains (et du reste du monde) ont été mises en lumière par les révélations de son ancien consultant Edward Snowden, puis de WikiLeaks.

Pourquoi donc la NSA, avec son budget annuel de plus de 10 milliards de dollars, ses 850.000 employés et ses « clients » comme la CIA ou le FBI, s'enquiquine-t-elle à organiser des camps d'été ?

« Notre ambition est d'intéresser les jeunes à la cybersécurité », nous explique le créateur et directeur du programme, Steve LaFountain. « Il y a entre 600.000 et 1 million d'emplois dans la cybersécurité qui ne sont pas pourvus aux Etats-Unis, parce que nous n'avons pas assez de gens entraînés à cette discipline. GenCyber vise à combler ce gap. »



Une enveloppe de 4 millions de dollars

D'une fac à l'autre, l'enseignement varie : le camp de San Bernardio (Californie) s'attarde sur les drones, tandis qu'au camp de Norwich (Vermont) les élèves fabriquent leurs propres ordinateurs, depuis l'assemblage des puces jusqu'au logiciel de sécurité interne, et peuvent le rapporter chez eux.

Lors des 47 camps organisés cet été, une vingtaine d'ados sont accueillis pendant une ou deux semaines, totalement gratuitement. Chaque camp représente un budget moyen 85.000 dollars, pour une enveloppe totale de 4 millions de dollars. L'ensemble est financé par la NSA et la National Science Foundation (NSF), équivalent américain de notre CNCRS (Centre national de la recherche scientifique). Les universités y sont aussi de leur poche, mais seulement pour la rémunération des professeurs, soit « une dizaine de milliers de dollars », selon Nasir Memon, responsable du programme à l'université de New York.

Derrière ces summer camps pointe l'objectif inavoué par la NSA, pas connue pour sa philanthropie, de repérer une nouvelle génération de petits génies de la sécurité informatique, et de les attirer dans les rangs de l'agence. Depuis les révélations de Snowden, la NSA peine à séduire les talents dont elle a besoin. Difficile pour l'espionne controversée de rivaliser avec l'esprit libertaire de la Silicon Valley et ses salaires mirobolants. Rien que pour cette année, l'agence serait à la recherche de 1.600 recrues, dont plusieurs dizaines dans la cybersécurité.

Steve LaFountain a été chargé de mettre en place plusieurs programmes pour attirer les talents universitaires, et il en a profité pour lancer les camps d'été pour collégiens et lycéens. L'intéressé se défend d'une quelconque ambition de repérer de (très) jeunes recrues :

« Il s'agit uniquement de les intéresser à la sécurité informatique », nous rétorque-t-il avec vigueur. « En offrant ce programme gratuitement, nous espérons bousculer les barrières économiques et géographiques qui empêchent les jeunes — en particulier ceux avec un faible accès à l'informatique dans leurs classes — d'apprendre les fondamentaux de la cybersécurité. »

« Un impact dans la formation des talents »

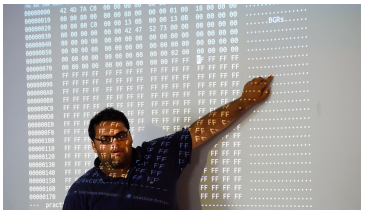
Les universités s'affichent sur la même ligne. Le programme GenCyber viserait uniquement à faire connaître les études de sciences informatiques aux lycéens du coin.

Ils font quelque chose de constructif et s'ouvrent à une nouvelle discipline », estime Nasir Memon, de l'université de New York. « En répétant l'opération partout dans le pays, le gouvernement a un vrai impact dans la formation des talents. »

Les facs insistent au passage sur le fait que la NSA laisse toute latitude aux instructeurs pour définir l'organisation et le programme du camp d'été. A l'université de New York, les professeurs entendent inciter des lycéennes à poursuivre un cursus dans leur département, en formant des apprenties-hackers sur deux semaines.

