Laboratoire d’analyses médicales piraté : demande de rançon et publication de résultats médicaux | Le Net Expert Informatique

	Laboratoire d’analyses médicales piraté : demande de rançon et publication de résultats médicaux

Le laboratoire de biologie médicale Labio est la cible d'un groupe de pirates. Ce dernier revendique avoir dérobé pas moins de 40 000 identifiants (nom, prénom, login et mot de passe), ainsi que « des centaines » de bilans médicaux. Une rançon de 20 000 euros est demandée et les fuites d'informations confidentielles ont déjà commencé.Les demandes de rançons sont de plus en plus courantes dans le cas des piratages de données informatiques. Récemment, on a par exemple le cas de SynoLocker sur les NAS Synology, de Feedly, puis de Domino's Pizza. Dans ce dernier cas, la société nous avait indiqué qu'elle ne refusait à céder aux demandes de son maitre chanteur, le groupe de pirates Rex Mundi, et qu'aucune transaction financière n'aurait lieu. Des données avaient finalement été mises en ligne quelques mois plus tard.

Rex Mundi demande une rançon de 20 000 euros ou des résultats d'analyse seront publiés
Aujourd'hui, rebelotte avec le même groupe Rex Mundi et, la encore, avec une demande de rançon. Cette fois-ci, c'est un laboratoire français d'analyse médicale qui est visé : Labio.fr. Via l'un de ses comptes Twitter, Rex Mundi indique avoir piraté le site la semaine dernière et détenir « des centaines » de résultats d'analyses sanguines ainsi que pas moins de 40 000 noms, prénoms, identifiants et mots de passe des clients. Les revendications sont les mêmes que pour Domino's Pizza : si la rançon exigée n'est pas payée – 20 000 euros dans le cas présent – les documents récupérés seront publiés dans leur intégralité.

Un ultimatum était fixé. Arrivé à son terme il y a peu, le groupe Rex Mundi a mis ses menaces à exécution et a commencé à dévoiler des informations via son site hébergé sur le réseau Tor. Deux documents sont disponibles. Le premier contient 15 000 noms, prénoms, identifiants et mots de passe qui proviendraient de comptes clients Labio. Le second comporte pour sa part une dizaine de résultats d'analyse du laboratoire de recherche médicale, certains récents, d'autres plus anciens.
Suivant les patients, on y retrouve de l'immuno-sérologie, de la biochimie urinaire et sanguine, de l'hématologie, etc. Autant dire que les informations sont très sensibles :

Nous avons effacé toutes les données confidentielles avant la mise en ligne de l'image

Labio aux abonnés absents, le serveur de résultats fermé « suite à un problème technique »
Nous avons évidemment tenté de contacter par téléphone différents laboratoires affiliés Labio.fr (ils sont quatorze, répartis dans le sud-est et principalement autour de Marseille). Une fois que nous nous sommes présentés en bonne et due forme (en tant que journalistes) et que nous que nous avons expliqué les raisons de notre appel (piratage et bilans médicaux dans la nature), nos correspondants nous ont tous répondu ne pas être au courant et ne rien pouvoir faire pour nous. Impossible également de demander à parler un responsable ou d'obtenir le nom d'une personne à contacter pour évoquer ce problème. La conversation coupait généralement court très vite.

On remarquera par contre que, hasard ou pas du calendrier, dès sa page d'accueil Labio.fr informe ses clients que, « suite à un problème technique, le serveur internet de résultats est temporairement indisponible », et ce, depuis plusieurs jours maintenant. Bien évidemment, nous avons contacté la CNIL et nous attendons également son retour sur la question.

Entre obligation de sécurisation et peine encourue par les pirates
Sur son site, la Commission nationale de l'informatique et des libertés rappelle qu'avec les données de santé, la sécurité est un « impératif » pour ceux qui les hébergent : « il vous appartient de prendre les dispositions nécessaires pour assurer la sécurité des données enregistrées et empêcher qu'elles ne soient divulguées ou utilisées à des fins détournées, surtout s'il s'agit d'informations couvertes par le secret médical » précise-t-elle. Il est notamment question du « chiffrement de tout ou partie des données », mais aussi du « chiffrement de la communication (ex. : chiffrement SSL avec une clef de 128 bits) » lorsque les données circulent sur Internet.

