Votre entreprise est-elle assurée contre les pirates informatiques ? | Le Net Expert Informatique

Cyberattaques: votre entreprise est-elle assurée contre les pirates ?

Pertes de données, poursuites judiciaires, systèmes informatiques endommagés… les cyberattaques représentent une nouvelle gamme de risques auxquels les entreprises petites et grandes sont confrontées. Sentant la bonne affaire, certains assureurs offrent maintenant une protection contre ces écueils. En quoi consiste une telle assurance ? Est-elle devenue incontournable ?

Évaluer les risques

Inutile de parler d'assurance si on ne connaît pas d'abord le risque auquel on est exposé. Celui d'être victime d'une cyberattaque ne se mesure pas tant selon la taille de l'entreprise que par rapport au type d'information que l'on y traite. Ce n'est donc pas seulement le souci des grandes boîtes. L'étude «Internet Security Threat Report 2014» du concepteur d'antivirus Symantec révèle d'ailleurs que 61 % des hameçonnages ciblés ont visé des PME en 2013, comparativement à 50 % un an plus tôt.

Or, des études récentes de Cisco montrent qu'un peu plus de la moitié des entreprises canadiennes n'ont pas encore mis en place un plan en matière de sécurité informatique. «C'est primordial pour déterminer les types de renseignements à protéger, les moyens de les stocker, les personnes qui y ont accès, l'équipement, etc.», précise Maya Raic, présidente-directrice générale de la Chambre de l'assurance de dommages.

Stockez-vous sur vos serveurs une base de données contenant le numéro d'assurance sociale de médecins spécialistes ? Ou un simple catalogue de vos produits ? Les données ont un degré de sensibilité variable. Cela dit, plus vous traitez de l'information de tiers ou de la propriété intellectuelle, plus vous avez de risques de poursuites en cas de brèche de sécurité.

« 117 339: c'est le nombre de cyberattaques commises chaque jour dans le monde, d'après une récente enquête de PwC. Et ce ne sont là que celles dont les entreprises sont conscientes, puisque près des 3/4 des attaques ne sont pas décelées. »

Des polices sur mesure

«On compte actuellement une dizaine d'assureurs au Canada qui protègent les entreprises contre les cyberrisques», soutient Maya Raic.

Comme on n'en est qu'aux balbutiements de ce type d'assurance, les clauses varient d'un assureur à l'autre. «On traite encore les clients au cas par cas, donc ceux-ci peuvent négocier les termes», mentionne Jean-François De Rico, associé au cabinet d'avocats Langlois Kronström Desjardins.

Les polices peuvent couvrir la responsabilité liée aux pertes de données (les recours collectifs potentiels, les atteintes à la réputation commerciale ou les frais liés au redémarrage des systèmes), la gestion de crise, l'interruption des affaires, la cyberextorsion, etc.

Quant aux exclusions standards, ces polices n'en comportent pas vraiment, contrairement aux autres types d'assurance qui excluent d'emblée certains risques. Ce que vous pourriez voir toutefois, c'est une clause qui délimite le cadre de l'assurance. «Par exemple, la responsabilité civile des dirigeants et des administrateurs n'est pas couverte par la cyberassurance, puisque cette protection existe déjà dans une autre police d'assurance sans lien avec le cybercrime», illustre Alexis Héroux, courtier en assurance de dommages chez Marsh Canada.

« Installer les mises à jour dans les 48h où elles sont disponibles par les fournisseurs d'antivirus réduit les risques de cyberattaques de 85%. »

C'est combien ?

Les limites de couverture varient énormément selon les compagnies d'assurance et peuvent aller de 500 000 dollars à 20 millions de dollars. Si plusieurs assureurs se réunissent, la limite peut même atteindre 250 millions de dollars.

On devine que le coût des primes varie tout autant, selon la limite choisie et l'ensemble des facteurs qui peuvent influencer le risque : le type et la quantité de données utilisées et recueillies par l'entreprise, le système de gestion en place, etc. Les PME dont les besoins de protection sont moindres pourraient réussir à obtenir une prime annuelle minimale de 1 500 dollars, mais c'est en général beaucoup plus coûteux. Retenez surtout que tout se négocie, selon votre budget.

« 201$: c'est le prix que coûte en moyenne chaque donnée de tiers sensible et confidentielle qui a été volée. »

Cela dit, comme pour les autres types d'assurance, les cyberrisques ne reposent jamais entièrement sur les épaules des assureurs. L'entreprise a sa part de responsabilité. Aussi, plus on a une infrastructure de sécurité sophistiquée et bien gérée, plus on réduit le risque, et donc le coût de la prime (voire la nécessité d'une protection d'assurance).

