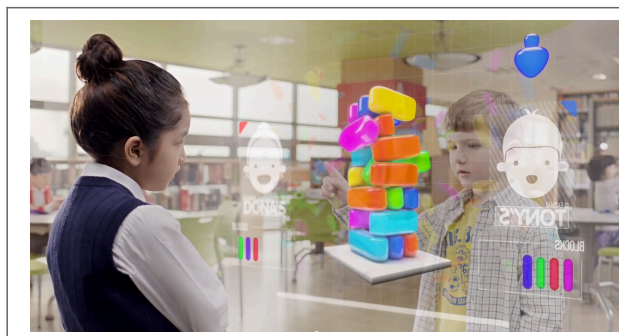


La société numérique d'aujourd'hui et de demain ? | Le Net Expert Informatique



La société numérique d'aujourd'hui et de demain ?

La diffusion au grand public du numérique s'est accélérée ces dernières années. Les enquêtes de l'Observatoire du numérique traduisent parfaitement ce succès. Il ressort notamment que les français ont un équipement adéquat et un usage élevé de l'internet. La France se place dans la moyenne des pays européens, mais on observe un décollage.

Équipements numériques :

82% des français ont un accès à internet depuis leur domicile. En 2002, c'était seulement 22% des foyers. La progression est fulgurante. L'Usage régulier d'internet (au moins une fois par semaine) concerne 78% des Français, contre 91% pour les Pays-Bas. L'Usage quotidien d'internet touche 66% des Français. Chiffres clés 2014

L'internet mobile confirme sa percée : 30% des particuliers de 16 ans et plus en France utilisent une connexion via un réseau de téléphonie mobile pour connecter leur appareil mobile à Internet, contre 23% dans l'UE et contre 56% en Suède. Enquête communautaire 2013

Pour les infrastructures du numérique, la France occupe une très bonne position sur les connexions à haut débit : elle se situe au 5e rang européen pour le ratio abonnements à haut débit par 100 habitants, soit 37% contre 28% dans l'UE. Enquête communautaire 2013

Usages du numérique :

59% des particuliers ont acheté des biens ou services en lignes sur la période étudiée, contre 47% des particuliers dans l'Union Européenne. Enquête communautaire 2013

L'administration numérique progresse bien en France, puisque 60% des particuliers et 90% des entreprises utilisent internet dans leurs relations avec l'administration, contre 41% et 88% dans l'UE. Enquête communautaire 2013

Les usages en entreprises sont plus contrastés et une marge de progression existe encore pour la possession d'un site web. Enquête communautaire 2013

L'ère du numérique est arrivée avec des équipements moins coûteux, un marché à forte concurrence et le développement des usages. La possession d'un ordinateur n'est plus un enjeu. Internet se massifie. Le nouvel enjeu, c'est l'internet mobile.

Le numérique, entendu comme l'ensemble des équipements permettant le passage à Internet et l'ensemble des services associés, est entré dans la vie des français. La France est devenue une société numérique. Quels sont les facteurs de cette transformation?

Un numérique séducteur : le marketing au renfort de la technologie.

Le succès du numérique peut d'abord s'expliquer par un procédé de miniaturisation des objets numériques qui sont devenus conviviaux. Steve Jobs a été visionnaire : il a pensé l'informatique comme un objet convivial. C'est penser les objets par les usages. Apple a changé la vision de l'informatique avec la conception assistée par l'usage.

Les avancées technologiques de l'informatique, conjuguées avec une meilleure prise en compte de l'utilisateur dans le développement d'interfaces numériques toujours plus simples, interactionnelles et esthétiques, ont permis d'ouvrir des pratiques numériques jusqu'alors restreintes à un public d'informaticiens.

Cette démocratisation des outils et des pratiques s'est faite à grand renfort de marketing. Internet arrive en France en 1994 mais ne prend son essor que plus tard. Apple ne devient pas spontanément une méga-marque. La culture numérique a lentement gagné la guerre du marketing.