Le terme « hacker » s'avère d'ailleurs quelque peu galvaudé, puisqu'il ne s'agit pas d'apprendre des techniques pour pirater des sites gouvernementaux ou des bases de données bancaires, mais plutôt de savoir mettre les mains dans le cambouis informatique.

Nous ne leur montrons pas d'outils de piratage mais plutôt ceux permettant de trouver ce qui ne va pas, dans l'optique de résoudre des crimes, d'aider les autres », précise Linda Sellie.



« On leur montre jamais rien d'illégal »

De 8h à 15h, dans une salle blafarde du deuxième étage de l'école polytechnique de l'université de New York, cette professeure spécialiste des algorithmes enseigne à une vingtaine de jeunes filles, bit par bit, le fonctionnement de la machine, de la programmation, des réseaux et d'internet, des bases de données, du cryptage… L'ambiance est studieuse. Sous des dizaines de lignes de code incompréhensibles projetées au tableau, les adolescentes s'affairent à changer des chiffres et des lettres blancs sur leurs écrans.

« C'est de la programmation informatique, ces lignes vont créer les pixels de la photo », nous explique Ashley, 17 ans, dans un sourire qui dévoile un appareil dentaire. « A la ligne 48, allez modifier les données pour dissimuler votre message dans l'image », lance sibylline Linda Sellie.

On leur montre comment l'informatique fonctionne, comment détecter des vulnérabilités et comment les réparer, mais jamais rien d'illégal », nous assure la seconde professeure, Phyllis Frankl.

A New York, trois sessions successives ont été organisées cet été, pour un total de 75 étudiantes, l'université ayant décidé de réserver ses camps aux filles, particulièrement peu présentes dans ce type de filières. Elles ont pour seul point commun d'être de bonnes élèves dans les écoles publiques environnantes. Iman, qui porte fièrement le voile islamique du haut de ses 17 ans, vient de Brooklyn et raconte être venue « pour faire quelque chose de [son] été ». Radhaka, 17 ans et d'origine pakistanaise, vit elle dans le Queens et a été encouragée ses profs « parce qu'[elle] veut devenir développeur ». Cachée derrière ses lunettes à monture large, Winxy, 18 ans, du Bronx, a vu dans ce camp « l'opportunité d'apprendre comment fonctionnent les ordinateurs », parce que « c'est toujours utile ».

Le professeure Linda Sellie note :

« Ces filles viennent avec une connaissance minimale en informatique. Elles repartiront avec une ouverture d'esprit vis-à-vis de la cybersécurité et surtout un usage plus prudent d'internet et des technologies. »

« C'est quoi déjà la NSA ? »

Si les lycéennes sont studieuses et appliquées dans leur apprentissage, elles semblent totalement indifférentes à la question de l'espionnage mené par la NSA. « C'est quoi déjà la NSA ? », interroge Iman, les sourcils froncés. Radhaka tente :

C'est l'agence de la sécurité, ils s'occupent de sécuriser des choses. »

Mira, 17 ans et originaire du New Jersey, renchérit : « Comme dans le livre 'La Forteresse digitale' », en référence au livre de Dan Brown dont l'intrigue se déroule au cœur de la NSA. Lorsque l'on évoque une surveillance généralisée des communications aux Etats-Unis, en s'appuyant notamment sur les opérateurs internet et télécom, le silence se fait. Ce sont aussi eux qui financent ce camp d'été, glisse-t-on enfin. « S'ils nous aident à étudier une discipline compliquée gratuitement, alors ils sont biens », rétorque Ashley.

L'agence, qui espère proposer 200 camps d'ici 2020, dont au moins un par Etat, semble avoir cette année rempli son objectif. Dès la fin du premier jour de camp à New York, plusieurs élèves disent déjà envisager de travailler dans la cybersécurité, et pourquoi pas pour la NSA. C'est le cas de la discrète Ashley, qui se dit « très excitée par ce qu'elle fait ». Son nouveau défi : décoder un message dissimulé dans des photos de la Skyline de New York, pour résoudre une enquête sur un meurtre fictif.

