5% des utilisateurs de Google seraient victimes d’un adware sur leur machine | Le Net Expert Informatique

5% des utilisateurs de Google seraient victimes d’un adware sur leur machine

Google a publié les résultats d’une étude sur la publicité intrusive et plus particulièrement les adware installés sur les machines des internautes à leur insu.

Google explique que depuis le début de l’année, la société a reçu 100 000 plaintes émanant des utilisateurs du navigateur Chrome, victimes d’adware. Ces logiciels malveillants injectent littéralement de la publicité au sein des pages Web affectant leur lisibilité, mais générant également des erreurs réseau ou malmenant les performances du navigateur.
En partenariat avec l’université de Berkeley en Californie, Google annonce avoir lancé une étude dont les résultats finaux seront dévoilés au 1er mai prochain. Celle-ci a été menée sur 100 millions de pages vues sur les sites de Google au travers des navigateurs Chrome, Firefox et Internet Explorer.
Google explique que les adware ciblent aussi bien les systèmes Windows et OS X ainsi que les trois navigateurs. En outre, plus de 5% des internautes visitant les sites de Google auraient au moins un injecteur publicitaire installé sur leur machine. La moitié d’entre eux en disposeraient d’au moins deux et un tiers en auraient au moins quatre.
En outre, 34% des extensions pour Chrome injectant des publicités seraient directement classées en tant que malwares. Les chercheurs ont trouvé 192 extensions malveillantes. Avant d’être bloquées celles-ci affectaient 14 millions d’utilisateurs. Google indique avoir implémenté les technologies de ces chercheurs pour scanner automatiquement le Chrome Web Store à la recherche de nouvelles menaces potentielles.

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 protection juridique du chef d’entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.clubic.com/antivirus-securite-informatique/actualite-761347-google-5-internautes-disposeraient-adware-machine.html?estat_svc=s%3D223023201608%26crmID%3D639453874_922037053

Europol met en garde contre les communications chiffrées | Le Net Expert Informatique

Europol met en garde contre les communications chiffrées

Europol, la police criminelle intergouvernementale, s'est récemment exprimée au sujet des communications chiffrées. Selon les autorités, cela représenterait un réel danger face à la menace terroriste.

Les informations partagés par Edward Snowden, ancien analyste à la NSA, sur les pratiques de surveillance massive orchestrées par les agences de renseignements ont fait l'effet d'une onde de choc. Du jour au lendemain, les plus grosses sociétés Internet ont été directement impliquées dans des affaires de cyber-surveillance. Autant dire que la confiance des internautes vis-à-vis des entreprises, mais également celle de ces dernières face aux gouvernements, en a pris un sacré coup.
Microsoft, Yahoo, Apple ou encore Google ont renforcé leur infrastructure et de plus en plus d'outils surgissent sur la Toile pour sécuriser les communications et la vie privée des internautes. En d'autres termes, la notion de vie privée a le vent en poupe, et ce n'est pas pour plaire à tout le monde. Pour Europol, l'existence de ces technologies est un frein à la lutte contre le terrorisme.

Dans une interview recueillie par la BBC, Rob Wainwright, directeur d'Europol, affirme que les efforts visant à chiffrer les communications par les grandes sociétés high-tech devient problématique. « C'est probablement devenu le plus gros problème pour la police et pour les services de sécurité dans leur lutte contre le terrorisme », affirme-t-il. Et d'ajouter « cela a changé la nature-même du travail contre le terrorisme lequel était jusqu'à présent fiable avec des communications que nous pouvions gérer à un autre qui ne fournit plus rien ».
Apple et Google ont pris le parti de chiffrer leurs systèmes d'exploitation mobiles, au grand dam du FBI. Aussi, Yahoo! a annoncé qu'un dispositif de chiffrement des emails serait proposé d'ici la fin de l'année sur son Webmail. Un mécanisme similaire est déjà disponible avec l'extension Mailvelope pour Chrome et Firefox. Le service sécurisé ProtonMail vient de lever 2 millions de dollars tandis que la messagerie instantanée CryptoCat gagne en popularité.
Pour M. Wainwright, les efforts des sociétés de la Sillicon Valley seraient « motivés par des impératifs commerciaux parce qu'ils perçoivent une demande des consommateurs souhaitant une meilleure vie privée pour leur communications ». D'emblée, ce n'est donc pas la vie privée des internautes qui prime mais les dangers potentiels d'une communication entre terroristes. D'emblée, les efforts des sociétés pour protéger leurs infrastructures et leurs services sont donc replacés à une campagne marketing…
Entre les agences de renseignement et les prestataires de services, le bras de fer ne fait que commencer. Le mois dernier Alex Stamos, responsable de la sécurité chez Yahoo! est monté au créneau contre le directeur de la NSA, lequel souhaite voire la mise en place d'une porte d'accès aux données de l'internaute de manière légale. Les géants du Web se sont rassemblés pour lancer un appel au Congrès américain afin que les services de renseignement cessent leurs collectes de données.