La diffusion grand public des médias numériques ne peut dès lors se réduire à un déterminisme technique. Quelque chose dans la société a favorisé la réception de ces outils. En 20 ans, 1993-2013, nous avons basculé dans le monde numérique. On peut comparer la situation à la diffusion de l'imprimerie en Europe entre 1450 et 1500.

Ces délais montrent bien que la seule innovation technique n'est rien avant d'être pleinement reconnue dans les usages comme une innovation sociale.

Entrée dans une société de l'information : les facteurs extrinsèques.

Le rapport Nora-Minc sur l'informatisation de la société en 1978 est une photographie prospective de la société actuelle fondée sur l'informatique et les télécommunications. Cette informatisation a conduit à une société de l'information, de l'outil d'information et des données. Une société de la connaissance où la valeur est tombée sur l'information.

La première des raisons, c'est la mondialisation qui conduit à une nouvelle phase du capitalisme, le néo-libéralisme, et au passage à une économie de services. En tant que média vierge, sans frontières et sans règles, Internet a incarné plus que n'importe quel autre espace le néo-libéralisme et symbolise bien cette époque.

La privatisation et la fin des monopoles dans le secteur des télécoms aux États-Unis et les politiques de dérégulation conduites en parallèle par la CE et les pays du sud ont préparé les économies à cet avènement. Enfin, la financiarisation de l'économie a achevé de déconnecter les flux financiers des réalités matérielles.

Au niveau politique, la disparition des idéologies a permis d'imposer un système unifié pour internet et d'ouvrir le réseau en remettant un peu plus en cause le rôle des états. Contrairement aux états, La démocratie profite de ces outils pour développer des modèles participatifs qui pourraient la sortir d'une situation de crise déjà éprouvée.

Enfin, les sociétés occidentales ont connu d'importants changements dans les systèmes éducatifs avec une population plus éduquée, confrontée à la formation continue. Le développement des MOOCs est une réponse à cette évolution. L'élévation du niveau de vie a également développé une société des loisirs qui met l'individu au cœur de l'économie.

Homo numericus : Un nouvel individu accueille le numérique dans sa vie.

D'un point de vue sociologique, les années 80 ont conduit à un changement de valeurs sociales avec le triomphe de l'individualisme et de nouveaux modèles familiaux éclatés. Cette décennie est le ferment de toute la société actuelle avec une critique du modèle classique et du patriarcat, l'émancipation des femmes et l'autonomie des individus.

Ces outils numériques favorisent l'individualisme. Au départ très chers et donc mis en commun, ils sont pourtant conçus comme des outils individuels. Aujourd'hui, le lien affectif à un mobile ou à un portable est avéré et il va aller en s'accroissant avec les objets connectés portatifs devenant une excroissance de leur propriétaire.

Conçu comme le prolongement de l'individu, ces outils lui ont donné l'opportunité de se créer une nouvelle identité numérique, parfois en opposition à une identité réelle. Elle va constituer une échappatoire pour l'individu dans une société en manque de repères. Cette situation fait émerger une nouvelle culture psychologique : la quête de soi.

Les communautés numériques, la blogosphère, puis le web 2.0 apportent un élément de réponse en ce qu'ils vont donner à l'individualisme la possibilité de se connecter. L'individu devient le noyau central de la société de services et de cette société de l'information. Sa croisade pour la quête du lien social sera désormais numérique.

En si peu de temps, le numérique est devenu un mode de vie, un idéal de transformation vers des sociétés dématérialisées, un puissant instrument de socialisation et presque une extension de nous même. Les discours idéologiques sont nombreux et contribuent puissamment à l'idée que nous allons rater quelque chose en nous déconnectant.

Le virtuel est désormais aussi important que le réel. Cet espace virtuel modifie l'individu, contracte sa perception du temps, de l'espace et des liens sociaux. Il donne des modèles de société. C'est un véritable séisme au niveau cognitif qui reconfigure l'être humain et la culture humaine, nous parlerons de plus en plus des « digital humanities ».

