Attaquer des sites internet : Désormais un service comme un autre…

Attaquer des sites internet : Désormais un service comme un autre…

Les hackers de Lizard Squad vendent leurs services pour attaquer les sites

Faites-leur attaquer les sites concurrents
Vous aussi vous trouvez que GamAlive est un site qui mériterait d'être mis hors service ? Vous aussi vous estimez que nous dépassons trop souvent les bornes et que notre irréverence mérite un châtiment digne de ce nom ? Vous aussi vous pensez que nos moqueries répétées contre, au choix, les religions, les défenseurs des animaux, les végétariens, les porteurs de tongs, les racistes, les homophobes, les routiers et les fans de Sexion d'Assaut ne peuvent rester impunies, justement parce que vous êtes un pieux routier végétarien racite et homophobe qui défend les animaux et écoute Sexion d'Assaut dans son camion qu'il conduit avec des tongs ?

Ne cherchez plus et faites tomber le site GamAlive.
En effet, les Lizard Squad, ce groupe de hackers à l'origine des perturbations du PSN et du Xbox Live durant les fêtes de Noël, proposent désormais leurs services contre une modeste rétribution.
Ainsi, pour une somme allant de 6 à 500 dollars, vous pouvez vous offrir leurs services. Des attaques DDoS sont proposées contre les sites de votre choix. Des attaques d'une durée de 100 secondes à 30 000 secondes. Réparties sur plusieurs journées, elles peuvent aller jusqu'à bloquer un site pendant une vingtaine de jours, selon leurs dires.
Actuellement, seuls les bitcoins sont acceptés comme moyen de paiement, mais Paypal devrait prochainement être proposé aux clients intéressés par leurs services, même si on doute que le géant américain du paiement en ligne accepte de blanchir de l'argent issu de la cybercriminalité. Car on vous rappelle, au cas où vous seriez un peu con (comme un routier fan de Sexion d'Assaut qui conduit en tongs), que s'offrir leurs services est un acte illégal et répréhensible.

Et non, nous ne vous donnerons pas l'adresse du site, pour des raisons évidentes et, là aussi, légales.
Lire la suite….

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

Source : http://www.gamalive.com/actus/23252-hackers-lizard-squad-services-payants-attaques-ddos-sites-propose.htm
Par Cedric Gasperini

En 2015, la cyberguerre va continuer à changer nos vies…

En 2015, la cyberguerre va continuer à changer nos vies…

En ce début d'année, Industrie & Technologies a repéré pour vous les 15 leviers qui vont booster l'innovation en 2015. Ils ne sont pas tous au même degré de maturité mais tous tireront la créativité et l'inventivité des centres de R&D. Aujourd'hui, la cybersécurité. Un sujet qui sera une préoccupation pour tous les industriels.

Pourquoi il faut la suivre :
Externalisation des données vers le cloud, BYOD et objets connectés, le développement de toutes ces nouvelles technologiques numériques inquiète les spécialistes de la cyber-sécurité. 2015 sera sans aucun doute l'année de la mise en place de dispositifs de défense (et d'attaques) pour permettre aux industriels de se défendre. Fin 2014, Symantec a d'ailleurs listé les principales menaces. Nous vous les présentons ici :

Les moyens de paiements électroniques en ligne de mire
Il est peu probable que des attaques à grande échelle similaires à celles qui ont ciblé les équipements de points de vente aux États-Unis se produisent en Europe. En effet, notre système de carte à puce associé à un code confidentiel ne facilite pas la récupération des données de carte bancaire. Cela dit, ces cartes à puce et à code confidentiel peuvent être subtilisées et utilisées pour effectuer des achats sur Internet. L'adoption grandissante des cartes de paiements sans contact, accompagnée du paiement sans contact via les mobiles, augmentera le risque d'attaques ponctuelles.

Les attaques de cyber-espionnage et de cyber-sabotage à prévoir
En 2015, les campagnes de cyber-espionnage et de cyber-sabotage financées par des États, telles que les opérations DragonFly et Turla observées en 2014, ou encore le spyware très récemment analysé et rendu public Regin, constitueront toujours des menaces pour la sécurité des infrastructures nationales et stratégiques dans le monde entier. Face à de telles campagnes visant à soutirer des renseignements et/ou à saboter des opérations, les entreprises et administrations devront revoir leur politique de cyber-sécurité et donner la priorité à la sécurité, qui deviendra un investissement stratégique plutôt que tactique.