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://pro.clubic.com/technologie-et-politique/actualite-761041-europol-garde-communications-chiffree.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_31/03/2015&partner=-&svc_position=91669690B&svc_misc=-&crmID=639453874_916696908&estat_url=http%3A%2F%2Fpro.clubic.com%2Ftechnologie-et-politique%2Factualite-761041-europol-garde-communications-chiffree.html

---

La Commission européenne conseille de quitter Facebook | Le Net Expert Informatique

La Commission européenne conseille de quitter Facebook

Un avocat de la Commission européenne a conseillé au procureur général de la Cour de Justice de l'Union Européenne (CJUE) de fermer son compte Facebook pour éviter que ses données personnelles soient exploitées aux Etats-Unis.

« Vous devriez envisager de fermer votre compte Facebook si vous en avez un » a conseillé Bernhard Schima, l'avocat de la Commission européenne, au procureur général de la JUE Yves Bot la semaine dernière. Une recommandation lancée dans le cadre d'une audience concernant la confidentialité des données des Européens vis-à-vis de l'utilisation qu'en fait le géant américain. La question avait été soulevée il y a plusieurs années par Max Schrems, un étudiant en droit autrichien qui a déclenché en août 2014 une procédure d'action collective mondiale à l'encontre de Facebook.
Mais le procès actuellement en cours oppose Max Schrems à l'équivalent irlandais de la CNIL, contre laquelle l'Autrichien a porté plainte, refusant de voir ses données personnelles stockées par Facebook – dont le siège européen se trouve en Irlande – transférées aux Etats-Unis pour alimenter le ciblage publicitaire de l'entreprise. Le réseau social n'est pas le seul concerné : Microsoft, Apple ou encore Yahoo sont également pointés du doigt.

Ciblage et espionnage
Max Schrems considère que les révélations d'Edward Snowden concernant l'espionnage des données pratiqué par la NSA met les Européens en danger à partir du moment où leurs données personnelles transitent aux Etats-Unis. Une accusation qui remet en question l'application du Safe Harbor, un ensemble de principes de protection des données personnelles, négociés entre les autorités américaines et la Commission européenne en 2001. Les entreprises qui adhèrent à ces principes peuvent recevoir des données en provenance de l'UE, mais la surveillance généralisée de la NSA remettrait en question l'application de ces règles.
On comprend mieux en quoi la petite phrase de l'avocat de la Commission européenne est lourde de sens : elle semble donner raison à la théorie de Max Schrems, engagé depuis longtemps contre la collecte d'information, jugée abusive, par Facebook.
Le commissaire irlandais à la protection des données considère quant à lui qu'il n'existe aucune preuve que le transfert des données de Max Schrems aux Etats-Unis lui a porté préjudice. « Ce n'est pas étonnant dans la mesure où la NSA n'est pas intéressée par les essais écrits par les étudiants en droit autrichiens » a-t-il ironisé. L'avocat général devrait rendre son avis sur l'affaire le 24 juin prochain.

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 protection juridique du chef d'entreprise.
Contactez-nous

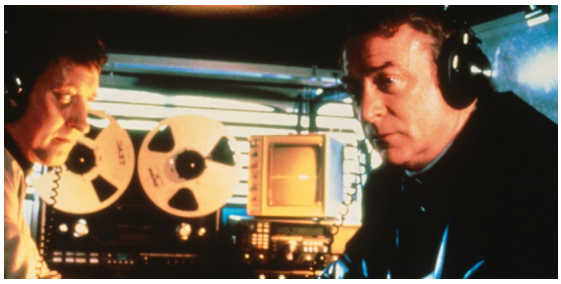
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://pro.clubic.com/blog-forum-reseaux-sociaux/facebook/actualite-760937-protection-donnees-personnelles-commission-europeenne-conseille-quitter-facebook.html

---

Les 8 techniques les plus ahurissantes des espions d'aujourd'hui | Le Net Expert

Informatique



Les 8 techniques les plus ahurissantes des espions d'aujourd'hui

Un projet de loi entend multiplier les possibilités de surveillance des agents du renseignement français. Tour des outils à disposition des services secrets dans le monde. Les services de renseignement français vont bientôt voir leurs possibilités d'espionnage multipliées, avec le projet de loi concocté par le gouvernement. L'occasion de faire le point sur l'éventail des outils à disposition des services secrets à travers le monde.