Une vision européenne du phénomène sur le site de la Commission.

Nous organisons régulièrement des actions de sensibilisation ou de formation au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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 plaît ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source : <http://siecledigital.fr/2015/08/societe-numerique-realites-perspectives/>

NSA Playset : un kit de surveillance électronique en open source | Le Net Expert

Informatique



NSA Playset : un kit
de surveillance
électronique en open
source

Une équipe de chercheurs tente d'imiter les techniques de la NSA à travers une série d'outils open source destinés à mettre en place des écoutes sophistiquées.

Via de petits outils ou gadgets bon marché dont le design est placé en open source, une communauté de chercheurs en sécurité informatique travaille à rendre accessibles au plus grand nombre les techniques les plus pointues de la NSA.

Les fruits d'une année de travaux ont été présentés la semaine passée dans le cadre de la conférence Black Hat USA 2015, organisée à Las Vegas.

Pour mettre au point leurs solutions d'espionnage électronique, les chercheurs se sont inspirés du catalogue ANT, du nom de cette entité qui fournit, au sein de la NSA, des services de piratage « sur étagère » aux différentes divisions de l'agence de renseignement.

Le catalogue en question avait été révélé fin 2013 par le quotidien allemand Der Spiegel, sur la base de documents exfiltrés par Edward Snowden. D'une cinquantaine de pages, il regroupe des exploits basés sur certaines techniques bien connues... et d'autres plus inédites, reposant notamment sur l'interception de signaux au coeur même des appareils ciblés.

Les outils – finalisés ou en cours de développement – doivent surtout permettre de préparer des systèmes qui peuvent y résister. Ils sont classés en cinq catégories.

Première sur la liste, l'interception radio passive. On y trouve, entre autres, Levitivirus (analyseur de spectre GSM qui prend la forme d'un téléphone Motorola dont le firmware a été modifié) et KeySweeper (enregistreur de frappe basé sur un matériel Arduino et déguisé en chargeur USB ; voir, à ce propos, notre article « Sécurité IT : les adaptateurs secteur ont des oreilles »).

Deuxième catégorie, la « domination physique » avec, entre autres, le dispositif Slotscreamer, qui s'insère dans un port PCIe sur la machine, offrant un accès direct à la mémoire et aux entrées-sorties. Le tout en contournant les mesures de sécurité physiques et logiques.

Troisième rubrique : les implants hardware, symbolisés par Chuckwagon, qui tire parti du port I2C – présent sur nombre d'ordinateurs – pour l'installation de malware.

En quatrième sur la liste, les techniques d'injection radio active, par exemple à travers Tiny Alamo, qui cible souris et clavier Bluetooth pour insérer des informations dans le système ciblé.

Ultime rubrique : les rétrorélecteurs, illustrés par Congaflock, destiné à être implanté sur tout type d'appareil transmettant des signaux par câble. Son rôle : récupérer de nombreuses données, de la frappe clavier aux images affichées sur l'écran.

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.itespresso.fr/nsa-playset-kit-surveillance-electronique-open-source-104776.html>

:

CNIL Besoin d'aide ? – Séances du conseil municipal : faut-il déclarer à la CNIL leur enregistrement vidéo ? | Le Net Expert Informatique

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p>  <p>vous informe...</p>	<p>Faut-il déclarer à la CNIL les enregistrement vidéo des séances du conseil municipal ?</p>
---	--

L'enregistrement et la diffusion sur internet des images d'une séance d'un conseil municipal constituent un traitement automatisé de données à caractère personnel. En effet, les membres du conseil peuvent être identifiés sur ces images.

Dès lors, celui qui filme et diffuse les images, qu'il s'agisse de la mairie, d'un conseiller municipal ou d'un membre du public, doit effectuer une déclaration normale auprès de la CNIL.
En outre, les personnes filmées doivent en être informées.