Les secteurs publics et privés devront davantage collaborer pour lutter contre la cyber-criminalité
Fortes des différents démantèlements de groupes de cyber-criminels tels que les opérations Gameover Zeus, Cryptolocker ou encore Blackshades menées en 2014, les autorités internationales adoptent une approche plus active et plus agressive vis-à-vis de la cyber-criminalité en renforçant leur collaboration avec l'industrie de la sécurité en ligne. Cette collaboration entre le secteur privé et les forces de police se poursuivra en 2015 afin d'avoir un impact durable et de stopper les cyber-criminels dans leur élan.

De nouvelles réglementations pour les entreprises européennes
À l'heure où l'Europe souhaite appliquer sa nouvelle législation sur la protection des données, la confidentialité et l'utilisation des informations demeureront au centre des préoccupations en 2015. Contraintes de garantir le respect des nouvelles réglementations, mais aussi de suivre le rythme de l'économie mondiale en exploitant leurs énormes volumes de données pour créer de nouveaux services et de trouver d'autres sources de revenu, les entreprises européennes vont devoir relever un certain nombre de défis en 2015.

Les plates-formes open source seront le maillon faible
L'année 2015 apportera son lot de vulnérabilités dans les bases de données open source et les plates-formes de services Web, que les pirates exploiteront en toute impunité. À l'instar de Heartbleed et Shellshock, ces vulnérabilités constituent une cible potentiellement juteuse pour les pirates, le plus gros risque continuant d'être lié aux failles connues; entreprises et particuliers n'appliquent pas toujours les patchs correctifs appropriés.

L'Internet des objets restera l'Internet des vulnérabilités, mais les attaques seront limitées et ponctuelles
«L'Internet des objets» étant essentiellement lié à la génération de données, les cyber-criminels redoubleront d'imagination pour exploiter les failles logicielles des appareils connectés. Seront notamment concernés les technologies portatives, les équipements domestiques connectés, comme les téléviseurs connectés et les routeurs, et les applications automobiles connectées. Cela dit, nous ne devrions pas observer d'attaques à grande échelle sur l'Internet des objets, seulement des attaques ponctuelles.

Les organisations reconnaîtront que le système identifiant/mot de passe classique a ses limites
À une époque où les organisations cherchent des solutions pour prévenir les intrusions et protéger leurs utilisateurs, elles seront heureuses d'apprendre que des alternatives à l'ancien système se profilent à l'horizon. Notamment, l'authentification à deux facteurs, qui n'exige pas seulement une information que seul le véritable propriétaire connaît (mot de passe, etc.), mais aussi une information que lui seul est censé détenir (numéro de téléphone portable, etc.). Toutefois, alors que chaque service commence à prendre ce genre de mesures, le consommateur va devoir de plus en plus composer avec des applications, numéros de téléphone et questions de sécurité multiples (et ce sur différentes plates-formes), risquant ainsi de lui compliquer la tâche.

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

Source : http://www.industrie-techno.com/en-2015-pas-de-repit-sur-le-front-de-la-cyberguerre.35237

Deux millions d’abonnés du site de TF1 piratés

Deux millions d’abonnés du site de TF1 piratés

Les données de deux millions d’abonnés du site de TF1 ont été piratées. Les hackers détiennent les RIB et autres informations sensibles de ces internautes.

Deux millions d’internautes menacés. Les abonnés du site de TF1 regarderont à deux fois avant de s’inscrire sur des plates-formes numériques. Deux millions d’entre eux ont en effet vu leurs données personnelles (RIB, mais aussi toutes les informations qui ont trait à l’identité numérique) piratées par des hackers vendredi. L’information, rapportée par RTL, a été révélée par Damien Bancal, un spécialiste en cybercriminalité qui a découvert ce piratage.