1. Ecouter les téléphones
Il s'agit de la pratique la plus évidente : l'écoute des conversations. En France, n'importe quel particulier peut être mis sur écoute dans le cadre d'une affaire portant « sur la sécurité nationale, la prévention du terrorisme, de la criminalité et de la délinquance organisée ».
Cette capacité s'est généralisée (pour atteindre un budget de 43 millions d'euros en 2013) et va parfois très loin. L'agence de renseignement américaine NSA s'est dotée d'une gigantesque capacité d'interception, avec son programme Mystic. En 2011, celui-ci aurait même servi à enregistrer 100% des appels passés dans un pays.
Pour simplifier les interceptions, la NSA a également des millions de données, notamment de Français, en se branchant directement sur le câble sous-marins ou les infrastructures internet par lesquels transitent 99% des télécommunications. L'agence était ainsi capable de récupérer en moyenne chaque jour 3 millions de données concernant des Français (conversations téléphoniques, SMS, historiques de connexions internet, e-mails échangés…).


Une écoute téléphonique dans le film « Le quatrième protocole » de John Mackenzie (1987) (AFP)

2. Ecouter Skype, Whatsapp et BBM
Les autorités françaises peuvent mettre en place des écoutes, sur simple décision administrative. Mais cette capacité d'écouter aux portes devrait s'étendre. Le projet de loi souhaite étendre les interceptions également aux SMS et aux e-mails. De plus, un discret amendement au projet de loi Macron va permettre d'étendre les écoutes aux services internet. A terme, les services pourront écouter/lire les conversations sur Skype, Hangout de Google, Whatsapp, WeChat, Line, Facebook Messenger, Viber, BBM, etc.
Microsoft aime à rappeler que, sur son service Skype, deux clefs de chiffrement aléatoires et inconnues de l'entreprise sont créées à chaque conversation, rendant techniquement impossible de brancher des écoutes. Seulement, l'argumentaire a été mis à mal à la suite d'une polémique en 2012 où le site Slate expliquait que des dispositifs techniques avaient été mis en place pour faciliter les interceptions de communication. L'année suivante, le « New York Times » révélait que Skype aidait les forces de l'ordre américaines à accéder aux données de ses clients.

3. La mallette qui écoute tout
Si l'écoute classique ne suffit pas, les services peuvent faire appel à une précieuse mallette : l'IMSI-catcher (parfois aussi désignée par sa marque, StingRay). Cet appareil permet de capter et d'enregistrer toutes les communications (appels, SMS) des téléphones à proximité. Techniquement, il se fait passer pour l'antenne de l'opérateur pour faire transiter par son disque dur toutes les conversations. Il suffit alors de se trouver à portée d'un suspect pour l'écouter.
Une solution largement utilisée par les agences de renseignement dans le monde entier. Aux Etats-Unis, pas moins de 46 agences locales dans 18 Etats y ont recours. Il faut dire que l'IMSI-catcher est plus accessible que jamais : il faut compter 1.800 dollars pour acquérir une mallette prête à l'emploi sur internet, selon « Wired ».

Le projet de loi du gouvernement prévoit d'autoriser leur utilisation par les services français, après avoir reçu l'aval d'un juge.
La NSA aurait même poussé le concept d'IMSI-catcher plus loin puisque, selon des documents d'Edward Snowden, la police fédérale américaine (US Marshall) utilise de petits avions de tourisme dotés de la même technologie afin de capter les communications de suspects.

4. L'aide des hackers
A l'image de James Bond, les services secrets peuvent utiliser micros et caméras pour surveiller des suspects. Ils peuvent aussi utiliser des balises GPS afin de les géolocaliser « en temps réel ». Des dispositifs que le projet de loi français entend légaliser. Mais il souhaite aller plus loin et permettre l'usage de logiciels espions.

Intitulés « keyloggers », ces logiciels-mouchards permettent de recopier en temps réel tout ce qui se passe sur un ordinateur, un smartphone ou une tablette. La navigation internet, les mots de passe saisis, les fichiers stockés… tout est accessible. Le texte du gouvernement précise que « des agents spécialement habilités » pourront « poser, mettre en œuvre ou retirer les dispositifs de captation ». Concrètement, des hackers des services de renseignement pirateront en toute légalité les machines des suspects pour mieux les espionner.

Issue du monde du piratage informatique, la pratique a fait des émules dans les services de renseignement. La NSA aurait ainsi développé un ver informatique, caché dans les disques durs vendus, capable d'espionner tous les faits et gestes, mais aussi de voler n'importe quel document de dizaine de milliers d'ordinateurs à travers le monde.

Mais la France n'est pas en reste puisque deux rapports indiquent que les services de renseignement hexagonaux ont développé leur propre logiciel malveillant, baptisé « Babar », qui renferme un keylogger. Objectif : écouter les conversations en ligne sur Skype, Yahoo Messenger et MSN, mais aussi de savoir quels sites ont été visités.