Cependant, quand on sait que même des spécialistes comme Symantec ont déjà été victimes d'une cyberattaque, il vaut mieux, parfois, investir un certain montant en assurance pour couvrir ces nouveaux aléas.

Source : http://www.lesaffaires.com/dossier/gestion-des-risques/cyberattaques-votre-entreprise-est-elle-assuree-contre-les-pirates-/579164

Google, aussi Big Brother de la santé ? | Le Net Expert Informatique

	Google, aussi Big Brother de la santé ?

Pour décrire les ambitions du fondateur de Google en matière de santé, il faut commencer par une métaphore automobile qui illustre la façon dont Larry Page conçoit la surveillance médicale. Autrefois, lorsqu'il conduisait une voiture, le conducteur savait que les pneus étaient mal gonflés lorsqu'ils éclataient, il savait que le moteur était en surchauffe lorsqu'un panache de fumée s'en échappait… Hormis le compteur de vitesse, il n'y avait guère d'indicateurs en temps réel de l'état de la mécanique.

Aujourd'hui, c'est l'inverse. On ne prête plus attention à la santé de notre moteur parce que justement on sait qu'il est sous surveillance, l'informatique embarquée nous prévient en cas de surchauffe ou de sous-gonflage des pneumatiques, avant même que la panne survienne. Or, en matière de santé, nous en sommes encore au tout début de l'automobile. Hormis nos sensations, nos douleurs, nous ne disposons pas en temps réel de détection, ni de capteurs pour nous informer et surtout prévenir l'apparition des problèmes avant même qu'ils ne deviennent graves.
Étrangement, nous surveillons en temps réel l'état de la mécanique d'un objet automobile (et on n'admettrait pas l'idée de ne pas avoir en permanence l'information sur la surchauffe de son moteur de voiture), mais en revanche nous acceptons encore l'idée de n'avoir strictement aucune information en temps réel sur la fiabilité de nos organes, sur leur surchauffe, sur leur sous-gonflage.
Tel est le constat de base des ingénieurs de Google sous la houlette de Larry Page, qui a recruté les meilleurs spécialistes des biotechnologies de la Silicon Valley. Larry Page et son complice Sergueï Brin ont fait une irruption remarquée dans le domaine de la santé, notamment en créant Calico (California Life Company), une filiale spécialisée dans la lutte contre les maladies et le vieillissement, dont l'ambition, disent les médias, est ni plus ni moins que de « tuer la mort », d'empêcher non seulement l'apparition des maladies mais le vieillissement humain lui-même.

Déjà des applications concrètes
Ce n'est pas d'aujourd'hui que les fondateurs de Google ont décidé de se lancer dans la recherche biomédicale. On entrevoit déjà des applications concrètes. Une des réalisations les plus « simples » est consacrée au diabète en reprenant le concept des lunettes connectées (les Google Glass qui permettent d'intégrer des écrans miniatures directement dans notre champ de vision), mais cette fois avec des lentilles de contact et des capteurs biologiques.
Plutôt que de se piquer perpétuellement, d'analyser leur glycémie à intervalle régulier mais distant, puis d'y remédier eux-mêmes en se piquant…, les diabétiques n'ont pas encore à disposition une assistance en temps réel, une mesure permanente du taux de sucre. Les ingénieurs de Google ont donc conçu des lentilles de contact munies d'un capteur de sucre et d'un émetteur HF : le capteur mesure directement sur l'oeil la glycémie, dans les larmes du patient, transmet l'information par wifi sur une montre et prochainement, un appareillage automatique injectera dans le corps des diabétiques la quantité d'insuline manquante, après mesure automatique sur notre oeil par une lentille intelligente. Pour reprendre la métaphore automobile, il s'agirait d'un suivi en temps réel de notre métabolisme exactement comme le manque d'essence sans besoin de s'arrêter à la pompe.

S'attaquer aux causes du vieillissement et des maladies
Larry Page ne limite pas les ambitions de Google à ce type d'objet. Son ambition est de s'attaquer aux causes du vieillissement et des maladies. « Tout ce que vous imaginez est probablement réalisable. Il vous suffit de le visualiser et d'y travailler », a récemment déclaré Larry Page aux cadres dirigeants de son entreprise.

Larry Page et ses équipes ont annoncé travailler sur la mise au point d'un nano système de détection des anomalies (dont les chercheurs parlent depuis plusieurs années comme une piste de recherche) qui pourrait, chez Google, devenir une réalité concrète dans quelques années. Dans le laboratoire secret où les ingénieurs de Google imaginent le monde de demain, Google X, on travaille à la mise au point concrète de nano-diagnostics.