Pour autant, le laboratoire de recherche n'est soumis à aucune obligation de communication auprès de ses clients, seuls les opérateurs le sont (voir le cas d'Orange par exemple), et il semblerait que Labio semble bien décidé à ne pas évoquer le sujet outre mesure, avec nous tout du moins. Si le laboratoire devait répondre à nos questions (nous les avons également contactés via le formulaire présent sur leur site), nous mettrons évidemment cette actualité à jour.

Mais que risquent exactement les pirates dans cette histoire ? Selon l'article 226-16 du Code pénal, « le fait, hors les cas prévus par la loi, de mettre ou de conserver en mémoire informatisée, sans le consentement exprès de l'intéressé, des données à caractère personnel qui, directement ou indirectement, font apparaître les origines raciales ou ethniques, les opinions politiques, philosophiques ou religieuses, ou les appartenances syndicales des personnes, ou qui sont relatives à la santé ou à l'orientation sexuelle de celles-ci, est puni de cinq ans d'emprisonnement et de 300 000 € d'amende ».

Quoi qu'il en soit, l'histoire n'est pas encore terminée puisque Rex Mundi indique que les publications de documents confidentiels continueront si la rançon exigée n'est pas payée.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINE 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

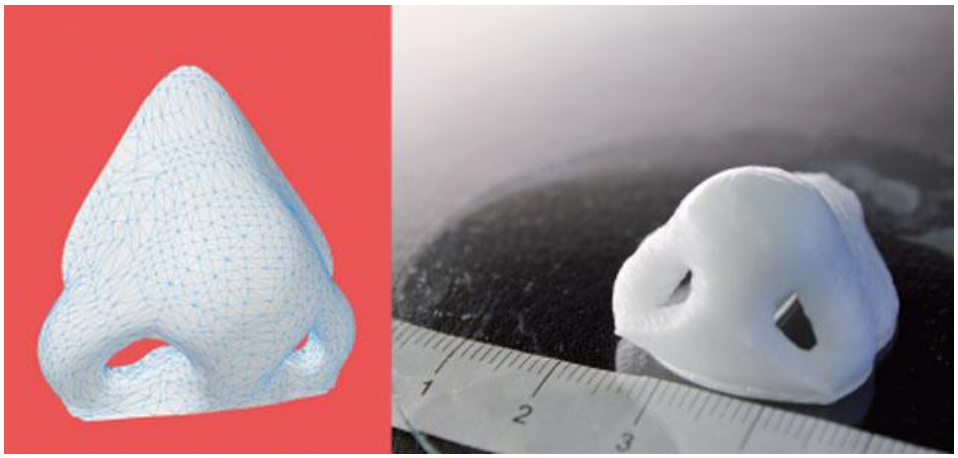
Liste des Laboratoires Labio proche de chez-vous (http://www.labio.fr/nos-laboratoires#labs) :
Laboratoire Centraix – Aix en Provence
Laboratoire des 2 Ormes – Aix en Provence
Laboratoire Celse L'Reste – Aix en Provence
Unité de Fertilité et de Procréation Médicalement Assistée du Pays d'Aix (PMA)
Centre Hospitalier du Pays d'Aix
Laboratoire d'Eguilles
Laboratoire des 5 Avenues – Marseille 6ème
Laboratoire de Saint Marcel – Marseille 11ème
Laboratoire de Saint Julien – Marseille 12ème
Laboratoire des 3 Lucs – Marseille 12ème
Laboratoire de Saint Jérôme – Marseille 13ème
Laboratoire de Saint Mitre- Marseille 13ème
Laboratoire de la Rotonde – Plan de Cuques
Laboratoire de Puricard
Laboratoire de Saint Rémy de Provence

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

Source : http://www.nextinpact.com/news/93499-labio-fr-pirate-demande-rancon-et-publication-resultats-medicaux.htm