Nous réalisons régulièrement des actions de mises en conformité de collectivités auprès de la CNIL. pour vous permettre de respecter la loi informatique et libertés, la réglementation de référence relative à la protection des données personnelles.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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 :

<https://cnil.epticahosting.com/selfcnil/site/template.do;jsessionid=1984913614D7AAF7D9FD169D254E833A?id=174&back=true>

Facebook laisse ouvert une faille permettant à des pirates de récolter vos données personnelles | Le Net Expert Informatique



Facebook laisse ouvert une faille permettant à des pirates de récolter vos données personnelles

Des pirates peuvent en toute impunité obtenir le nom, la photo de votre profil et votre emplacement de votre compte Facebook vu que le réseau social n'a pas estimé que cette faille en est réellement une.

Via une faille de sécurité dans Facebook, Reza Moaiandin, un ingénieur logiciel, a réussi à obtenir les noms, les photos de profil et les emplacements des utilisateurs du réseau social, ce qui correspond tout de même à des données privées.

Pour obtenir ces données, le chercheur n'a rien piraté, il a simplement utilisé des possibilités offertes. En l'occurrence, la fonction permettant de trouver un utilisateur à partir de son numéro de téléphone, un paramètre de confidentialité méconnu est qui est par défaut autorisé pour « Tout le monde ». Cela signifie que n'importe qui peut retrouver n'importe qui simplement en connaissant son numéro de téléphone.

Futé, Reza Moaiandin a utilisé un algorithme simple pour générer des milliers de numéros mobiles possibles valables pour les États-Unis, le Royaume-Uni et le Canada. Via une API, il a ensuite simplement cherché à obtenir les données associées aux numéros.

Le fait que le système donne la possibilité de relier des profils Facebook à des numéros de téléphone à une telle échelle est une véritable faille de sécurité vu que c'est une porte ouverte à tous les abus.

Alors que cette faille a été communiquée au réseau social au mois d'avril, Facebook ne la pas corrigée. Un ingénieur indique que cette vulnérabilité n'est pas considérée comme étant une faille de sécurité.

Si Facebook ne compte rien faire pour protéger les données personnelles de ses utilisateurs, la solution est donc que ce soient eux qui se protègent.

Pour ce faire, ils doivent limiter l'accès à leurs informations via cette fonctionnalité méconnue. Pour ce faire, il faut aller dans « Paramètres », puis « Vie privée » et chercher les personnes qui peuvent vous chercher en utilisant le numéro de téléphone fourni. Il faut modifier ce paramètre pour le mettre sur « Amis ».

Il est à souligner que Facebook s'est réfugié justement derrière le fait que chaque utilisateur peut régler la confidentialité de ses données. En clair, le réseau social ne se déclare pas responsable !

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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.linformatique.org/facebook-laisse-ouvert-une-faille-permettant-a-des-pirates-de-recolter-vos-donnees-personnelles/>

L'Afrique menacée par la cybercriminalité | Le Net

Expert Informatique



L'Afrique menacée par la cybercriminalité

L'Afrique est à la traîne en matière de législation sur la cyber-sécurité, un vide juridique qui constitue un véritable danger pour le continent, où, non seulement, il engendre d'énormes pertes économiques, mais porte atteinte à la souveraineté des pays du continent, en mettant les données personnelles des Etats et des citoyens à la merci des firmes internationales du numérique.

L'Afrique n'a aucune maîtrise de la chaîne numérique. Par conséquent, elle se retrouve dans un système de colonisation et de dépendance numérique, fait observer le Pr Olivier Sagna, Secrétaire Général de l'observatoire sur les systèmes d'information, les réseaux et les inforoutes au Sénégal (OSIRIS).

Sagna regrette le fait que « l'Afrique ne possède pas de point d'échange internet, tous les messages échangés passent par un point de transit, qui en fonction des accords et des coûts de droits de communications internationaux, coûte des millions de dollars » aux pays du continent noir.