Former des apprentis-hackers oui, mais à condition qu'ils restent du bon côté des autorités.

Source : http://tempsreel.nouvelobs.com/tech/20150828.OBS4906/a-l-ecole-de-la-cybersecurite-bienvenue-au-summer-camp-de-la-nsa.html

Par Boris Manenti

Top 5 des arnaques du moment en Côte d’Ivoire | Le Net Expert Informatique

	**Top 5 des arnaques du moment en Côte d’Ivoire**

A mi-parcours de son activité 2015, la Plateforme de Lutte Contre la Cybercriminalité (PLCC) dans un souci de prévention, vous présente à travers cet article, les arnaques auxquels vous pourriez être confronté, parce que prisées par les cyberdélinquants. Voici le top 5 des arnaques du semestre écoulé, en nombre de dossiers traités, sur les 491 dossiers reçu par la PLCC, et leurs préjudices enregistrés, sur les 1 milliard 199 millions 319 milles 880 Fcfa de dommage subit par les victimes des 6 premiers mois de l'année 2015.

1- L'ACCÈS FRAUDULEUX À UN SYSTÈME D'INFORMATION

Cette arnaque concerne les détournements de transfert d'argent. C'est une escroquerie qui consiste pour le cyberdélinquant à faire à votre insu le retrait d'une somme d'argent qui vous est destinée via une institution de transfert d'argent. Elle occupe la première place de notre classement, avec 91 dossiers traités par la PLCC, pour un préjudice estimé à 68 millions 903 milles 772 F CFA. Ce sont les populations ivoiriennes qui sont surtout touchées par cette infraction »nouvelle ».

2- FRAUDE SUR LE PORTEFEUILLE ÉLECTRONIQUE

Elle s'est développée avec l'avènement des services Mobile Money proposés par les compagnies de téléphonie mobile dans nos pays africains. Les cyberdélinquants s'attaquent au portefeuille électronique des utilisateurs en vidant leur compte. Avec 86 dossiers et un préjudice estimé à 37 millions 906 milles 300 F CFA, cette arnaque occupe la seconde marche du podium. Toujours avec les populations ivoiriennes qui prennent la place de victime numéro un des cyberdélinquants depuis un certain temps (voir article CYBERCRIMINALITÉ EN CÔTE D'IVOIRE: LESIVOIRIENS, PLUS TOUCHÉS PAR LES ARNAQUES).

3- L'ARNAQUE AUX FAUX SENTIMENTS

Considérée comme la »mère » des arnaques sur internet, l'arnaque aux faux sentiments, bien qu'elle soit la plus connue, continue de faire des victimes. C'est une escroquerie qui consiste pour le cyberdélinquant a utiliser les sentiments amoureux de leur proie pour leur soutirer de l'argent.
Si en nombre de dossier la baisse est significative par rapport aux semestres des années antérieurs (59 dossiers reçus), elle continue d'affoler les compteurs en terme de préjudice avec 448 millions 431 milles 586 F CFA seulement pour le premier semestre 2015 soit 37,39 % du préjudice totale, toute catégorie confondue, du premier semestre 2015, estimé à 1 milliard 199 millions 319 milles 880 Fcfa.

4- LE CHANTAGE À LA VIDÉO

Classé 4ième, le chantage à la vidéo peut être vue comme une résultante de l'arnaque aux faux sentiments. Le cyberdélinquant menace de divulguer des photos ou vidéo à caractère sexuelle de vous, prise dans l'intimité d'une relation.
Avec 54 dossiers, pour un préjudice de 66 millions 832 milles 324 F CFA, cette arnaque touche de plus en plus les Ivoiriens.