---

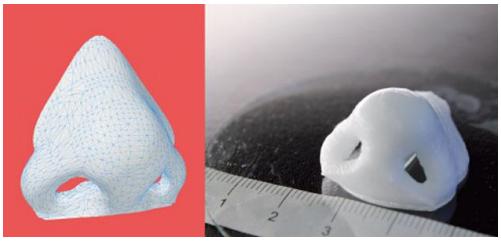
Impression 3D : des cartilages de nez imprimés en seulement 16 minutes | Le Net Expert Informatique



Impression 3D : des cartilages de nez imprimés en seulement 16 minutes

L'impression 3D continue son avancée dans le domaine médical. Des chercheurs d'un laboratoire de Zurich ont conçu un moyen d'imprimer une structure de nez humain qui, une fois greffée, peut s'intégrer à l'organisme.

Les chercheurs du laboratoire de recherche sur le développement et la régénération du cartilage, dépendant de l'École polytechnique fédérale de Zurich, en Suisse, viennent de dévoiler une avancée importante en matière d'impression 3D dans le domaine médical. A l'aide d'une imprimante 3D, ils sont parvenus à concevoir un cartilage de nez à l'aide de biopolymère et de vrai cartilage, le tout en seulement 16 minutes.
Le résultat obtenu peut ensuite être transplanté sur un être humain, et sa conception organique permet d'éviter au mieux le rejet puisque des cellules récupérées par biopsie sur le patient sont intégrées à la démarche d'impression. Au fil du temps, le cartilage imprimé en 3D est donc assimilé par l'organisme. Selon l'équipe de chercheurs, il devrait être impossible de différencier la greffe, des cartilages d'origine, au bout d'un certain temps.
Une découverte qui pourrait aider de nombreux patients dans le cadre, notamment, de la chirurgie reconstructrice. L'exemple du nez est intéressant, car à l'aide de la modélisation 3D, il serait possible de recréer un modèle totalement fidèle à la réalité, pour ne pas voir de différence avant et après un accident. Mais d'autres organes du corps pourraient bénéficier de ce type de technologie, comme une oreille ou un genou, par exemple.



Une technologie coûteuse
Mais reste, à l'heure actuelle, une limite importante, à savoir le coût de fabrication de ce genre de greffon. La « bio-impression » est très coûteuse, et encore inabordable pour la plupart des hôpitaux. Néanmoins, pour les chercheurs, développer ce genre de technique va s'avérer nécessaire par la suite. « Le potentiel de la bio-impression 3D va encore se développer à l'avenir, jusqu'à devenir la technologie ultime permettant aux patients de recouvrer la santé » estime Matti Kesti, responsable du projet. La route est encore longue, mais le futur est prometteur. Par contre, pour imprimer des humains, il faudra attendre un peu…

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/mag/sport/actualite-759491-impression-3d-cartilages-nez-imprimes-16-minutes.html?estat_svc=s%3D223023201608%26crmID%3D639453874_904240618

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.

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

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

Recherche Web : Google a bien triché, et devait être sanctionné | Le Net Expert

Informatique

Recherche Web : Google a bien triché, et devait être sanctionné

En 2013, le régulateur US avait refermé le dossier antitrust sans sanctionner Google. Mais un rapport de la FTC, livré par erreur, atteste de la manipulation des résultats de recherche par Google, au profit de ses services et au détriment des concurrents et même des utilisateurs.

Suite à de longs mois d'enquête, le régulateur américain du commerce (FTC) avait finalement conclu un accord avec Google dans le cadre d'une plainte pour abus de position dominante. Aucune mesure contraignante n'avait été prise à l'encontre du géant de la recherche.Pour autant, cette décision ne signifie pas que les pratiques de Google dans la recherche en ligne aient été jugées par les enquêteurs de la FTC comme saines sur le plan concurrentiel.
Bien au contraire, et c'est d'ailleurs ce que démontre un rapport obtenu par le Wall Street Journal.