Selon le Directeur associé de Performances Group au Sénégal, Mouhamed Tidiane Seck, plus de 17 millions de victimes dans le monde ont fait les frais de la cybercriminalité, entre 2012 et 2013. Soit une augmentation de 87% de cas malveillants, occasionnant des conséquences économiques évaluées à trois milliards de dollars de perte bancaire.

L'Afrique du Sud, est l'un des rares pays du continent, grâce à la force de ses lobbys, à avoir mis en place une politique de protection des données personnelles à l'endroit des firmes internationales du numérique.

Concernant l'aspect juridique sur la protection des données personnelles, le Dr Mouhamadou Lo, Président de la Commission de protection des Données Personnelles (CDP) refuse de parler de « désert juridique » en Afrique. « En Afrique, en plus de l'Afrique du Sud, il existe deux textes au niveau de la région Ouest africaine », a indiqué Dr Mouhamadou Lo.

Sur cette dynamique, il faut souligner que la Convention de l'Union Africaine sur la Cyber-sécurité et la protection des données à caractère personnel a été adoptée à Malabo en 2014. « Voter une loi est un premier pas, mais il faut la mise en place d'une commission opérationnelle », a-t-il conclu.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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.lemagazedumanager.com/11300-senegal-la-cybercriminalite-une-menace-pour-lafrique.html>

Google devient Alphabet | Le Net Expert Informatique



Les deux fondateurs de Google annoncent une importante restructuration donnant naissance à une nouvelle société, Alphabet, laquelle englobera le moteur de recherche, les activités satellite historiques et tous les projets initiés par le duo.

Larry Page et Sergey Brin ont annoncé lundi 10 août la plus profonde restructuration financière jamais entreprise par Google depuis son introduction en bourse en 2004. Dans une lettre commune, ils indiquent que le groupe qu'ils ont fondé sera désormais englobé au sein d'une nouvelle société, baptisée Alphabet.



is for Google

As Sergey and I wrote in the original founders letter 11 years ago, "Google is not a conventional company. We do not intend to become one." [more](#)

Larry Page

Un nom à dimension holistique, qui recouvrira les activités historiques du moteur de recherche ainsi que les nouveaux projets lancés au sein de ses laboratoires qui deviendront autant de nouvelles entités, de Life Sciences et ses lentilles connectées pour diabétiques à Calico, dont l'objectif consiste à prolonger la vie de l'homme en passant par la livraison par drone promise par Wing. Google ne sera donc plus désormais que le « G » de l'Alphabet selon Page et Brin.

« Qu'est donc Alphabet ? Alphabet consiste principalement en une collection de sociétés. Dont la plus importante est bien sûr Google. Ce nouveau Google est un peu allégé, dans la mesure où les sociétés qui sont éloignées de nos principaux produits liés à Internet sont maintenant contenus dans Alphabet », expliquent les deux hommes.

L'explication appelle à la logique, partant du principe qu'il n'est pas forcément aisé de mener un moteur de recherche, la première régie publicitaire en ligne au monde et le développement de voitures autonomes ou la recherche en biotechnologies à l'aide de rôles uniques.

« Fondamentalement, nous pensons que (cette nouvelle structure) nous permettra de mieux adapter notre gestion dans la mesure où nous conduisons de façon indépendante des choses qui ne sont pas liées ». Chaque entité au sein d'Alphabet sera menée par son propre chef d'orchestre, Page et Brin assurant le pilotage général, le premier en tant que CEO et le second au poste de président.

La direction du nouveau Google reviendra quant à elle à Sundar Pichai. Il englobe la recherche, la publicité en ligne, YouTube, la cartographie, Android et l'ensemble des infrastructures techniques associées, qui constituent aujourd'hui le bras armé de Google sur le plan financier.

Nest (thermostat connecté), Fiber (fournisseur d'accès) et les différentes entités dédiées à l'investissement (Google Ventures, Google Capital), activités moins « stables » dans le sens où elles induisent des investissements importants associés à une certaine part de risque, appartiendront en revanche à l'ensemble Alphabet.