Techniquement, les hackers sont parvenus à attaquer la partie abonnement presse du site de TF1, sur laquelle il est possible de s’abonner à différents journaux. Une plate-forme que la chaîne privée ne gère pas directement, c’est un prestataire commercial externe qui assure son fonctionnement.

Des usurpations d’identités numériques possibles
Selon Damien Bancal, le spécialiste en cyber-criminalité, ce piratage de grande ampleur pourrait permettre aux hackers d’usurper l’identité des personnes inscrites sur le site. Cela pourrait également déboucher sur « une utilisation de ces données pour lancer d’autres escroqueries, aujourd’hui ou plus tard ».
Autre possibilité, cette base de données pourrait être vendue plusieurs milliers ou millions d’euros à d’autres cybercriminels. Les administrateurs du site ont quant à eux déjà corrigé la faille technique dans laquelle se sont engouffrés les pirates.

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

Source : http://www.europe1.fr/medias/tf1-piratage-de-masse-des-donnees-d-abonnes-2333529

Tor sous la menace d’une

attaque en mesure de corrompre l’anonymat des utilisateurs, les serveurs Directory Authorities dans le viseur

Tor sous la menace d’une attaque en mesure de corrompre l’anonymat des utilisateurs, les serveurs

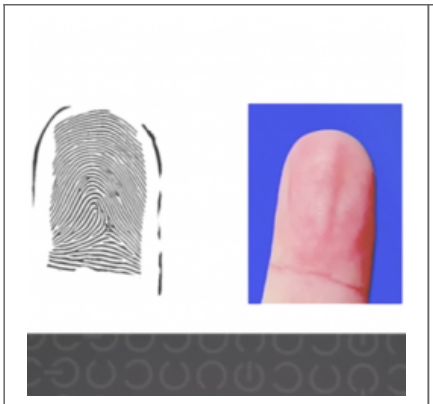
Depuis les révélations d’Edward Snowden sur les pratiques d’espionnage de la NSA et du GHCQ, le réseau anonyme Tor a largement gagné en popularité, ce qui l’a rendu inévitablement le centre des convoitises des agences gouvernementales et la cible de plusieurs attaques.

C’est dans ce contexte que le directeur du projet Tor – Roger Dingledine – a annoncé que le réseau anonyme serait sous la menace d’une attaque informatique ou d’une procédure judiciaire dans les prochains jours.
Dans son billet de blog, Dingledine a tenu à rassurer les utilisateurs que des dispositifs techniques ont été pris pour assurer l’anonymat des utilisateurs, alors qu’ils seront notifiés en cas d’attaques dans les plus brefs délais via le blog et le compte Twitter du projet. De plus, la redondance de l’infrastructure du réseau devrait permettre le fonctionnement de Tor même en cas d’attaque selon le même responsable.
Toutefois, des réserves peuvent être émises quant à la capacité de Tor à résister à cette menace, en effet ladite attaque/procédure cible principalement les serveurs DA (Directory Authorities) via une attaque de type DDoS ou encore par la saisie des serveurs physiques, hors ces derniers qui sont au nombre limité de 10, jouent un rôle crucial dans l’anonymat du réseau, en mettant à disposition des utilisateurs une liste de relais potentiels qui seront par la suite utilisés pour débuter toute communication.
Ainsi, la perturbation du bon fonctionnement des serveurs DA devrait impacter le réseau, pire encore ces serveurs sont aussi responsables de la validation de la liste des relais utilisables, validation qui se fait chaque heure par l’aval de la majorité (au moins 5 serveurs), dès lors le contrôle d’au moins 5 serveurs DA permettrait à l’attaquant de réorienter le trafic vers des relais non sécurisés et déjà sous son emprise, ce qui pourrait signer le coup d’arrêt temporaire de tout le réseau Tor.
À noter aussi que les serveurs DA sont les premiers à être contactés par les utilisateurs, de ce fait leurs adresses IP sont inscrites en dur dans le code du client, ce qui limite le champ d’action et de riposte des responsables du projet.
Quant à la cause d’une telle entreprise, les spéculations vont bon train, allant même à affirmer que cela est relatif au récent piratage de Sony, même si aucune information n’a filtrée lors de l’annonce officielle.
Finalement, le mystère reste entier et les risques sont accrus pour les utilisateurs, ce qui laisse place à la vigilance et à la prudence comme étant les seules consignes en vigueur.