5. Ecouter autour du téléphone, même éteint
Le téléphone portable est décidément devenu le meilleur ami des agences de renseignement. Outre les écoutes et la géolocalisation, le mobile peut facilement se transformer en micro, même s'il est éteint.

Des documents d'Edward Snowden ont ainsi mis en lumière que la NSA (encore et toujours) est capable d'installer à distance un programme fantôme sur un portable afin de le transformer en espion. Le magazine « Wired » qui rapporte l'information n'entre pas dans les détails, mais ce ver permet de faire croire que l'appareil s'éteint alors qu'il continue de transmettre des informations (sur son contenu notamment). Pour s'en prémunir, la seule solution est de retirer la batterie.

Des hackers ont fait savoir depuis longtemps qu'il est possible de pirater un téléphone et d'en faire un véritable mouchard : écoute des appels, copie des SMS, géolocalisation, écouter les sons environnant (dans un rayon de 5 à 8 mètres), enregistrer la vidéo captée par l'objectif… Et la fonction micro fonctionne même si l'appareil est éteint (mais conserve sa batterie). Une fonction qui a sûrement déjà séduit des agences de renseignement à travers le monde.

6. La carte des interactions humaines
La NSA a aussi un appétit vorace pour les métadonnées. Tous les échanges électroniques (appels, SMS, e-mails, surf sur internet) colportent également des détails sur ceux-ci : qui communique avec qui, à quelle heure, pendant combien de temps, depuis où, etc. Des données qui se rapprochent des fadettes (les factures téléphoniques détaillées) et qui intéressent grandement la NSA.

L'agence a mis en place un programme visant à collecter et à stocker l'ensemble des métadonnées obtenues par les opérateurs télécoms américains. Objectif : constituer une gigantesque base de données permettant, à tout moment, de connaître les interactions entre personnes sur le sol américain. Une idée qui plaît aussi aux renseignements français, déjà experts des fadettes. Le projet de loi souhaite que les autorités puissent avoir accès aux métadonnées d'une personne ciblée sans demander l'avis d'un juge, il suffira d'une autorisation administrative.

Afin de mieux appréhender ce que les métadonnées peuvent dire de nous et de nos interactions, le Massachusetts Institute of Technology (MIT) propose l'outil Immersion qui permet de visualiser sa galaxie de relations basée sur son adresse Gmail de Google.

7. La constitution d'une banque de photos
Toujours selon des documents de Snowden, la NSA collecte chaque jour une quantité astronomique de photos (« des millions d'images ») afin de s'en servir dans le cadre de reconnaissance faciale. Le tout est récupéré dans des e-mails, SMS, sur les réseaux sociaux, via les outils de vidéo-conférences, etc.
Quotidiennement, l'agence obtiendrait 55.000 photos permettant d'identifier des individus, afin d'alimenter une immense banque d'images. L'objectif étant de pouvoir identifier rapidement un suspect, en particulier quand la banque d'images des photos de passeports ne suffit pas.

8. Fouiner dans les téléchargements illégaux
Les téléchargements illégaux peuvent aussi aider les autorités, ou du moins les aiguiller. Un document d'Edward Snowden a révélé que les services secrets canadiens ont chaque jour scruté l'ensemble des téléchargements réalisés sur des plateformes comme MegaUpload ou RapidShare, afin de repérer les manuels et documents édités par des groupes terroristes, afin d'identifier leurs auteurs et ceux qui les consultent. Ils produisaient alors une liste de suspects, transmise à leurs alliés, dont les Etats-Unis. En somme, une aiguille dans une botte de 10 à 15 millions de téléchargements quotidiens.

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://tempsreel.nouvelobs.com/tech/20150317.OBS4818/les-8-techniques-les-plus-ahurissantes-des-espions-d-aujourd-hui.html
Par Boris Manenti

L’immatriculation des drones bientôt obligatoire ? | Le Net Expert Informatique

	L’immatriculation des drones bientôt obligatoire ? #drones

Les propriétaires de drones de loisir seront-ils bientôt obligés d'immatriculer leur appareil, de la même manière que lorsqu'ils achètent une voiture ou une moto ? C'est en tout cas l'une des idées intéressant actuellement le gouvernement, parmi bien d'autres.

Même si les drones ont un peu moins défrayé la chronique des faits divers ces derniers jours, les pouvoirs publics continuent d'examiner les solutions qui permettraient de mieux lutter contre les survols illicites (de centrales, de sites sensibles, d'espaces urbains…). Interrogé en décembre dernier par le député Patrice Verchère, le ministre de l'Intérieur vient de présenter plusieurs de ses pistes de réforme au travers d'une réponse écrite parue mardi au Journal officiel.