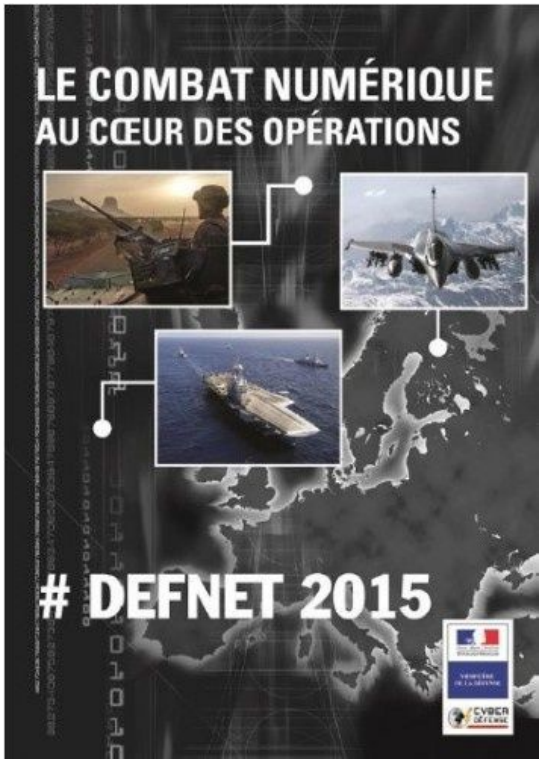
Google a altéré volontairement le ranking
Et ce rapport émane directement du régulateur qui, suite à une requête du WSJ demandant la communication d'un document public, a envoyé par erreur une version non expurgée et partielle du rapport d'enquête du personnel de la FTC.
Les conclusions y sont bien plus tranchées que les informations livrées à l'époque par la FTC pour justifier de faire mettre un terme à son litige avec Google. De nouveaux détails soulignent ainsi que Google a bien manipulé les résultats de recherche au profit de ses propres services, y compris lorsque ces résultats étaient d'une pertinence moindre pour l'utilisateur.
Le WSJ, grâce à cette erreur de l'administration, révèle ainsi plusieurs des pratiques constatées par le régulateur et qui n'avaient jamais été communiquées.

Dans le shopping par exemple, Google classait les résultats de son service avant ceux de ses concurrents, alors que celui-ci affichait un taux de clic inférieur.Le personnel de la FTC chargé de l'enquête estimait donc que Google plaçait volontairement ses services au-dessus de ceux de ses concurrents, comme Yelp, TripAdvisor ou Expedia, qui eux se voyaient dans le même temps rétrogradés par le moteur en termes de ranking, en dépit de leur pertinence pour l'utilisateur.

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

Source : http://www.zdnet.fr/actualites/recherche-web-google-a-bien-triche-et-devait-etre-sanctionne-39816656.htm

Deux bâtiments de notre marine nationale victime d’une cyberattaque sans précédent | Le Net Expert Informatique



Deux bâtiments de notre marine nationale victime d’une cyberattaque sans précédent

Vengeance de Vladimir Poutine ? Malveillance d'un hacker jihadiste ? On ne sait pas… Toujours est-il que deux bâtiments de notre marine nationale, le « Mistral » et son jumeau le «Tonnerre », actuellement en opérations en Méditerranée, viennent de faire de l'objet de cyberattaques simultanées. Leurs ordinateurs de bord ont été infectés par un virus informatique, générant un dysfonctionnement du SCADA, le système de contrôle automatisé qui permet gérer les principales fonctions de ces bateaux de guerre, à commencer par leurs radars et leurs systèmes d'armes. Un groupe d'intervention rapide composé de six membres de nos forces spéciales de cyberdéfense est en cours de déploiement sur les deux navires afin de résoudre la crise au plus vite.

Jusqu'au 27 mars, ce second exercice interarmées doit valider les choix de la chaîne de cyber-défense des armées françaises. Les administrations et opérateurs vitaux sont également concernés.