5- L'ARNAQUE AUX FAUX HÉRITAGES

La dernière place de ce top 5 revient à l'arnaque aux faux l'héritage. L'une des plus vielles ruses utilisée par les cyberdélinquants. Et pourtant, elle continue de faire des victimes. C'est une escroquerie ou tentative d'escroquerie, à la fois très ancienne et très commune encore aujourd'hui. Les escrocs vous envoient un mail vousinformant que vous avez été choisi pour toucher un fabuleux héritage providentiel.
Ce sont 37 dossiers qui ont été introduit à la PLCC, pour un préjudice qui s'élève à 407 millions 920 milles 762 F CFA.
Le nombre d'affaires et le montant des préjudices liés à ces infractions indiquent que le travail de sensibilisation contre la cybercriminalité doit se poursuivre. Car bien que la majorité de ces arnaques soit connue et expliquée à travers la toile, elles sont encore nombreuses ces personnes qui se laissent duper par les cyberdélinquants. Une fois de plus la PLCC vous invite à la prudence !!!

lu sur http://cybercrime.interieur.gouv.ci/

Source :
http://www.imatin.net/article/societe/broutages-cybercriminalite-en-cote-d-rsquo-ivoire-voici-le-top-5-des-arnaques-du-moment_30029_1440509278.html

---

Affaire Ashley Madison : deux

personnes se seraient suicidées | Le Net Expert Informatique

Affaire Ashley Madison : deux personnes se seraient suicidées

La police de Toronto enquête sur « deux cas non confirmés » de suicide, à la suite du dévoilement de l'identité de millions de clients du site web de rencontres extraconjugales Ashley Madison.

Les policiers n'ont pas donné plus de détails, expliquant que leur enquête se poursuivait. Pour sa part, l'exploitant du site offre une récompense d'un demi-million de dollars pour tout indice permettant d'arrêter la ou les personnes responsables de son piratage.

La police décrit la cyberattaque, revendiquée par le groupe Impact Team, comme étant « très sophistiquée ».

« Il s'agit de l'un des plus gros actes de piratage au monde. »

— Bryce Evans, surintendant, police de Toronto

Selon le policier Bryce Evans, la fuite de données « n'est pas un jeu » et a eu un « énorme impact social et économique ». « On parle de familles, d'enfants, d'épouses et de leurs maris. Ça va avoir un impact sur leur vie », a-t-il affirmé en précisant que la police ne se souciait pas de la nature des activités du site.

Les pirates informatiques, accusant la compagnie de tromperie, ont publié, la semaine dernière, l'identité de millions de clients, incluant des milliers de Canadiens, certains ayant des adresses courriel d'employés des gouvernements ontarien et fédéral ainsi que de la police de Toronto. Ces renseignements, toutefois, n'ont pas pu être vérifiés.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

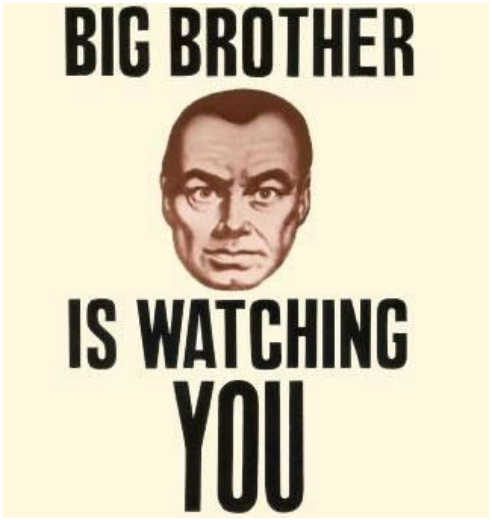
Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source :
http://ici.radio-canada.ca/regions/ontario/2015/08/24/001-ashley-madison-toronto-enquete-police.shtml

---

Alerte Faille Android ! Big Brother pourrait bien vous

surveiller | Le Net Expert Informatique

	Alerte Faille Android ! Big Brother pourrait bien vous surveiller

Des chercheurs en sécurité ont récemment découvert une faille de sécurité considérée comme la pire jamais découverte dans le système Android. Détecté dans la bibliothèque multimédia de l'OS, ce bug nommé « Stagefright » expose près d'1 milliard de terminaux Android aux malwares.