Vers un durcissement des sanctions

« La dissuasion des usages malveillants de drones civils peut être renforcée par un durcissement de la législation » expose d'entrée Bernard Cazeneuve. Comment ? « En rendant possible le prononcé d'une peine complémentaire de confiscation, soit par une augmentation du quantum des peines encourues dans le titre III du livre II de la VIème partie du code des transports, soit par l'insertion dans ce code d'un nouvel article le prévoyant. » En clair, les sanctions administratives et pénales prévues en cas de violation de la réglementation pourraient être relevées. Même si le nombre d'infractions possibles est actuellement assez vaste, on retient habituellement que l'article L6232-4 du Code des transports punit d'un an d'emprisonnement et de 75 000 euros d'amende le fait de ne pas respecter les règles de sécurité applicables aux drones (interdiction de voler de nuit, au-dessus de personnes, etc.).

Cazeneuve pose une option sur l'immatriculation obligatoire des drones

Le « premier flic de France » affirme ensuite qu'une immatriculation des drones « est également une option ». L'exécutif songe en effet à transposer l'obligation qui pèse actuellement sur tous les propriétaires d'aéronefs civils (ULM, planeurs…). Une formalité administrative qui coûte 91 euros. « Il convient d'en évaluer préalablement les conséquences, particulièrement en termes de gestion de fichier qui en découlerait » temporise néanmoins Bernard Cazeneuve.

Mieux détecter et neutraliser certains drones

« Au titre de la réponse capacitaire et juridique aux drones malveillants, l'identification électronique des drones en vol à l'aide de signaux émis, facilitant leur détection, est en outre un axe de travail susceptible de donner lieu à une mesure législative » ajoute le ministre de l'Intérieur. Avant de poursuivre : « Il en est de même de l'insertion dans les logiciels de vols des drones civils, fabriqués et utilisés en France, de zones interdites de survol. » Derrière ces mots, on comprend que l'exécutif envisage de doter les drones français de sortes de GPS qui permettraient d'une part de les repérer dès lors qu'ils approchent d'une zone sensible, voire carrément de les mettre en « panne volontaire » s'ils y pénètrent.

Enfin, dans un tout autre registre, le locataire de la Place Beauvau indique que la mise en place d'un « régime d'assurance obligatoire pour les usages de drones à des fins de loisirs » est actuellement « à l'étude ».

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.nextinpact.com/news/93584-limmatriculation-drones-bientot-obligatoire.htm

Les réserves de la CNIL sur le projet de loi renseignement | Le Net Expert Informatique

Les réserves de la CNIL sur le projet de loi renseignement

Il n'y aura pas de surveillance généralisée du citoyen, assure-t-on à Matignon, alors que le projet de loi renseignement doit être présenté jeudi en Conseil des ministres. Cela n'a pas empêché la Commission nationale de l'informatique et des libertés (CNIL) d'émettre un certain nombre de réserves sur ce texte, dont le calendrier a été accéléré après les attentats contre Charlie Hebdo et le supermarché casher de la porte de Vincennes.

Le projet de loi va permettre « une surveillance beaucoup plus large et intrusive », estime un pré-rapport dont « Les Echos » ont pu prendre connaissance. Si les objectifs du gouvernement paraissent « justifiés », « les atteintes portées au respect de la vie privée doivent être limitées au strict nécessaire », écrit la CNIL.

Trois dispositifs nouveaux (collecte automatique d'informations sur les réseau, pose de sondes, sorte de mouchard permettant de collecter des informations en direct sur des personnes surveillées, et pose d'antennes à proximité de suspects) permettent de « collecter de manière indifférenciée un volume important de données » sur « des personnes relativement étrangères » aux suspects. « Ce changement a des conséquences particulièrement graves sur la protection de la vie privée et des données personnelles », avertit la CNIL.

« Aspiration massive de données »

Dans le détail, la détection « par un traitement automatique » des comportements suspects ressemble fort à de la surveillance généralisée. A Matignon, on se montre soucieux de faire de la « pédagogie » sur le sujet. L'objectif de la mesure, explique-t-on, est de détecter « les signaux faibles » permettant d'identifier des individus susceptibles de basculer dans le terrorisme. « Aujourd'hui, ceux qui partent n'ont pas été détectés avant leur départ [vers la Syrie, etc., ndlr]. Or, 89 sont morts, dont un garçon de 14 ans », rappelle-t-on à Matignon.

Pour détecter ces inconnus, les agents veulent pouvoir analyser les flux de données, savoir qui communique avec qui, et quels sont les sites jihadistes visités. Pas d'autres moyens donc que de faire de la surveillance sur le réseau des opérateurs. « Nous voulons insérer dans les équipements des opérateurs des boîtes noires contenant des algorithmes identifiant des comportements marqueurs », précise Matignon. Si en théorie, la disposition pourrait s'appliquer aux géants du Net, les agents de l'Etat préfèrent d'abord aller traiter avec les opérateurs télécoms, considérant qu'ils sauront se montrer plus ouverts à leurs requêtes.