Au Nasdaq, Alphabet Inc. remplacera Google Inc. en tant qu'entité publique, et l'ensemble des actions sera automatiquement convertis, à valeur et droits équivalents.

En attendant de mesurer l'accueil des marchés boursiers face à ce changement inédit, Page et Brin renouvellent leur profession de foi : cette nouvelle organisation devrait selon eux permettre d'accomplir des tâches toujours plus importantes, inscrites dans une vision à long terme, tout en favorisant le développement de l'ensemble de l'écosystème, de façon toujours plus transparente... pour in fine « améliorer la vie d'autant de personnes que possible ».

Derrière la portée symbolique et les accents humanistes de la déclaration, difficile de ne pas supposer en arrière plan des manœuvres plus terre à terre, visant à redonner de l'agilité sur le plan financier à celle qui fut un jour une start-up et pèse aujourd'hui parmi les plus importantes capitalisations boursières de la planète.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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://pro.clubic.com/entreprises/google/actualite-776160-google-restructure-sein-maison-mere-alphabet.html>

Par Alexandre Laurent

Une faille de sécurité de Hacking Team a été utilisée par un important groupe de pirates | Le Net Expert Informatique

 <p>Le Net Expert INFORMATIQUE Protection des données personnelles Sécurité Informatique - Cybercriminalité</p> <p>vous informe...</p>	<h2>Une faille de sécurité de Hacking Team a été utilisée par un important groupe de pirates</h2>
--	---

Des groupes de pirates informatiques ont utilisé, peu après leur publication, le contenu des fichiers volés à l'entreprise Hacking Team pour se livrer à des tentatives de piratage, révèle l'entreprise de sécurité Kaspersky. Selon Kaspersky, le groupe « Darkhotel », notamment, a utilisé des vulnérabilités qui avaient été employées par Hacking Team, une entreprise spécialisée dans la vente de logiciels de surveillance.

« Darkhotel » s'est notamment signalé par le passé pour avoir utilisé des méthodes élaborées pour placer des logiciels espions – par exemple en prenant le contrôle des réseaux wifi utilisés dans de grands hôtels. Parmi ses cibles figurent des dirigeants de très grandes entreprises, dans la chimie, les cosmétiques ou la pharmacie, des militaires et des responsables d'ONG, dans plusieurs pays d'Europe, d'Asie et d'Afrique, toujours selon Kaspersky. Des cibles et un niveau de sophistication qui laissent supposer à Kaspersky qu'il s'agit d'un groupe étatique ou soutenu par un Etat.

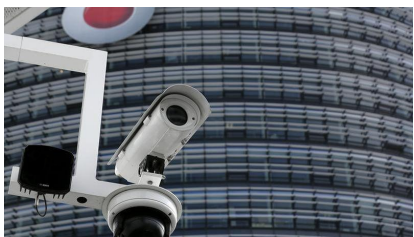
Hacking Team, société italienne à la réputation sulfureuse, est spécialisée dans la vente de logiciels espions et de dispositifs de surveillance électronique. L'intégralité des données de l'entreprise a été publiée en ligne après un piratage, y compris le contenu des messageries de la société. Des associations et des élus européens ont demandé l'ouverture d'une enquête sur les pratiques commerciales de la société, soupçonnée d'avoir notamment vendu des logiciels au Soudan, et une réforme de la législation sur l'exportation de ces technologies.

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 plaît ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.lemonde.fr/pixels/article/2015/08/10/une-faille-de-securite-de-hacking-team-a-ete-utilisee-par-un-important-groupe-de-pirates_4719735_4408996.html

Démonstrations de piratages au salon de «hackers» de Las Vegas | Le Net Expert Informatique



Démonstrations de piratages au salon de «hackers» de Las Vegas

Des pirates informatiques ont fait aussi bien que la bande de George Clooney dans *Ocean's eleven* en arrivant samedi, lors d'un salon à Las Vegas, à ouvrir un coffre-fort et à tromper la vigilance des caméras de surveillance sans être repérés.