L'idée de base est la suivante : vous ingérez dans votre organisme des micro-objets, des nano objects, capables de détecter les cellules défaillantes, les cellules mutantes (si vos cellules se dégradent et sont par exemple à un stade pré-cancéreux). Là encore ces nano détecteurs seraient connectés à une montre qui collecte l'information. L'idée est d'avancer au maximum le stade du diagnostic.

Et ce qui est imaginé pour le cancer pourrait être développé pour d'autres maladies. Dans une récente interview, Larry Page a expliqué que l'ambition était bien plus grande en effet. Résoudre le cancer, dit-il, accroîtrait l'espérance de vie humaine de quelques années seulement, alors qu'en revanche, s'attaquer, sur les chromosomes, aux racines du vieillissement permettrait d'atteindre ce qu'on peut appeler la vie éternelle, en tout cas une longévité bien supérieure. Il ne faut pas s'attendre à des annonces dans les prochaines années, c'est un travail de longue haleine car précisément les labos de recherche de Google ont les moyens et la consigne de travailler sur le très long terme.

En résumé, dans le domaine de la santé, Larry Page ne veut pas se contenter d'améliorer à la marge le sort des patients mais cherche ni plus ni moins à révolutionner ce domaine comme il a révolutionné les sciences de l'information. Il est un chaud partisan de ce qu'on appelle le transhumanisme, ou l'homme augmenté, ce qui fait débat chez les penseurs, les philosophes et les religieux, et qui fait peur souvent pour tout ce qui concerne l'intelligence artificielle. Le transhumanisme ne lui fait pas peur, il en a pris la tête avec des moyens en milliards de dollars.

Pourquoi Google s'intéresse à la santé ?
Le fondateur du célèbre moteur de recherche Internet se consacre à la santé pour plusieurs raisons.
– Il y a tout d'abord un sentiment d'injustice ressenti dans sa jeunesse, lorsqu'il était étudiant, quand son père est décédé des suites de la polio, une maladie qui avait quasiment disparu de la surface de la planète mais qui a emporté son père, Carl Page, brillant informaticien.
– Deuxième élément : les problèmes de santé dans l'entourage des fondateurs de Google, (la mère de son acolyte souffre de la maladie de Parkinson) et les inquiétudes sur la santé de Larry Page lui-même, qui est atteint depuis quelque temps d'un mal mystérieux : une paralysie d'une corde vocale, qui lui donne une voix altérée et qui a fait craindre un cancer en affolant récemment les cours de l'action Google.

Enfin il y a la grande ambition, l'ambition d'apporter au monde entier des inventions qui serviront à des millions de personnes. On sait que de plus en plus le « big data » – le traitement d'informations nombreuses et complexes – sera une donnée fondamentale des traitements individualisés du futur. Larry Page, d'abord avec son moteur de recherche, puis avec sa voiture sans conducteur et ses Google glass, a déjà révolutionné plusieurs fois le monde, quoi de plus beau pour un tel homme que de révolutionner la santé humaine, la longévité, au point de chercher à éradiquer les causes du vieillissement et toucher du doigt la perspective divine de la vie éternelle.

Source : http://www.francetvinfo.fr/sante/decouverte-scientifique/google-et-la-sante-un-nouveau-big-brother_902537.html

De graves failles dans les NAS Synology à corriger | Le Net Expert Informatique

De graves failles dans les NAS Synology à corriger

Le fabricant de NAS Synology a corrigé plusieurs vulnérabilités dans son OS maison DSM (DiskStation Manager) – et ses composants associés – qui anime ses appliances de stockage, dont l'une pouvait permettre à des attaquants de compromettre les données stockées.

En effet, la vulnérabilité la plus sérieuse concerne donc Synology Photo Station, une fonction du DSM, le système d'exploitation basé sur Linux. Photo Station permet aux utilisateurs de créer des albums photo en ligne et des blogs accessibles à distance via l'adresse IP publique du périphérique. Mais des chercheurs en sécurité de l'entreprise néerlandaise Securify ont découvert que Photo Station n'effaçait pas correctement les entrées utilisateur, laissant à des attaquants la possibilité d'injecter des commandes système qui pourraient être exécutées avec les privilèges du serveur web.
De plus, Photo Station n'est pas protégé contre le cross-site request forgery (CSRF), une technique qui permet à un site web de forcer le navigateur d'un visiteur à exécuter des actions malveillantes sur un site différent de celui sur lequel il se connecte. Donc, même si Photo Station n'est pas configuré pour être accessible depuis Internet, un attaquant pourrait inciter un utilisateur situé sur le même réseau que le périphérique NAS à visiter une page web malveillante qui utiliserait le CSRF pour exploiter la vulnérabilité par commande d'injection sur le réseau LAN local. « En tirant parti de cette faille, des attaquants pourraient compromettre le périphérique NAS, et toutes les données qui y sont stockées », ont expliqué les chercheurs dans un avis qui comprend également une preuve de concept de l'exploit.