Inévitablement, une partie des flux échappera aux services, Google ayant depuis les révélations d'Edward Snowden chiffré l'ensemble des connexions de ses utilisateurs.

Quant à la captation en temps réel des données géolocalisées de personnes mises sous surveillance (3.000 personnes environ), elle est assimilée par la CNIL à un dispositif « d'aspiration massive et directe des données par l'intermédiaire de la pose de sondes ». Enfin, le système « IMSI Catcher » (pose d'antennes relais à proximité d'un suspect) permet aussi d'intercepter des informations sur des personnes n'ayant rien à voir avec les faits, regrette la CNIL.

De leur côté, les interceptions de sécurité – les fameuses écoutes – ne sont plus « exceptionnelles », note la CNIL, même si le texte « renforce les modalités de contrôle ». Surtout, la loi donne la possibilité « par réaction en chaîne » d'écouter « des personnes qui n'auraient pas été en relation avec la personne surveillée ».

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lesechos.fr/tech-medias/hightech/0204235783787-les-reserves-de-la-cnil-sur-le-projet-de-loi-renseignement-1103298.php
Par Sandrine Cassini

Est-ce que l'iPhone est

vulnérable ? | Le Net Expert Informatique

	**Est-ce que l'iPhone est vulnérable ?**

Est-ce que les iPhone sont vulnérables à l'espionnage, c'est la question que l'on peut se poser en sachant que la CIA cherche à le casser depuis sa création.

Selon la récente publication de The Intercept, on sait que la CIA a tenté de « casser », percé le chiffrement, des produits Apple depuis 2006. Cela signifie que l'agence américaine a bien évidemment aussi tenté de percer les sécurités de l'iPhone vu que la première édition est sortie en 2007. La grande question est de savoir si la CIA est arrivée à ses fins.
Sans revenir sur tous les détails de cette révélation faite sur la base des documents dévoilés par Edward Snowden, on peut comprendre de nombreuses choses à partir de cette nouvelle affaire d'espionnage des utilisateurs.
Pour commencer, il n'y avait pas que la NSA qui cherchait à collecter des données personnelles des utilisateurs de smartphones. Alors que les lois américaines empêchent normalement l'espionnage des citoyens américains, on peut sérieusement se poser la question si ces textes n'ont pas tout simplement été bafoués en essayant de casser le chiffrement des iPhone alors que les Américains sont friands de produits Apple.
Si découvrir des failles dans les systèmes Apple s'explique par le fait de vouloir obtenir des données des utilisateurs, on peut se poser la question de savoir pourquoi la CIA n'a pas averti Apple de l'existence de ces failles ? Il semble évident que cela aurait été un aveu de culpabilité. Par contre, un peu prendre cet aspect d'un autre point vu en considérant que ce que les agences américaines ont fait, d'autres agences de pays hostiles ont également pu le faire. De fait, ne pas communiquer ces failles serait une mise en danger des données personnelles des citoyens américains.
En sachant tout cela, on comprend parfaitement pourquoi les constructeurs, notamment Apple, ont renforcé la sécurité de leurs systèmes et refusent d'ouvrir des backdoors « légales » pour les autorités. En effet, comment pourrait-il exister une moindre confiance ?
En sachant tout cela, on ne comprend par contre pas la véhémence des agences américaines qui dénoncent les méthodes de cryptage mises en place par les entreprises. En effet, ces mesures ne visent que la protection des données des utilisateurs, notamment des biens appartenant à des Américains.
Au final, le débat sur la protection des données personnelles va encore faire couler beaucoup d'encre.

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.linformatique.org/est-ce-que-liphone-est-vulnerable/

Projet de loi relatif au renseignement | Le Net Expert Informatique

Projet de loi relatif au renseignement

Le Conseil d'État a été saisi le 20 février 2015 et le 5 mars 2015 du projet de loi relatif au renseignement.