En exploitant la faille « Stagefright », les hackers peuvent accéder aux contacts et aux autres données stockées dans un appareil mobile telles que les photos et les vidéos. Ils peuvent également accéder au microphone et à la caméra de cet appareil, ce qui leur permet d'espionner l'utilisateur via l'enregistrement de son et la prise d'images.

Tous les appareils exécutant des versions Android 2.2 Froyo jusqu'aux versions 5.1.1 Lollipop sont concernés. Cela représente environ 95% de l'ensemble des terminaux Android.

Le plus effrayant, c'est que les pirates ont uniquement besoin du numéro de téléphone de l'utilisateur pour infecter son appareil. Le malware est transmis lors de l'envoi d'un message multimédia à n'importe quelle application de messagerie pouvant traiter les formats vidéo MPEG4, telle que l'application de messagerie par défaut de l'appareil Android, Google Hangouts ou Whatsapp. Comme ces applications de messagerie Android récupèrent automatiquement des vidéos ou du contenu audio, le code malveillant est exécuté sans que l'utilisateur n'ait besoin de faire quoi que ce soit. En effet, la faille n'exige pas que la victime ouvre le message ou clique sur un lien. Il s'agit d'un malware unique en son genre car ce type de menace nécessite généralement une action de la part de l'utilisateur pour que l'appareil soit infecté. Il pourrait par exemple être relayé via un lien envoyé par courrier électronique ou partagé sur les réseaux sociaux. Toutefois, cela nécessiterait encore et toujours une action de la part de l'utilisateur, puisque le chargement d'une vidéo se fait uniquement via l'ouverture d'un lien. Cela est extrêmement dangereux, car si les utilisateurs sont infectés via MMS, aucune action ne leur sera demandée et les effets indésirables seront imperceptibles. Avant même que les victimes s'en aperçoivent, le hacker est en mesure d'exécuter le code et de retirer toute trace attestant que l'appareil a été infecté.

Le rêve du cybercriminel et du dictateur

Les cybercriminels profitent de cette faille de sécurité pour espionner des millions de personnes et exécuter d'autres codes malveillants. Les gouvernements répressifs pourraient abuser de ce bug en vue d'espionner leurs citoyens ou leurs ennemis. Toutefois, ce bug pourrait également être utilisé à des fins d'espionnage apolitique. Les pirates peuvent facilement surveiller les personnes de leur entourage comme leur conjoint ou leurs voisins. Ils n'ont besoin pour ce faire que du numéro de téléphone de la personne visée. Les hackers ont aussi la possibilité de dérober des informations personnelles qu'ils utiliseront pour faire chanter des millions de personnes ou usurper leur identité. Les conséquences possibles de ce type de faille sont donc à prendre au sérieux.

Une nécessité urgente de patchs

Des patchs complets doivent désormais être fournis par les fabricants de téléphones à l'aide d'une mise à jour à distance ou « over-the-air » (OTA) d'un firmware pour les versions Android 2.2 et plus. Malheureusement, les mises à jour pour appareils Android ont toujours mis beaucoup de temps pour arriver jusqu'à l'utilisateur final. Espérons que les constructeurs réagiront plus rapidement dans ce cas précis.

Google y a pour sa part déjà répondu d'après un témoignage d'HTC publié dans le magazine d'information hebdomadaire américain Time : « Google a informé HTC de cette problématique et fourni les patchs nécessaires qu'HTC a commencé à prendre en compte dans les projets mis en œuvre au début du mois de juillet. Tous les projets en cours contiennent le patch requis. » Pour le moment et par mesure de précaution, il est recommandé aux utilisateurs de désactiver la fonction récupération automatique des MMS dans les paramètres par défaut de l'application de messagerie.

Source : http://www.journaldun
et.com/solutions/expert/61932/big-brother-po
urrait-bien-vous-surveiller-grace-a-la-faille-stagefright.shtml
Par Filip Chytrý