La cyberdéfense monte en puissance au sein des armées françaises avec la tenue jusqu'au 27 mars de DEFNET 2015, le second exercice interarmées grandeur nature consacré à ce thème.
« Il s'agit d'entraîner l'ensemble de la chaîne de cyber-défense » explique Le lieutenant-colonel Stéphane Dossé, le directeur de l'exercice, qui précise : « Il ne faut pas voir la cyber-défense comme un grand show hollywoodien. C'est un travail opérationnel du quotidien où il faut maintenir et renforcer une ligne de défense, comme dans l'armée de terre ».
Dans la forme, on risque donc d'être bien loin de la vidéo promotionnelle publiée par le Ministère de la Défense en février dernier sur la cyber-guerre : pas de terroristes encagoulés tapis dans l'ombre, pas de missiles expédiés en salve depuis un bâtiment de marine, pas de sergent chef Néo pour prendre à bras le corps la Matrice.
'La cyberdéfense : le combat numérique au coeur des opérations ', vidéo promotionnelle publiée en février 2015 par le Ministère de la Défense.

Un premier exercice avait eu lieu en octobre dernier, avec « un thème simple, sur un seul lieu ». DEFNET 2015 s'articule lui sur une dimension multi-sites. Sept sites militaires sont concernés, ainsi que deux bâtiments de la Marine nationale.
Le scenario de DEFNET 2015 simule, dans un contexte international fictif, des menaces et des attaques cyber multiples contre plusieurs sites sur des thèmes très différents, mentionne le communiqué de presse du Ministère de la Défense. Il associe les spécialistes de cyberdéfense des unités interarmées et des trois armées.
SI militaire, opérateurs vitaux et administrations
Le Ministère de la défense définit la cyberdéfence comme « l'ensemble des actions défensives et offensives conduites dans le cyberespace pour garantir le bon fonctionnement du ministère de la Défense et l'efficacité de l'action des forces armées en préparation ou dans la planification et la conduite des opérations ».
Mais dans le cadre de cet exercice, le périmètre de protection couvre en plus des systèmes d'information militaires, les opérateurs d'importance vitale et les administrations, raison pour laquelle l'Anssi est associée au projet.
A noter que cet exercice est l'occasion de tester le nouveau modèle de réserve cyber. Il s'agit d'accueillir des équipes de volontaires sur des sites militaires, simulant des sites d'intervention. Des équipes d'expérimentation sont constituées d'un réserviste des armées, d'un ou deux enseignants et de 10 à 12 étudiants en informatique et télécommunication d'un niveau bac+ à bac+5 (CentraleSupélec, Telecom Paris Tech ou encore l'Epita sont partenaires).
Elles devront effectuer un travail d'éradication de code malveillant et de réinstallation de système. L'exercice rassemble en tout un effectif de 580 personnes.

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

Source :
http://www.zdnet.fr/actualites/defnet-2015-un-exercice-de-cyberdefense-multi-sites-est-en-cours-39816640.htm
Par Guillaume Serries

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….

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

Apologie du terrorisme : un premier site bloqué en France | Le Net Expert Informatique

Crédit capture d'écran ministère de l'Intérieur

Apologie du terrorisme : un premier site bloqué en France

En audition au Sénat, l'Office central de lutte contre la cybercriminalité avait affirmé qu'une cinquantaine de sites internet pourraient être concernés par ces mesures de blocage.

