La Cnil interdit la géolocalisation du salarié en dehors du temps de travail | Le Net Expert Informatique

La Cnil interdit la géolocalisation du salarié en dehors du temps de travail

Par une délibération du 4 juin 2015, la Cnil a décidé de renforcer l'encadrement du recours au dispositif de géolocalisation.

La Commission nationale de l'informatique et des libertés (Cnil) constate le développement de dispositifs dits de géolocalisation permettant aux organismes privés ou publics de prendre connaissance de la position géographique, à un instant donné ou en continu, des employés par la localisation des véhicules mis à leur disposition pour l'accomplissement de leur mission. Ainsi, l'employeur peut contrôler le respect des règles d'utilisation d'un véhicule par ses employés grâce à la géolocalisation.
Ce dispositif permet de collecter des données à caractère personnel et sont donc soumis aux dispositions de la loi du 6 janvier 1978.
Par délibération n° 2015-165 du 4 juin 2015, la Cnil a considéré qu'il était nécessaire de compléter la norme permettant de simplifier la déclaration des traitements visant à géolocaliser un véhicule utilisé par un employé.
Dans cette délibération, la Cnil précise que le recours au dispositif peut servir à justifier la réalisation d'une prestation auprès d'un client ou d'un donneur d'ordre, ou bien à lutter contre le vol du véhicule.
En outre, la Cnil interdit formellement aux employeurs de collecter des données de localisation en dehors du temps de travail du salarié, à savoir lors de ses temps de pause et du trajet entre son domicile et le lieu de travail.
La faculté de désactiver la fonction de géolocalisation doit être laissée à l'employé. Toutefois, la Cnil souligne que des explications pourront être demandées au salarié lorsque les désactivations sont trop longues ou trop fréquentes.
Enfin, les employeurs publics et privés devront se conformer au nouveau dispositif avant le 17 juin 2016.

Source : http://droit-public.lemondedudroit.fr/droit-a-entreprises/droit-social/206288-la-cnil-interdit-la-geolocalisation-du-salarie-en-dehors-du-temps-de-travail.html

La Gendarmerie Nationale souhaite s’équiper d’une vingtaine de drones | Le Net Expert Informatique

	La Gendarmerie Nationale souhaite s’équiper d’une vingtaine de drones

La Gendarmerie nationale souhaite s'équiper d'une flotte de drones, comme l'avait récemment annoncé Bernard Cazeneuve. Et c'est un appel d'offres qui a été lancé pour l'achat d'une vingtaine de drones répondant à certains critères spécifiques.

Le ministère de l'Intérieur vient de lancer un appel d'offres visant » la fourniture de microdrones au profit de la Gendarmerie nationale, le maintien en condition opérationnelle des microdrones acquis, et la formation pour la fonction de télépilote ». Plus qu'une flotte de drones, il est question des dispositifs ainsi que d'une formation à leur utilisation et leur entretien.
La Gendarmerie nationale devrait disposer de 23 appareils de la famille des « quadrirotors à décollage vertical » qui permettent un contrôle précis, une stabilité accrue, mais qui permettront le vol stationnaire pour la mise en place d'opération de surveillance.
Il sera question de 4 à 6 drones haut de gamme qui devront disposer d'un mode de vol manuel et automatique. Le drone devra être capable de voler tout seul selon un ensemble de points de passage prédéfini. Son autonomie devra être d'au moins 20 minutes avec une vitesse équivalente à un kilomètre avalé en moins de deux minutes. L'appareil devra embarquer une caméra et retransmettre ses images en direct.
Un second lot de 19 à 30 drones sera constitué de modèles plus accessibles. La Gendarmerie nationale souhaite toujours un mode de vol automatique ainsi qu'une caméra embarquée, mais ici, la question de l'autonomie et de la vitesse importent moins, puisqu'il s'agira avant tout de mener des opérations de surveillance fixe dans le cadre d'interventions de sécurisation de la voie publique.
La Gendarmerie nationale souhaite des drones fiables, équipés de zoom x10 au minimum, le tout avec un relatif silence opérationnel permettant la mise en place d'une surveillance discrète.