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

Sources :
http://www.developpez.com/actu/79522/Tor-sous-la-menace-d-une-attaque-en-mesure-de-corrompre-l-anonymat-des-utilisateurs-les-serveurs-Directory-Authorities-dans-le-viseur/
https://blog.torproject.org/blog/possible-upcoming-attempts-disable-tor-network
par Arsene Newman

Un hacker parvient à reproduire des empreintes digitales à partir de photos



Un hacker parvient à reproduire des empreintes digitales à partir de photos

Il suffit de prendre la photo des doigts de la personne ciblée avec un appareil photo classique pour récupérer ses empreintes digitales.

On savait déjà quil était possible de récupérer les empreintes digitales d'une personne ayant touché une surface lisse, comme un verre ou un smartphone. Mais un hacker allemand a montré qu'il était possible de voler ces caractéristiques biométriques spécifiques à partir d'une simple photo.
Lors de la 31e convention annuelle (27-30 décembre, Hambourg, Allemagne) du Chaos Computer Club, la plus grande association de hackers européens, un hacker du nom de Jan Krissler, également connu sous le pseudonyme de « Starbug », a expliqué comment reproduire les empreintes digitales d'une personne à partir de simples photos.
Pour sa démonstration, il a copié l'empreinte de la ministre de la Défense allemande, Ursula Von der Leyen.
En effet, il suffit de prendre la photo des doigts de la personne ciblée avec un appareil photo classique pour récupérer ses empreintes digitales. Étant donné que ces empreintes peuvent être utilisées pour l'authentification biométrique, « Starbug » estime que sa démonstration va vraisemblablement obliger « les politiciens à porter des gants lors de leurs apparitions publiques ».
Pour réussir son exploit, Jan Krissler a utilisé le logiciel VeriFinger disponible dans le commerce. Comme source, il est reparti d'un gros plan du pouce de la ministre, pris lors d'une conférence de presse donnée en octobre dernier, plus d'autres photos prises sous des angles différents pour restituer une image complète de l'empreinte digitale.

Si la méthode est aussi facile à réaliser que ce qu'a montré le hacker, elle pourrait remettre en question l'usage des empreintes digitales pour la sécurisation de certains accès. Et dans ce cas, il faut garder ces options de détournement en mémoire. Mais, même si la reproduction des empreintes digitales s'avère viable pour forcer l'accès d'un système, aussi bien un smartphone qu'un lieu très sécurisé, l'exploit accompli par le hacker au 31C3 ne signifie pas pour autant que leur usage est devenu brusquement obsolète.
Les systèmes de sécurité parfaits n'existent pas, et les empreintes digitales ont encore leur place dans la sécurisation des systèmes. Dans un grand nombre de situations, on peut renforcer la sécurité en ajoutant des codes PIN, et il est toujours temps de coupler les solutions biométriques existantes avec des codes ou d'autres protections par mots de passe pour multiplier les niveaux de sécurité.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-un-hacker-parvient-a-reproduire-des-empreintes-digitales-a-partir-de-photos-59753.html
Par Jean Elyan

Les hackers iraniens montent en puissance

Les hackers iraniens montent en puissance

Les pirates informatiques iraniens montent en puissance et ont déjà dérobé des données « hautement sensibles » lors d'attaques contre des gouvernements et des entreprises aux Etats-Unis, en Chine ou en France, affirme aujourd'hui une société américaine de cyber-sécurité. « A mesure que les capacités de l'Iran en matière de cyber-attaque se transforment, la probabilité d'une attaque qui aurait un impact dans le monde réel, à un niveau national ou mondial, augmente très rapidement », met en garde Cylance.

Selon son rapport, l'opération « Cleaver » menée depuis deux ans par des hackers basés à Téhéran leur a déjà permis de conduire une « importante campagne d'infiltration et de surveillance » dans une longue liste de pays qui compte également Israël, l'Arabie Saoudite, l'Allemagne ou l'Inde. Leurs attaques ont ciblé les gouvernements mais également les entreprises du secteur militaire ou pétrolier ainsi que des infrastructures stratégiques (aéroports, hôpitaux…), énumère la société qui affirme avoir des « preuves » que la sécurité aérienne a été par exemple particulièrement « compromise » en Corée du Sud et au Pakistan.