La réalité a fini par dépasser la fiction. Eric Van Albert et Zach Banks, deux chercheurs en informatique, ont fait dans la vraie vie ce que Hollywood a déjà accompli à moult reprises. Ils ont détourné le flux vidéo de caméras de sécurité pour injecter à la place leurs propres images et ainsi tromper la vigilance des surveillants en leur faisant croire que tout était normal. En général, au cinéma, c'est là que les cambrioleurs en profitent pour amasser leur butin et s'enfuir ni vu ni connu. Dans les faits, il ne s'agit que d'une simple démonstration, réalisée à l'occasion de la Def Conf, un célèbre salon de «hackers» à Las Vegas.

«Nous avons mis sur pied notre dispositif en restant le plus fidèle possible à ce qui se fait dans les films», a déclaré Eric Van Albert. «Nous voulions voir à quel point ce type d'attaque était plausible», a-t-il ajouté. Lui et son acolyte ont dépensé environ 500 dollars pour fabriquer l'outil qui permet de pénétrer le câble reliant les caméras aux écrans des gardiens. Le flux est ensuite passé à la moulinette d'un programme informatique qui restitue des images inoffensives.

Ouvrir un coffre-fort avec une clef USB

Les deux chercheurs pourraient s'associer avec Daniel Petro et Oscar Salazar de Bishop Fox, une entreprise de sécurité informatique qui a réussi à ouvrir un coffre-fort avec une clé USB. Le coffre n'était pas une boîte en métal épais «toute bête» mais était équipé pour compter les billets et créditer les comptes de dépositaires par internet. Les deux hommes ont indiqué qu'ils avaient choisi la prise USB parce qu'elle leur permettait d'utiliser un ordinateur plus puissant pour ouvrir le coffre. Mais Daniel Petro a souligné que, de toute façon, il fallait accéder physiquement au coffre pour pouvoir en retirer l'argent.

Pour éviter que ce scénario hollywoodien ne se répète, les deux hommes ont prévenu la compagnie qui fabrique les coffres-forts, et qui a déjà trouvé une parade à ce type d'attaque.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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

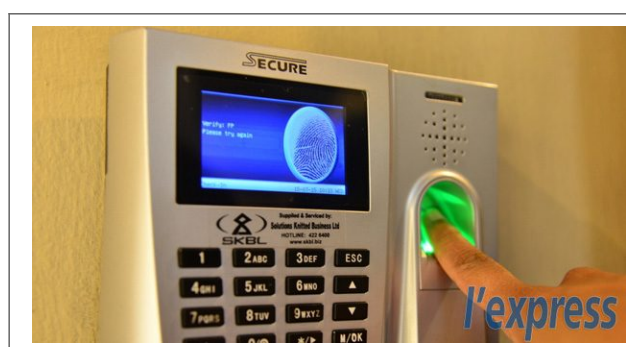
Cet article vous plait ? Partagez !

Un avis ? Laissez-nous un commentaire !

Source

<http://www.lefigaro.fr/secteur/high-tech/2015/08/09/32001-20150809ARTFIG00158-des-hackers-s-inspirent-de-hollywood-pour-piller-des-coffres-forts.php>

Données biométriques au travail : les employeurs dans le flou | Le Net Expert Informatique



Données biométriques
au travail : les
employeurs dans le
flou

Les données biométriques sont à nouveau au cœur du débat. Il n'est pour l'heure pas interdit aux entreprises de réclamer ces données à leurs employés. Mais la situation est-elle sur le point de changer ? C'est la question qui se pose après que l'ICT Appeal Tribunal a donné raison à Amanda Jones, à titre posthume, ce mercredi 5 août. Celle-ci avait refusé de donner ses empreintes digitales alors qu'elle était employée à la Clavis Primary School, à Moka. Elle aurait été renvoyée à la suite de son refus.