Source : http://www.generation-nt.com/gendarmerie-nationale-equipe-drones-volants-actualite-1916394.html

Comment la France écoute (aussi) le monde | Le Net Expert Informatique

Comment la France écoute (aussi) le monde

Révélations sur un vaste plan de la DGSE pour intercepter les communications internationales passant par les câbles sous-marins : lancé en secret par Nicolas Sarkozy, il vient d'être légalisé par François Hollande en toute discrétion.

Il n'y a pas que la NSA. La France aussi écoute le monde. Après une enquête de plusieurs semaines, « l'Obs » révèle que :
– Début 2008, Nicolas Sarkozy a autorisé la DGSE à espionner les communications internationales transitant par les câbles sous-marins qui relient l'Europe au reste du monde. Un plan de 700 millions d'euros sur cinq ans (2008-2013) a été lancé par le service secret pour installer des stations d'interceptions à l'arrivée des câbles en France (notamment à Marseille, Penmarch et Saint-Valéry-en-Caux).
– Au moins cinq câbles majeurs ont été mis sur écoute pendant cette période avec l'aide de l'opérateur Orange et du groupe Alcatel-Lucent dont le TAT14 vers les Etats-Unis ; le I-Me We vers l'Inde ; le Sea-Me-We 4 vers l'Asie du Sud-est ; et le ACE vers l'Afrique de l'Ouest.
– La DGSE a passé un grand accord de coopération avec le GCHQ britannique. C'est une annexe secrète au traité de défense dit de Lancaster House, signé le 2 novembre 2010 par Nicolas Sarkozy et David Cameron.
– François Hollande a autorisé la DGSE à étendre ces opérations à d'autres câbles dans un nouveau plan quinquennal (2014-2019). L'article L-854-1 de la toute nouvelle loi sur le renseignement vise à les légaliser en catimini.
C'est un plan classé « très secret », exposé ici pour la première fois. Un projet de la Direction générale de la sécurité extérieure (DGSE) autorisé par Nicolas Sarkozy il y a sept ans et poursuivi sous François Hollande, qui explique leur surprenante modération après la révélation de leur mise sur écoute par la NSA. Une vaste entreprise française d'espionnage que la loi sur le renseignement, adoptée le 24 juin, vient de légaliser en catimini.
Cette histoire de l'ombre, « L'Obs » a pu la reconstituer grâce aux témoignages anonymes de plusieurs responsables actuels et passés. Il y est question de stations clandestines installées par la DGSE sur les côtes françaises pour « écouter » les câbles sous-marins, de la complicité de grandes entreprises hexagonales, des accords secrets entre le service français et ses homologues anglo-saxons et de l'indigence du contrôle parlementaire…

La France à la traîne
L'affaire commence début janvier 2008, dans le bureau du chef de l'Etat, à l'Elysée. Nicolas Sarkozy a réuni le Premier ministre, François Fillon, le patron de la DGSE, Pierre Brochand, et quelques collaborateurs. Au menu : l'avenir des services spéciaux français. Leur problème ? Ils sont devenus (presque) sourds. Ils ont de plus en plus de mal à écouter les communications mondiales…
Lire la suite….

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

Source : http://tempsreel.nouvelobs.com/societe/20150625.OBS1569/exclusif-comment-la-france-ecoute-aussi-le-monde.html?cm_mmc=EMV-_-NO-_-20150701_NLNOACTU08H-_-exclusif-comment-la-france-ecoute-aussi-le-monde#xtor=EPR-1-Actu8h-20150701

WHOIS : vos informations personnelles bientôt publiques ? | Le Net Expert Informatique

L'ICANN pourrait bientôt modifier le système du WHOIS. Le régulateur propose notamment d'interdire aux propriétaires de sites « à but commercial » de s'enregistrer via proxy, soit de façon anonyme. Le texte ne laisse pas les associations insensibles, qui y voient une menace pour ceux qui s'expriment librement sur leurs sites.