« Les capacités techniques de l'opération Cleaver évoluent plus vite que toutes les précédentes tentatives iraniennes », assure Cylance, selon qui cette offensive répond aux cyber-attaques subies par Téhéran en provenance d'Israël ou des Etats-Unis et visant son programme nucléaire controversé. L'attaque du virus informatique « Stuxnet », qui avait frappé l'Iran vers 2010-2011, aurait ainsi « ouvert les yeux » des autorités de Téhéran en révélant leur vulnérabilité et les a conduits à « contre-attaquer » en lançant l'opération « Cleaver », explique le rapport, selon qui le soutien du régime à cette offensive ne fait aucun doute.

Plusieurs grandes entreprises américaines, dont Apple ou la banque JPMorgan ont récemment été victimes de cyber-attaques dont l'origine n'a pas été formellement identifiée, suscitant des mises en garde croissantes des autorités.

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

Source : http://www.lefigaro.fr/flash-actu/2014/12/03/97001-20141203FILWWW00452-les-hackers-iraniens-montent-en-puissance.php
Par Gilbert Kallenborn

Reprenez le contrôle de votre identité en ligne avec IndieHosters

Reprenez le contrôle de votre identité en ligne avec IndieHosters

Quand on s'inscrit avec un des géants du web comme Google ou Facebook, on souscrit à beaucoup plus qu'un seul service. On peut par exemple utiliser les mêmes identifiants pour s'enregistrer partout sur le web. C'est très pratique. Sauf que si votre compte se fait un jour pirater ou supprimer, vous perdez votre mail et tous les accès aux différents services que vous utilisez. IndieHosters veut vous aider à reprendre le contrôle de votre identité en ligne sans perdre le côté pratique.

Il existe de nombreuses alternatives aux identifications de Facebook et Google. Elles s'appellent OpenID ou Mozilla Personna. Le problème avec ces outils, c'est qu'ils demandent d'être hébergés sur un serveur en ligne et qu'ils doivent être régulièrement mis à jour. Les compétences techniques demandées dépassent bien souvent les bases des internautes avertis et c'est une galère qui décourage même les utilisateurs les plus motivés.
Aujourd'hui, si vous allez chez un hébergeur connu comme OVH ou Gandi, vous aurez droit en un seul clic à une adresse mail, un hébergement pour un site web, une base de données et WordPress ou quelques logiciels libres.
IndieHosters veut aller encore plus loin en proposant tous les outils qui vous permettent de gérer votre identité en ligne. Et pour garantir la confidentialité des données, ils vous offrent en prime un certificat TSL (identique à celui utilisé pour les opérations bancaires en ligne par exemple). Vos données vous appartiennent et elles ne sont pas accessibles pour l'hébergeur. Et comme vous bénéficiez d'un serveur chez IndieHosters, vous pouvez également en profiter pour créer votre blog.
Quand vous souscrivez chez IndieHosters, le serveur se trouve chez une personne et vous pouvez déménager de serveur en allant chez quelqu'un d'autre en un seul clic. Pour l'instant, ils ne sont que 2 chez IndieHosters : Pierre Ozoux et Michiel de Jong. Dans les mois qui viennent, IndieHosters accueillera de nouveaux hébergeurs indépendants et proposera de plus en plus de logiciels libres accessibles et administrables par des débutants, comme Owncloud, la solution alternative à Dropbox.
Pour se développer, ils ont lancé une campagne de financement participatif sur IndieGogo. Et j'ai rencontré Pierre Ozoux alors qu'il était de passage à Toulouse pour qu'il m'explique son projet.
Le but avoué d'IndieHosters est que chaque personne puisse créer son propre nom de domaine, son adresse email, son système d'enregistrement en ligne et finisse un jour par quitter Google, Facebook et consorts. Si vous voulez rejoindre ce mouvement, dépêchez-vous, la campagne de financement se termine dans quelques jours seulement.