Ce projet de loi définit la **mission des services spécialisés de renseignement** et les **conditions dans lesquelles ces services peuvent être autorisés, pour le recueil de renseignements** relatifs à des intérêts publics limitativement énumérés, à recourir à des techniques portant sur l'accès administratif aux données de connexion, les interceptions de sécurité, la localisation, la sonorisation de certains lieux et véhicules, la captation d'images et de données informatiques, enfin à des mesures de surveillance internationale.
Il instaure pour l'ensemble de ces techniques, à l'exception des mesures de surveillance internationale, un régime d'autorisation préalable du Premier ministre après avis et sous le contrôle d'une autorité administrative indépendante dénommée « Commission nationale de contrôle des techniques de renseignement », qui pourra recevoir des réclamations de toute personne y ayant un intérêt direct et personnel. Il fixe les durées de conservation des données collectées.
Il prévoit un régime spécifique d'autorisation et de contrôle pour les mesures de surveillance et de contrôle des transmissions émises ou reçues à l'étranger.
Il institue un recours juridictionnel devant le Conseil d'État ouvert à toute personne y ayant un intérêt direct et personnel, ainsi qu'à la Commission nationale de contrôle des techniques de renseignement, tout en prévoyant des règles procédurales dérogatoires destinées à préserver le secret de la défense nationale.
Le Conseil d'État a veillé à ce que soient conciliées les nécessités propres aux objectifs poursuivis, notamment celui de la protection de la sécurité nationale, et le respect de la vie privée protégé par l'article 2 de la Déclaration des droits de l'homme et du citoyen et l'article 8 de la Convention européenne de sauvegarde des droits de l'homme et des libertés fondamentales. Il s'est attaché à préciser et renforcer les garanties nécessaires à la mise en œuvre des techniques de renseignement, tenant en particulier à l'existence, d'une part, d'un contrôle administratif s'exerçant au moment de l'autorisation et en cours d'exécution, d'autre part, s'agissant d'une procédure administrative spéciale, d'un contrôle juridictionnel approfondi du Conseil d'État statuant au contentieux.

Lire la suite….

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.legifrance.gouv.fr/Droit-francais/Les-avis-du-Conseil-d-Etat-rendus-sur-les-projets-de-loi/Projet-de-loi-relatif-au-renseignement-PRMX1504410L-19-03-2015

La sécurité selon Yahoo : chiffrement et mot de passe jetable | Le Net Expert Informatique

La sécurité selon Yahoo : chiffrement et mot de passe jetable

Yahoo a soumis sur GitHub le code d'un plugin permettant de chiffrer de bout-en-bout les courriels envoyés depuis son service de messagerie. La firme veut aussi faire disparaître le mot de passe et implémente un système OTP, un mot de passe à usage unique.

Depuis les révélations autour d'Edward Snowden concernant l'espionnage américain, la sécurité et la confidentialité des communications préoccupent nettement plus les fournisseurs de services en ligne, dont Yahoo et Google.
La firme de Marissa Mayer a ainsi notamment choisi d'adopter le chiffrement des échanges. Et dans ce cadre, Yahoo travaille à une solution de chiffrement de bout-en-bout de la messagerie par l'intermédiaire d'un plugin.

Stamos répond à la NSA avec un plugin
Afin de s'assurer de la robustesse de cette technologie, le directeur de la sécurité de Yahoo, Alex Stamos, fait appel à l'expertise de la communauté. Le code du plugin a été publié sur GitHub et disponible pour être audité et les vulnérabilités identifiées.
Yahoo a collaboré avec Google pour que leurs systèmes de messagerie soient compatibles avec le plugin de chiffrement, qui devrait être finalisé d'ici la fin de l'année et est basé sur le standard OpenPGP.
A noter que Yahoo, comme d'autres services Web, planche également sur la sécurisation de la phase d'authentification. Comment ? En proposant des méthodes alternatives au mot de passe classique, dont la vulnérabilité est établie.
Ainsi, Yahoo a implémenté un système OTP ou One Time Password. Après avoir activé la fonction et communiqué un numéro de téléphone mobile Yahoo, l'utilisateur n'a plus à mémoriser son mot de passe habituel.
Lors de la connexion, l'internaute n'a qu'à cliquer sur le bouton déclenchant l'envoi du mot de passe. Celui-ci parvient sous la forme d'un SMS comportant un code de 4 caractères. Il ne reste plus qu'à le saisir pour se connecter.

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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.zdnet.fr/actualites/la-securite-selon-yahoo-chiffrement-et-mot-de-passe-jetable-39816374.htm

---

Biométrie sur le lieu de

travail : quelles limites ? | Le Net Expert Informatique

Biométrie sur le lieu de travail : quelles limites ?

En Suède, la société Epicenter a récemment pris la décision d'implanter une puce électronique à ses salariés, afin de remplacer le badge d'accès aux locaux de l'entreprise et de faire fonctionner la photocopieuse. Qu'en est-il en France ?

1/ Qu'est-ce que la biométrie ?

La biométrie peut être définie comme la technique d'identification d'une personne à partir de ses caractéristiques physiques (empreintes digitales, iris de l'œil,…) ou biologiques (sang, ADN,…).
Pour la CNIL, « la biométrie regroupe l'ensemble des techniques informatiques permettant de reconnaître automatiquement un individu à partir de ses caractéristiques physiques, biologiques, voire comportementales. »
La CNIL ajoute que les données biométriques sont des données à caractère personnel en que qu'elles permettent d'identifier une personne, ayant la particularité d'être uniques et permanentes.
Ainsi, elles permettent le traçage des individus, agissant comme un « identificateur unique. »
Sur le plan professionnel, la biométrie peut être utilisée à plusieurs fins, et notamment pour autoriser l'accès aux locaux de l'entreprise, contrôler le temps de travail ou allumer l'ordinateur de travail.
Ce dispositif de contrôle est cependant soumis à de nombreuses conditions, compte tenu des contraintes qu'il fait peser sur les libertés individuelles.