WHOIS est souvent décrit comme l'annuaire d'Internet. Lors de l'enregistrement d'un nom de domaine, un internaute doit renseigner diverses informations personnelles, de son état civil à son numéro de téléphone en passant par son adresse de domicile. Ces informations alimentent les bases de données des registres de noms de domaine, et sont consultables via l'outil WHOIS.
Pour des questions évidentes de protection de la vie privée et de confidentialité, les données fournies par le propriétaire d'un nom de domaine ne sont pas accessibles au public. Les registres de renseignement proposent fréquemment en option la possibilité de s'enregistrer via proxy. Les seules tierces personnes alors en mesure d'accéder aux bases de données non anonymisées sont celles détenant une autorisation légale, tel qu'un mandat judiciaire.
Mais cette situation connaîtrait ses derniers jours. L'ICANN prévoit en effet de modifier le système en profondeur. Le régulateur étudie actuellement un projet, lequel envisage notamment que les noms de domaine « utilisés dans un but commercial soient inéligibles à l'enregistrement proxy/privacy ». En d'autres termes, les propriétaires de sites contenant un quelconque élément transactionnel ne pourront plus s'enregistrer de façon anonyme : leurs informations personnelles devront être publiques.

L'anonymat, garant de la liberté d'expression
Alors que l'ICANN doit se prononcer le 7 juillet sur ce texte, l'Electronic Frontier Foundation appelle les internautes à s'y opposer. Selon l'EFF, le terme « but commercial » englobe un grand nombre de sites, et la vie privée de leurs propriétaires, des personnes physiques, seraient menacée. L'association prend pour exemple TG Storytime, un site destiné aux auteurs transgenres et hébergés par Joe Six-Pack, lui-même transgenre. Si l'ICANN devait modifier la régulation en vigueur, ses adresses, numéros de téléphone et mails seraient alors exposées à la vue de tous, trolls et harceleurs compris.
Le changement a été impulsé par les géants américains du divertissement, signale l'EFF, ce que l'ICANN ne cache pas. En effet, à de nombreuses reprises, le régulateur d'Internet écrit que cette proposition vise à faciliter le signalement de sites violant le droit d'auteur (ou toute autre propriété intellectuelle). Pour l'EFF, « ces entreprises veulent de nouveaux outils pour découvrir l'identité des propriétaires de sites Web qu'ils veulent accuser de violation de droit d'auteur et contrefaçon de marque, de préférence sans une ordonnance du tribunal ».
« L'avantage limité de cette évolution est manifestement compensé par les risques supplémentaires pour les propriétaires de sites, qui vont souffrir d'un risque plus élevé de harcèlement, d'intimidation et de vol d'identité ».
Il est vrai que, malgré les gardes fous prévus par l'ICANN, la plupart des informations fournies pour l'enregistrement d'un nom de domaine sont sensibles, tant IRL (In Real Life) que dans le monde virtuel. En appelant à s'opposer au texte, l'association entend faire réagir sur un recul de l'anonymat, qui affectera ceux qui portent des opinions impopulaires ou marginales mais aussi les lanceurs d'alerte et tous ceux susceptibles de dénoncer « la criminalité et la corruption ».

Source : http://www.linformaticien.com/actualites/id/37199/whois-vos-informations-personnelles-bientot-publiques.aspx
Par Guillaume Périssat

Exclusif : 47 grandes entreprises françaises ciblées par une tentative d’escroquerie à grande échelle | Le Net Expert Informatique

	47 grandes entreprises françaises ciblées par une tentative d’escroquerie à grande échelle

Selon nos informations, une cinquantaine de grandes entreprises sont actuellement – ou ont été au cours des derniers jours – la cible d'un réseau criminel spécialisé dans l'escroquerie aux faux ordres de virement (FOVI), encore appelée « Arnaque au président ». La technique n'est pas nouvelle. Ce qui interpelle, dans le cas présent, c'est l'ampleur de l'offensive mise à jour.

« L'arnaque au président » n'est pas vraiment d'un genre nouveau. D'ailleurs son pionnier, Gilbert Chikli, poursuivi par 33 banques et aujourd'hui réfugié en Israël, vient d'être condamné par contumace à 7 ans de prison et à 1 millions d'euros d'amende.

En cause : des escroqueries jugées « hors-norme », dont l'essaimage est devenu en quelques mois la bête noire des grandes directions financières, à commencer par celles que l'on pensait être les plus aguerries. Ainsi en 2012, c'est KPMG qui en a fait les frais : le géant mondial de l'audit et du conseil en fiscalité a laissé s'envoler à son insu pas moins de 7,6 millions d'euros.