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

Source : http://www.gizmodo.fr/2014/12/18/reprenez-le-controle-de-votre-identite-en-ligne-avec-indiehosters.html

---

Accès administratif aux données de connexion: rassuré avec le décret ?

Accès administratif aux données de connexion: rassuré avec le décret ?

Le décret sur l'accès administratif aux données de connexion, en lien avec l'article 20 de la LPM, a été publié le 24 décembre. La cyber-surveillance tend à se généraliser malgré la vigilance de la CNIL.

C'est un grand classique quel que soit le gouvernement : la tentation de faire passer des décrets juste avant Noël pour éviter de faire trop de bruit. Mais le tour de passe-passe n'a pas échappé à des médias vigilants sur la protection de la vie privée comme NextInpact.

Dans le JORF en date du 26 décembre, on découvre le décret 2014-1576 « relatif à l'accès administratif aux données de connexion » (qui avait été approuvé le 24 décembre).
Une belle tentative de mettre en œuvre en catimini d'ici le premier janvier 2015 ce qui avait provoqué une polémique sur la protection des droits civils à l'ère numérique dans le cadre de l'examen du projet de loi sur la programmation militaire (LPM).
Adopté en décembre 2013, le texte dense intègre un article 20 au contour flou qui a des répercussions sur la vie civile : l'accès par les autorités – sans décision judiciaire – aux données de connexion des internautes.
Une approche qui suscitait des craintes sur l'encadrement de l'accès aux données à caractère personnel. Gare à la dérive cyber-sécuritaire, estimait des associations professionnelles du secteur IT comme Renaissance Numérique ou l'ASIC à l'époque.
Ainsi, la loi prévoit initialement l'accès par l'administration aux « informations ou documents traités ou conservés par leurs réseaux ou services de communications électroniques ». Le champ des données surveillées n'était pas limité aux seules données de connexion, mais pouvait concerner l'ensemble des données stockées par l'utilisateur : documents sur le cloud, mails, échanges sur les réseaux sociaux, pseudos, mots de passé, etc.

L'élargissement de la cyber-surveillance reste d'actualité avec la publication du décret associé à l'article 20 de la LPM. Le régime d'exception de l'accès administratif aux données de connexion – jusqu'ici associé principalement à la lutte antiterroriste – est généralisé : « Les données détenues par les opérateurs qui peuvent être demandées sont de plus en plus nombreuses et sont accessibles à un nombre de plus en plus important d'organismes. »
Et ce, pour des finalités très différentes » au nom de divers intérêts nationaux : « sauvegarde des éléments essentiels du potentiel scientifique et économique de la France », « prévention du terrorisme, de la criminalité et de la délinquance organisées et de la reconstitution ou du maintien de groupements dissous ».

Le spectre du Big Brother serait écarté partiellement avec les nouveaux éléments fournis dans le décret du 24 décembre sur « l'accès administratif aux données de connexion ». Celui-ci limite la collecte d'information aux données de connexion (identité de la personne, date et heure de communication, etc.) mais il reste néanmoins à préciser l'exact périmètre des données recueillies.

Bonne nouvelle : le décret semble écarter les risques de droit de regard sur les contenus.
De même, la DGSE, la DGSI ou tout autre service de police judiciaire ne pourront pas directement installer des logiciels d'espionnage (« mouchards ») de manière intensive sur les réseaux des opérateurs.
Selon l'avis de la CNIL rendu le 4 décembre (sur ce qui était à l'époque un projet de décret) mais qui vient juste d'être publié dans le prolongement de la promulgation du décret, il en résulte que « cette formulation interdit toute possibilité d'aspiration massive et directe des données par les services concernés et, plus généralement, tout accès direct des agents des services de renseignement aux réseaux des opérateurs, dans la mesure où l'intervention sur les réseaux concernés est réalisée par les opérateurs de communication eux-mêmes ».
L'autorité française en charge de la protection des données personnelles reste vigilante. « Elle appelle l'attention du gouvernement sur les risques qui en résultent pour la vie privée et la protection des données à caractère personnel et sur la nécessité d'adapter le régime juridique national en matière de conservation et d'accès aux données personnelles des utilisateurs de services de communications électroniques. »
L'année 2015 va mal démarrer alors que le gouvernement prépare une loi sur le numérique. L'occasion d'éclaircir le débat ? Dans le cadre de la consultation gouvernementale ouverte au grand public pour élaborer cette loi, on espère un peu plus de transparence à propos de cette extension de la cyber-surveillance.