Le blocage du site www.islamic-news.info a été demandé par l'Office central de lutte contre la cybercriminalité.
Pour la première fois en France, un site internet a été bloqué administrativement pour apologie du terrorisme, a révélé le site spécialisé Next INpact. Consécutivement à l'adoption au mois de décembre de la loi de « lutte contre le terrorisme », le site www.islamic-news.info n'est plus accessible depuis le lundi 16 mars.
Sa page d'accueille redirige les internautes vers le site su ministère de l'intérieur et affiche le message suivant : « Vous avez été redirigé vers ce site officiel car votre ordinateur allait se connecter à une page dont le contenu provoque à des actes de terrorisme [sic] ou fait publiquement l'apologie d'actes de terrorisme ».
Un décret de la loi de « lutte contre le terrorisme » permet à l'Office central de lutte contre la cybercriminalité (OCLCTIC) d'exiger aux fournisseurs d'accès à internet le blocage sous 24 heures des sites désignés comme faisant « l'apologie du terrorisme ». Et ce sans consultation d'un juge.
En audition au Sénat, l'Office central de lutte contre la cybercriminalité avait affirmé qu'une cinquantaine de sites internet jihadistes pourraient être concernés par ces mesures de blocage.
D'après David Thomson, le journaliste de RFI qui a découvert ce blocage, le site » islamic-news.info » est « un site pro-jihad assez peu influent ». Celui-ci se définit comme « un site d'information musulman qui se concentre en particulier sur les territoires dits islamiques » et dit vouloir « fournir une information détaillée de l'actualité du monde musulman ainsi que des explications d'ordre politique et historique ».
Les auteurs du site précisent : « Ce site d'information n'est en aucun cas partisan d'un quelconque groupe, organisation ou mouvement politique, religieux, civil ou armé. Ceci étant, nous considérons qu'il est de notre droit de dénoncer la manipulation, même lorsqu'elle concerne des organisations classées comme 'terroristes' à l'image d'Al-Qaïda, de l'Etat islamique ou des Frères musulmans. Le fait de réfuter des affirmations s'attaquant à ces organisations ne peut en aucune manière signifier une adhésion de notre part à celles-ci ni même faire la promotion de leurs idées et actes. »

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

Source : http://www.atlantico.fr/pepites/apologie-terrorisme-premier-site-bloque-en-france-2042029.html

Attention, insérer cette clé USB dans votre PC peut le détruire ! | Le Net Expert Informatique

Attention, insérer cette clé USB dans votre PC peut le détruire !

Un facétieux hacker a mis au point une fausse clé USB capable de griller une machine lorsqu'elle est insérée dans une prise d'un ordinateur.

On ne le répètera jamais assez : n'insérez jamais dans votre ordinateur une clé USB si vous ne savez pas d'ou elle provient. Car elle pourrait non seulement inoculer un malware dans votre machine, mais aussi carrément… le détruire !
Bon, inutile de trop s'inquiéter, ce danger n'est encore que très théorique. Mais un facétieux hacker russe a bel et bien mis au point une fausse clé USB en mesure de griller les circuits d'un ordinateur en lui infligeant une décharge électrique. L'idée de ce projet est partie d'une légende urbaine amusante : « j'ai lu un article sur un gars qui a volé une clé USB dans le métro. Elle traînait dans la poche extérieure du sac d'un autre type. Il y avait marqué 128 dessus. Le gars est rentré chez lui, l'a inséré dans son ordinateur et la clé a grillé la machine. Alors il a écrit 129 sur la clé et l'a mis dans la poche extérieure de son sac. »

Pour fabriquer sa petite bombe, notre homme, qui travaille dans une entreprise d'électronique, a conçu un petit circuit imprimé et acheté quelques composants. Sa fausse clé contient plusieurs condensateurs et un convertisseur DC/DC. Lorsque la clé est branchée, les condensateurs se chargent grâce au port USB. Lorsqu'ils sont chargés, le convertisseur s'arrête et un transistor décharge l'énergie via les fils de données du port. Lorsqu'ils sont déchargés, le processus de charge reprend… et ainsi de suite jusqu'à ce que la clé grille la machine. Il estime être capable de détruire jusqu'au processeur avec son « invention ».
Ouf, notre hacker ne donne aucun détail qui pourrait permettre de créer son propre « USB Killer ». Il a évidemment plutôt conçu son appareil pour éveiller les consciences aux dangers que représente une clé USB inconnue. Et termine par une boutade : « quant aux applications de cet appareil, je ne les évoquerai pas. Mais un ancien collègue me dit que c'est comme la bombe atomique : c'est cool de l'avoir, mais il ne faut pas l'utiliser. »

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

Source : http://www.01net.com/editorial/648920/attention-inserer-cette-cle-usb-dans-votre-pc-peut-le-detruire/
Par Eric LB

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.

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.

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