Ces tentatives d'escroquerie n'épargnent personne : pas plus Michelin ou le Palais de l'Elysée, que nos PME régionales. Si Gilbert Chikli promet aujourd'hui avoir tiré sa révérence, il n'est en revanche pas improbable qu'il ait, directement ou non, inspiré quelques disciples.

47 entreprises sous la menace imminente de la criminalité financière

C'est une longue liste de cibles que s'est procuré la rédaction du JDE, par l'intermédiaire d'un cabinet privé spécialisé dans l'investigation et la lutte anti-fraude. Pour des raisons évidentes de sécurité, les consultants qui nous ont transmis cette information préfèrent rester anonymes.

Ils témoignent : « la spécificité de cette affaire réside dans l'ampleur de l'attaque. A ce jour, nous ne pouvons confirmer son état de progression ou son éventuel aboutissement. Nous avons contacté chacune des entreprises ciblées pour tenter d'être mis en relation avec les directions générales ou financières afin de de les en avertir. Malheureusement, le personnel n'étant pas toujours sensibilisé à ce type de risque, certains de nos appels sont restés sans suite. »

Une situation qui n'étonne guère ces analystes rompus à la gestion des affaires réservées des dirigeants : «Malheureusement, ces escroqueries aboutissent la plupart du temps à cause de défaillances dans la sûreté et les procédures internes de l'entreprise. La formation des collaborateurs, la circulation intelligente de l'information et l'instauration de procédures de vérification restent les meilleurs remparts contre ces attaques. »

Parmi les entreprises ciblées ou déjà attaquées, recensées par les enquêteurs, on retrouve de grands noms de l'économie française, des groupes familiaux plus discrets, et des enseignes bien connues des Français. « Des attaques qui sont en préparation depuis fin avril », précisent nos interlocuteurs, qui nous livrent ci-après le nom des entreprises ou organismes concernés :

Direction Finance, Ludendo, Système U, Abbott, 3 Suisses, GE Capital, Sonepar, Joué Club, Monoprix, BHR Béton, La Redoute, Eurofactor, Sephora, Picard, Imerys, Groupe Flo, GSF, DB Apparel, Optic 2000, Marionnaud, Groupe Pigeon, Invacare, Franck Provost, Auchan, Continental Corporation, Pronatura, Finifac, Provalliance, Carrefour, Vivendi, Korian, Accor, Servair, Bricorama, SKF, SNEF, SNCF, Rexel, Ecolab, Soprasteria, Chausson Matériaux, Faurecia, Immochan, Eiffage, Clemessy.

Comment réagir en cas d'attaque ?

« Nous avons pris des mesures directes pour tenter d'endiguer la marge de manœuvre des 'assaillants' et prévenir le risque d'escroquerie, et travaillons en étroite relation avec nos partenaires depuis plus d'un mois, expliquent les analystes. Surtout, nous accompagnons nos clients dans la mise en place d'une procédure judiciaire à l'encontre des auteurs de la tentative d'escroquerie, en sachant pertinemment qu'elle sera longue et complexe. »

D'après le cabinet, en effet, les quelques traces électroniques analysées laissent apparaître un mode opératoire assez classique, probablement piloté depuis Israël ou un territoire voisin comme l'indiquent les paquets de données qui ont été analysés.

« Dans certains pays, les moyens de paiement prépayés sont très répandus et peu régulés, donc difficilement traçables. Ils peuvent être ensuite utilisés en France, pour acquérir de l'information légale sur les sociétés ou à l'étranger, pour recourir anonymement aux services d'une plateforme téléphonique ». Ce sont également ces cartes prépayées qui, en toute vraisemblance, auront permis aux escrocs de réserver des noms de domaine pour peaufiner leur déguisement électronique.

Un déguisement qui va, selon les experts, jusqu'à l'usurpation d'identité de personnes vivantes ou décédées : « Pour brouiller les pistes, ces brigands 2.0 utilisent vos adresses, numéros de téléphone, dates de naissance pour réserver des noms de domaine et procéder à certaines formalités en ligne. C'est probablement supposé divertir les enquêteurs », ironise l'un de nos experts.