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

Source : http://www.itespresso.fr/acces-administratif-donnees-connexion-rassure-publication-decret-85710.html

Confidentialité et cryptage récompensés

Confidentialité et cryptage récompensés

Sophia Genetics. La société lausannoise devient la première entreprise doublement certifiée ISO 13485 et ISO 27001.

Sophia Genetics, leader européen en génomique clinique et séquençage ADN de nouvelle génération (NGS), devient la première entreprise doublement certifiée ISO 13485 et ISO 27001.
D'après un communiqué, l'entreprise précise que les certifications du groupe BSI récompensent, entre autres, l'approche de Sophia Genetics du traitement de l'information et du cryptage des données de patients. Cette dernière, en instance d'obtention de brevet, vise à protéger la confidentialité des informations génomiques.
Les serveurs redondants installés par Sophia Genetics dans divers sites hautement sécurisés, offrent à ses clients la confiance nécessaire afin de traiter, analyser et stocker les données de milliers de patients suspectés ou atteints de maladies chroniques.
La certification ISO 27001 a été attribuée à la plateforme Information Security Management System de Sophia pour toutes les informations sécurisées internes et externes de ses clients.
Sophia Genetics se charge à l'heure actuelle de l'analyse, du stockage et du traitement des données de plus de 30 hôpitaux et laboratoires de pointe en Europe.

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

Source : http://www.agefi.com/une/detail/archive/2014/december/artikel/sophia-genetics-la-societe-lausannoise-devient-la-premiere-entreprise-doublement-certifiee-iso-13485-et-iso-27001-388417.html

Le site web de l'Internet System Consortium touché par un malware

Le site web de l'Internet System Consortium touché par un malware

Le site web de l'Internet System Consortium, qui édite notamment la solution BIND pour la gestion de DNS, a été victime d'un malware. Les utilisateurs qui ont visité le site web de l'ISC dans les dernières semaines sont invités à scanner leurs machines.

Le site web de l'Internet System Consortium a été temporairement mis hors ligne suite à la découverte d'une attaque ayant pu affecter les visiteurs du site. Une page statique est actuellement en ligne avec des indications nécessaires pour les utilisateurs de BIND, le serveur DNS proposé par l'ISC. L'attaque subie par le consortium n'a pas affecté les programmes publiés par l'ISC dont le code source est hébergé sur un serveur différent du site web. Selon The Register, qui a contacté un membre de l'Internet System Consortium, l'attaque n'était pas ciblée et n'a touché que le site web, qui avait recours au CMS WordPress. Une attaque automatisée « inhérente aux CMS de ce type » ajoute Dan Mahoney, responsable de la sécurité de l'ISC.
L'attaque a permis aux attaquants de rediriger certains internautes vers une page distribuant un malware windows, le Angler Exploit Kit. Celui ci est connu depuis quelques temps et exploite plusieurs failles dans Flash, Internet Explorer et SilverLight pour ensuite exécuter du code malveillant sur la machine ciblée. La finalité du malware reste encore peu connue, mais mieux vaut prévenir que guérir. Pour l'instant, l'ISC n'a pas encore signalé d'utilisateur infecté par leur site mais a préféré mettre le site hors ligne en attendant de résoudre le problème.
Plus de peur que de mal donc, mais l'ISC fait partie des sociétés vitales pour Internet : le consortium développe et maintient le code de BIND, le serveur DNS le plus largement utilisé aujourd'hui sur le réseau et héberge l'un des 13 serveurs racine du DNS. Si ces derniers ne sont pas affectés par l'attaque, les internautes et administrateurs systèmes qui ont visité le site wordpress de l'ISC avant le 22 décembre ont en revanche de quoi s'inquiéter.

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

Source : http://www.zdnet.fr/actualites/le-site-web-de-l-internet-system-consortium-touche-par-un-malware-39812011.htm
Par Louis Adam