2/ Dans quels cas peut-elle être admise ?

La CNIL a défini un cadre applicable à certains dispositifs biométriques, permettant à l'employeur de bénéficier d'une procédure simplifiée en adressant à la CNIL une simple déclaration de conformité.
Ces dispositifs sont au nombre de trois et visent ceux reposant sur la reconnaissance :
• du contour de la main pour assurer le contrôle d'accès au restaurant scolaire (autorisation n°AU-009) ;
• du contour de la main pour assurer le contrôle d'accès aux locaux et à la restauration sur les lieux de travail (autorisation n°AU-007) ;
• de l'empreinte digitale exclusivement enregistrée sur un support individuel détenu par la personne concernée pour contrôler l'accès aux locaux professionnels (autorisation n°AU-008).

Si le dispositif biométrique obéit à l'une de ces trois finalités, l'employeur peut présenter une déclaration simplifiée auprès de la CNIL.

NB. L'utilisation de dispositifs de reconnaissance biométrique, pour la gestion des contrôles d'accès aux locaux, des horaires et de la restauration ne peut pas faire l'objet de cette demande d'autorisation.

Le recours à la biométrie n'est donc possible que dans des hypothèses très limitées, et ne saurait justifier un contrôle des horaires de travail.
Si le dispositif n'est pas conforme à l'une de ces autorisations uniques, il est possible de solliciter une autorisation spécifique auprès de la CNIL.
Cette dernière examine au cas par cas les demandes qui lui sont adressées afin de déterminer si, au regard des éléments du dossier, le dispositif est proportionné ou non à la finalité (CNIL.fr).
Cette exigence de la CNIL rejoint les dispositions de l'article L. 1121-1 du Code du travail selon lesquelles « nul ne peut apporter aux droits des personnes et aux libertés individuelles et collectives de restrictions qui ne seraient pas justifiées par la nature de la tâche à accomplir ni proportionnées au but recherché. »

3/ Dans quelles conditions ?

Lorsqu'il est justifié, le recours à la biométrie est soumis à de nombreuses conditions de consultation et d'information.

3.1/ Information / consultation du comité d'entreprise

L'information / consultation du comité d'entreprise est requise sur le fondement de trois articles spécifiques :
– Article L. 2323-13 du Code du travail : « Le comité d'entreprise est informé et consulté, préalablement à tout projet important d'introduction de nouvelles technologies, lorsque celles-ci sont susceptibles d'avoir des conséquences sur l'emploi, la qualification, la rémunération, la formation ou les conditions de travail. »
– Article L. 2323-32, alinéa 3 du Code du travail : « Il est aussi informé, préalablement à leur introduction dans l'entreprise, sur les traitements automatisés de gestion du personnel et sur toute modification de ceux-ci. »
– Article L. 2323-32, alinéa 3 du Code du travail : « Le comité d'entreprise est informé et consulté, préalablement à la décision de mise en œuvre dans l'entreprise, sur les moyens ou les techniques permettant un contrôle de l'activité des salariés. »

La consultation du comité d'entreprise doit permettre à ce dernier de donner son avis sur la pertinence et la proportionnalité entre l'utilisation de la biométrie et la finalité recherchée.

3.2/ Information / consultation du CHSCT

Le CHSCT doit également être informé et consulté sur le recours à la biométrie, en application de l'article L. 4612-8 du Code du travail.
Ce texte dispose en effet que « le comité d'hygiène, de sécurité et des conditions de travail est consulté avant toute décision d'aménagement important modifiant les conditions de santé et de sécurité ou les conditions de travail… »
La Cour d'appel de Paris (CA Paris 5 décembre 2007, n° 07-11402) a retenu cette solution concernant l'enregistrement automatique des communications des salariés.
Il y a lieu de considérer que la mise en place de la biométrie impose à l'employeur la saisine préalable du CHSCT, compte tenu des termes très larges de l'article L. 4612-8 du Code du travail.

3.3/ Information des salariés

Enfin, chaque salarié doit être informé, conformément à l'article L. 1222-4 du Code du travail selon lequel « aucune information concernant personnellement un salarié ne peut être collectée par un dispositif qui n'a pas été porté préalablement à sa connaissance. »
Bien que le texte ne l'exige pas expressément, il est fortement conseillé de procéder à une information individuelle de chaque salarié, afin d'éviter toute contestation.

Expert Informatique 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 protection juridique du chef d'entreprise.
Contactez-nous

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.village-justice.com/articles/Biometrie-sur-lieu-travail-quelles,18886.html