Piqûre de rappel : le mode opératoire

Une opération couronnée de succès est une opération bien préparée. Les escrocs commencent par une phase de renseignement en « zone grise », en collectant un maximum d'informations sur leur cible. C'est ce qu'on appelle le « social engineering », dont le but est de recueillir suffisamment de données quant à l'environnement humain (personnes clés, numéros de téléphone, adresse email) et économique (contrats, fournisseurs, bilans, etc.) de l'entreprise.

C'est bien moins compliqué qu'il n'y paraît : munis d'une carte prépayée, il leur suffit de se rendre sur une base de données de type Infogreffe et de télécharger les documents les plus riches en information : derniers statuts et actes déposés, PV d'assemblées générales, ou comptes annuels par exemple. L'identification, sur les réseaux sociaux, des « personnes clés » dans l'organigramme de la cible permet parfois de se familiariser avec leurs futurs interlocuteurs.

Depuis une plateforme téléphonique située à l'étranger, mais avec un numéro français d'apparence, l'escroc appelle un directeur financier, un service comptable, ou tout individu ayant compétence à agir sur les comptes de l'entreprise.

Se faisant généralement passer pour le dirigeant de l'entreprise, il déploie alors des trésors de créativité et/ou de séduction. Tantôt flatteur, tantôt menaçant, il prétexte une situation d'urgence (opération boursière sensible, ou imminence d'un contrôle fiscal par exemple) et exige le virement immédiat d'une importante somme sur un compte habituellement hébergé en Chine.

Nos interlocuteurs invitent donc les entreprises à la plus grande vigilance : « ces offensives sont généralement fulgurantes et, le temps de réagir, nos escrocs sont déjà loin »…

Source : http://www.journaldeleconomie.fr/Exclusif-47-grandes-entreprises-francaises-ciblees-par-une-tentative-d-escroquerie-a-grande-echelle_a2456.html

Quelques conseils pour préserver votre e-réputation | Le Net Expert Informatique

Quelques conseils pour préserver votre e-réputation

Sur le web, rien ne se perd. Toutes les données qui vous concernent sont potentiellement accessibles par tous. Qu'il s'agisse des photographies de votre vie étudiante festive, des archives du blog que vous aviez tenu lors d'un voyage à l'étranger, de votre participation sur la liste électorale d'un parti politique sulfureux lors d'élections locales ou encore du jugement relatant une condamnation pénale : vous laissez des traces.

Celles-ci peuvent se révéler encombrantes. Comment faire pour qu'elles soient déréférencées des moteurs de recherche et ainsi rendues inaccessibles ?

Tout d'abord, il peut être utile de consacrer quelques minutes au paramétrage de la confidentialité de son compte sur les réseaux sociaux, afin de préserver le caractère privé de ses publications. Celles-ci ne seront alors pas accessibles par le biais des moteurs de recherche mais réservées à vos amis et relations.

Dans le cas où le contenu visé est publié sur un site web tiers, tel qu'un éditeur de presse, un blog ou un forum de discussion, il est possible de demander sa suppression en s'adressant directement à l'éditeur du site concerné ou, lorsque celui-ci ne réagit pas ou n'a pu être identifié, à l'hébergeur (qui assure le stockage du site sur ses serveurs).

En cas d'échec de cette démarche, les moteurs de recherche pourront être sollicités au titre du droit à l'oubli, par le biais des différents formulaires qu'ils proposent désormais [1].

Les principaux refus opposés par les moteurs de recherche sont justifiés par le fait que l'information litigieuse est toujours d'actualité, qu'elle ne concerne pas une personne physique, que l'internaute est un personnage public ou que le plaignant est un personnage public.

En dernier recours, le Tribunal compétent pourra être saisi. Attention toutefois, le juge saisi analyse en détail la demande présentée afin de s'assurer qu'elle ne porte pas atteinte à la liberté d'information du public. Ainsi, le Tribunal de grande instance de Paris a rejeté une demande de suppression et de désindexation d'un article en ligne du quotidien 20 Minutes [2]. L'article litigieux, accessible sur le site internet du quotidien, intitulé « Un cavalier accusé de viol », relatait le placement en garde à vue d'un cavalier de niveau international soupçonné d'être impliqué dans le viol d'une stagiaire.