Le jugement de l'ICT Appeal Tribunal soulève de nouveau la question du droit des employés de refuser de donner leurs empreintes digitales. Pour l'instant, comme l'explique Pradeep Dursun, président de la Mauritius Employers' Federation (MEF), donner ses empreintes digitales fait partie des conditions d'emploi dans certaines entreprises.

Mais depuis les contestations de la part, entre autres, d'employés de la Cargo Handling Corporation Ltd et d'Alteo Limited, les employeurs sont dans le flou. La MEF attend que la Cour suprême tranche dans l'affaire opposant des syndicats de l'industrie sucrière à Alteo Limited sur cette question. Elle sera alors fixée. Mais, précise Pradeep Dursun, ce n'est pas seulement le privé qui est concerné, mais aussi le secteur public.

De leur côté, les syndicats maintiennent la pression sur cette question de protection des données personnelles. Des syndicalistes du privé, ainsi que Radhakrishna Sadien de la Government Services Employees' Association, souhaitent que les données biométriques soient détruites au même titre que celles de la carte d'identité nationale.

Une employée obtient gain de cause à titre posthume

Amanda Jones, une ex-enseignante de la Clavis Primary School, avait fait appel au Data Protection Office (DPO) à la suite de son renvoi. Celui-ci avait réclamé une enquête de la police. La plaignante, qui est décédée le 17 juin 2014 en Australie, a ensuite obtenu gain de cause auprès du DPO. La Clavis Primary School a fait appel auprès de l'ICT Appeal Tribunal, qui a rejeté cet appel. Dans son jugement, le tribunal a indiqué qu'à aucun moment il n'y a eu d'accord explicite de l'employée. Mais l'institution primaire privée pourrait saisir le recours en appel de la décision de l'ICT Appeal Tribunal, a indiqué à l'express l'avocat de la Clavis Primary School, Me Hervé Duval Jr.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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.lexpress.mu/article/266939/donnees-biometriques-au-travail-employeurs-dans-flou>

Le Pentagone visé par une cyber-attaque russe ! | Le Net Expert Informatique



Le Pentagone
visé par une
cyber-attaque
russe !

Aux alentours du 25 juillet, des pirates informatiques russes ont lancé « une cyber-attaque sophistiquée » contre un système de courriels non confidentiels de l'état-major interarmées au Pentagone, selon des responsables américains ayant requis l'anonymat et cités par la chaîne NBC. Aucune fuite d'informations secrètes n'aurait eu lieu.

Le système informatique du Pentagone est débranché depuis une quinzaine de jours, l'attaque ayant visé 4 000 civils et militaires qui travaillent pour l'état-major interarmées, précise NBC.

Le Pentagone confirme avoir mis le système hors-circuit pour mener une enquête approfondie.

« Par principe et pour des raisons de sécurité opérationnelle, nous ne commentons pas les cyber-incidents ou attaques contre nos réseaux », a indiqué la lieutenant-colonel Valérie Henderson, l'une des porte-paroles du Pentagone dans un courriel.

Selon NBC, l'attaque était automatisée et a réussi, en moins d'une minute, à amasser et à rediffuser les informations collectées sur Internet. La cyber-attaque a été coordonnée par le biais de comptes cryptés et par les réseaux sociaux, d'après ces responsables américains anonymes. Le gouvernement russe n'a pas été directement accusé d'être à l'origine de l'attaque. Mais au regard de sa sophistication, l'attaque aurait été menée par des gens travaillant pour le compte d'une agence gouvernementale, précise NBC.

Ce n'est pas la première fois que des « hackers russes » mythiques sont accusés d'attaques contre les sites de médias et d'institutions occidentales. Fin avril dernier, le porte-parole du Kremlin, Dmitri Peskov, commentait les rapports sur les attaques de « pirates informatiques russes » contre les réseaux informatiques américains et estimait qu'accuser Moscou de tous les maux « était devenu une sorte de sport ».

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.

Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI

Tel : 06 19 71 79 12

formateur n°93 84 03041 84

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.partiantioniste.com/actualites/le-pentagone-vise-par-une-cyber-attaque-russe-2492.html> :