Les juges ont rejeté la demande de droit à l'oubli, en faisant prévaloir la liberté d'information et l'intérêt légitime à divulguer des informations visant une personne exerçant une profession faisant appel au public et encadrant une activité proposée, notamment, à des enfants.

Au contraire, dans une décision précédente, la même juridiction avait ordonné à la société Google de retirer de ses résultats de recherche un lien vers un article du Parisien évoquant la condamnation, datant de 2006, d'une internaute pour escroquerie à une peine de trois ans de prison dont trois mois fermes. La plaignante, à la recherche d'un emploi, s'était tournée vers la Justice à la suite du refus préalablement opposé par le géant américain.

Lorsque votre demande est rejetée par le tribunal saisi, il reste possible de faire appel à des structures spécialisées qui tenteront de renvoyer au-delà de la troisième page de résultats, le contenu qui vous gêne.

A l'heure où de plus en plus de plateformes proposent aux internautes de redevenir propriétaires de leurs données personnelles et de gagner de l'argent en louant leurs profils [3] aux marques et annonceurs, il est plus que jamais important de permettre aux internautes de retrouver la maîtrise de leur e-réputation.

Source : http://www.village-justice.com/articles/Quelques-conseils-pour-preserver,19708.html

Chief Digital Officer (CDO) – Qui et pour faire quoi au juste ? | Le Net Expert Informatique

Chief Digital Officer (CDO) – Qui et pour faire quoi au juste ?

Acteur de la transformation numérique, le CDO apparaît dans l'organigramme de 22% des entreprises françaises interrogées. Ils devraient être 37% en 2016. Mais pour « transformer, fédérer et piloter », ce profil hybride n'a pas toujours la vie facile.

C'est la formule du moment : la transformation numérique. Tous les secteurs, ou presque, sont concernés ou le seront dans les prochaines années. Le « digital » n'est « plus – et ne doit plus être –un canal (de vente, de communication, de relation client), mais un outil de transformation des organisations et des métiers » écrit Novedia, partenaire du 1er baromètre des CDO (http://www.viseo.com/fr/telechargement/resultats-du-barometre-cdo-2015).

Le numérique se déploie en entreprise donc. Et pour accompagner et piloter cette transformation, celles-ci créent parfois un poste dédié : le Chief Digital Officer ou directeur du numérique. Ils ne sont toutefois pas légion, et essentiellement présents dans les grandes entreprises d'après l'étude réalisée auprès de 201 dirigeants français.

Les services et grandes entreprises plus concernés

22% des sondés déclarent disposer d'un CDO, dont 37% parmi les sociétés de plus d'un milliard d'euros de chiffre d'affaires – contre seulement 5% pour celles réalisant moins de 250 millions d'euros de CA. En 2016, 37% des entreprises auront un patron du numérique selon le baromètre.

Mais à quoi ressemble ou devrait ressembler ce fameux CDO ? Pour 65% des répondants, cette fonction doit être rattachée au Comex. Ils sont seulement 17% à le lier à la DSI et 14% au marketing. La stratégie numérique devrait donc se piloter d'en haut. Néanmoins, un tiers des CDO interrogés regrettent « que leur niveau hiérarchique et leur pouvoir sont inadaptés aux enjeux de leur fonction. »

Et une fois nommé, en quoi consisteront, dans les grandes lignes, les tâches du CDO ? « Transformer, fédérer et piloter » d'après les données recueillies. C'est un peu vague oui, mais il faudra faire avec. Cela semble néanmoins rejoindre les conclusions d'une autre étude soulignant le fait que les enjeux de la transformation numérique étaient organisationnels avant d'être techniques.

Existe-t-il une voie royale au poste de CDO et quelles compétences ce dernier doit-il posséder ? Ce « gendre idéal » ne paraît pas avoir de contours prédéfinis. Trois grandes sensibilités néanmoins : technologie, marketing et métiers. Dans quelles proportions ? Difficile à dire… Un peu de tout.

Un hybride pour affronter les freins culturels

Les répondants estiment donc que le CDO doit être doté d'une culture hybride. Cela se traduit par un profil caractérisé notamment par « Transversalité, compréhension des enjeux marketing et IT », « une bonne culture des métiers » et une capacité à « Expliquer et convaincre, fédérer, briser les silos ».

Mais pour cet acteur nommé pour amorcer du changement dans l'entreprise, tout n'est pas simple. Pour 43% des sondés, le CDO est confronté aux freins culturels à la transformation. 19% estiment en outre qu'il manque de budget pour remplir son office.

La problématique n'est pas franchement nouvelle : le changement provoque des résistances et se heurte à une certaine forme d'inertie héritée d'années de pratique. « C'est une relation disruptive avec les autres fonctions : le CDO remet en cause la façon dont les autres fonctionnent » commente par exemple un répondant. Bon courage donc.

Source : http://www.zdnet.fr/actualites/chief-digital-officer-cdo-qui-et-pour-faire-quoi-au-juste-39821562.htm
Par Christophe Auffray

L’anonymat du WHOIS remis en question à l’ICANN | Le Net Expert Informatique

	L’anonymat du WHOIS remis en question à l’ICANN

Une proposition de l'ICANN s'est attiré les foudres des commentateurs et de l'EFF. La suggestion propose de rendre impossible l'anonymisation des données personnelles sur le service WHOIS pour les sites à vocation commerciale.

Le service WHOIS est un outil particulièrement utile pour savoir qui se cache derrière un nom de domaine et comment contacter les responsables d'un site. Fourni par les registres de noms de domaines, il permet d'interroger les bases de données des bureaux d'enregistrement afin de connaître le nom et l'identité de la personne ou de la société détenant le nom de domaine, ainsi que certaines informations de contacts.
Ces informations ne sont pas forcement accessibles à tout le monde : dans de nombreux cas et pour éviter de voir ces informations personnelles à l'air libre, les bureaux d'enregistrement proposent un service d'enregistrement via proxy permettant de dissimuler au public les données et de les réserver aux seules personnes munies d'autorisations légales fournies par un service judiciaire national. Le service agit donc comme un écran afin d'offrir un moyen de contacter le propriétaire du nom de domaine tout en protégeant ses données personnelles.
Mais une proposition de l'ICANN, ouverte depuis mardi aux commentaires publics, envisage de revenir sur le fonctionnement de ce système en ouvrant à tous les données WHOIS des sites à but commercial. Selon l'EFF, cette règle s'appliquant « à tous les sites commerciaux » pourrait toucher de nombreux petits administrateurs de sites et de communautés en ligne qui ont choisi de mettre en place de la publicité ou un système de dons pour subvenir au coût de leur site.
L'EFF cite ainsi l'exemple de TG Storytime, un paisible site de fanfiction à destination des communautés LGBT, qui pourrait ainsi se voir obligé de révéler certaines informations personnelles liées à l'administrateur du site si la nouvelle proposition était approuvée par l'ICANN.

L'EFF dans la boucle
L'EFF explique que ce changement est notamment soutenu par le secteur du divertissement, qui entend ainsi simplifier les procédures judiciaires à l'égard des sites diffusant des contenus constituant des infractions relatives à la propriété intellectuelle. Outre le risque que cette proposition peut faire peser sur les données personnelles des utilisateurs, on peut également évoquer les dangers relatifs à la cybersécurité.
Cedric Pernet, dans son ouvrage sur les Advanced Persistent Threat, citait ainsi les informations de service WHOIS parmi la liste des sources utiles aux attaquants pour préparer leurs attaques, en leur permettant d'identifier précisément le bureau d'enregistrement d'un site, un numéro de téléphone ou encore le nom de l'employé chargé d'administrer le nom de domaine.Autant d'informations utiles pour une attaque de type spear phishing.
La proposition est ouverte aux commentaires jusqu'au 7 juillet, et suscite déjà un certain engouement de la part des opposants à ce changement de politique, qui ont déjà posté des milliers de commentaires invitant l'ICANN à refuser cette proposition.

Source : http://www.zdnet.fr/actualites/l-anonymat-du-whois-remis-en-question-a-l-icann-39821566.htm
Par Louis Adam

Un centre de compétence Kaspersky doit être mis en place très prochainement au Gabon | Le Net Expert Informatique

Un centre de compétence Kaspersky doit être mis en place très prochainement au Gabon

Un centre de compétence Kaspersky doit être mis en place très prochainement au Gabon, selon les termes d'un accord de partenariat signé mardi à Libreville entre l'Agence nationale des infrastructures numériques et des fréquences (Aninf) et l'éditeur Kaspersky.

En vertu de cet accord, signé par le directeur général de l'Aninf, Alex Bernard Bongo Ondimba et le vice-président de Kaspersky, Veniamin Levtsov, le futur centre, qui aura, par ailleurs, une vocation sous régionale, doit permettre au Gabon d'assurer la veille, la détection, l'analyse et la prévention des cyber-attaque.

« Ce partenariat est très salutaire pour le Gabon du fait qu'il nous permettra de nous doter d'un véritable système de défense en matière de virus et en ce qui concerne la cybercriminalité », a déclaré M. Alex Bernard Bongo Ondimba.

Outre la mise en place d'un centre de compétence au Gabon, l'accord signé porte également sur le transfert des compétences dans les domaines de la sécurité industrielle et de la cybercriminalité.

'Nous entendons contribuer à sauver le monde en mettant en place des systèmes de lutte contre des attaques axées sur la cybercriminalité. Nous voulons également apporter nos compétences aux structures locales », a affirmé, pour sa part, M. Levtsov.

Implantée dans plusieurs pays d'Afrique et dans d'autres continents, Kasperky est une entreprise russe leader mondiale en matière de sécurité informatique.

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

Source :
https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14e3b659f932c0fd?compose=14e2eb99aeedd11a

La première soirée Implant Party débarque à Paris | Le Net Expert Informatique

	La première soirée Implant Party débarque à Paris

La première « implant party » française a été organisée à Paris dans le cadre de l'opération Futur en Seine à La Gaîté Lyrique. Le concept, se faire implanter une puce sous la peau pour différentes applications du quotidien.

Sommes-nous en train d'assister à un tournant dans le domaine de l'interface homme/technologie ? Jusqu'à maintenant (sauf cas extrême), les modifications corporelles se cantonnaient aux tatouages, aux piercings ou écarteurs et à la chirurgie esthétique.
Mais depuis quelques mois, une nouvelle tendance née dans les pays scandinaves devient de plus en plus populaire, les Implant Party. Un concept qui consiste à se faire implanter une puce NFC sous la peau et permettre à son porteur d'interagir avec de nombreuses technologies de notre quotidien.

Une puce NFC sous la peau
Ce weekend, Paris a accueilli sa première implant party dans le cadre de l'opération Futur en Seine à La Gaîté Lyrique. Chacun pouvait venir se faire implanter une puce NFC par un spécialiste formé à cette opération.
Bien entendu, pas question de faire n'importe quoi et l'opération, facturée 200 euros, est effectuée dans des conditions d'hygiène drastiques et dans un environnement totalement stérilisé. Le biohacker (nom donné à la personne qui reçoit l'implant) se voit injecter une puce NFC grosse comme un grain de riz sous la peau après une anesthésie locale. Une fois l'opération effectuée, il devient possible pour le porteur de la puce d'interagir sans contact avec les équipements NFC qui l'entoure.

Des applications multiples, notamment dans le domaine professionnel
Déverrouiller son smartphone, ouvrir une porte, allumer un ordinateur ou encore payer un petit achat du quotidien d'un simple geste de la main, voilà ce que permet la technologie implanté dans le biohacker.
Ce mouvement d'un nouveau genre a été créé en Suède par l'association à but non lucratif Bionyfiken. 400 salariés suédois se sont récemment vus proposer la possibilité de se faire implanter une puce NFC pour entrer dans leurs locaux, payer leur repas ou faire des photocopies. Si jamais le biohacker regrette son acte, il est possible de se faire enlever la puce.

Source : http://www.begeek.fr/les-implant-party-debarquent-a-paris-172890