Des ransomwares s'attaquent à Synology
La version 6.3-2945 de Photo Station livrée la semaine dernière par Synology corrige cette vulnérabilité. Mais les notes de version font simplement état « d'améliorations de sécurité » sans donner de détails. La nouvelle version corrige aussi deux vulnérabilités cross-site scripting (XSS) identifiées par les chercheurs de Securify. Celles-ci pourraient être exploitées pour tromper les utilisateurs de Photo Station en les incitant à cliquer sur une URL malveillante qui exécute un code voyou dans leurs navigateurs. En cas de succès de ces attaques, des pirates pourraient voler les jetons de session ou les identifiants de connexion des utilisateurs de Photo Station ou exécuter des actions arbitraires en usurpant leur identité.
La semaine dernière Synology a corrigé une vulnérabilité similaire dans l'interface de gestion de DiskStation Manager. Les utilisateurs sont invités à mettre DSM à jour en version 5.2-5565 Update 1. Dans le passé, les boitiers NAS de Synology ont déjà été la cible de pirates. Ainsi, pas plus tard que l'an dernier, des attaquants ont exploité une vulnérabilité pour infecter plusieurs boitiers avec un ransomware destiné à crypter les fichiers stockés. Auparavant, les pirates avaient réussi à s'introduire dans les boitiers NAS de Synology pour faire tourner des programmes qui généraient de la crypto-monnaie pour leur compte.

Source : http://www.lemondeinformatique.fr/actualites/lire-synology-corrige-de-graves-failles-dans-son-os-dsm-61277.html
Par Jean Elyan

Contrôles de la CNIL en 2015 – Demandez le programme… | Le Net Expert Informatique

Contrôles de la CNIL en 2015 – Demandez le programme…

En 2015, la CNIL contrôlera des technologies ou des traitements récemment mis en œuvre et faisant partie du quotidien des Français.

En 2015, un objectif d'environ 550 contrôles est prévu (421 contrôles réalisés en 2014), se décomposant de la façon suivante :
• environ 350 vérifications sur place, sur audition ou sur pièces. Un quart des contrôles sur place portera sur les dispositifs de vidéoprotection / vidéosurveillance
• 200 contrôles en ligne.

Les thématiques prioritaires des contrôles 2015
Comme chaque année, la CNIL prévoit de dédier une part significative de son activité de contrôle à des thèmes choisis du fait de leur impact sur les libertés et du nombre important de personnes concernées.

Le paiement sans contact : le large développement de ces dispositifs en fait une thématique de première importance, eu égard notamment au nombre de personnes concernées. Outre les questions de sécurité, la prise en compte du droit d'opposition sera notamment vérifiée.

Le traitement de données personnelles dans le cadre de la gestion des risques psycho-sociaux (RPS) en entreprise : dans le prolongement de l'accord national interprofessionnel de 2008 relatif à l'amélioration des conditions de travail, de plus en plus d'entreprises diligentent des enquêtes sur les risques psychosociaux auprès de leur salariés afin d'évaluer et de mieux lutter contre le stress au travail. Ces enquêtes soulèvent des questions pratiques qui ont conduit de nombreux salariés à saisir la CNIL. Les contrôles s'opèreront auprès de prestataires et d'entreprises (publiques et privées) ayant mené une enquête RPS ces dernières années.

Le Fichier National des Permis de Conduire mis en œuvre par le ministère de l'Intérieur : ce fichier répertorie l'ensemble des permis de conduire enregistrés en France (environ 40 millions). Le solde des points restants sur le permis est consultable en ligne depuis le site telepoints.info. Le FNPC comporte également toutes les décisions relatives au permis de conduire, et notamment, les décisions administratives (retrait, suspension, annulation, restriction du droit d'en faire usage) et judiciaires (y compris les compositions pénales, amendes ainsi que les procès-verbaux des infractions constatées). Les vérifications porteront en particulier sur la fiabilité et la mise à jour des données, leurs modalités d'accès et leur sécurisation.

Les objets connectés « bien-être et santé » : un écosystème s'est développé autour d'une offre bien-être et santé comprenant des objets connectés et des services en ligne, permettant le suivi individuel et le partage de données relatives par exemple à l'activité physique ou l'évolution de la corpulence du détenteur. Ces dispositifs suscitent de nombreuses interrogations quant à l'information et au consentement des utilisateurs.

Les outils de mesure de fréquentation des lieux publics : ces nouveaux dispositifs déployés dans l'espace public (centres commerciaux, quartiers ou villes entières) permettent via les connexions aux bornes mobiles et wifi une mesure fine du trafic de données personnelles. Ces mesures permettent entre autres objectifs de monétiser l'espace publicitaire. Des contrôles sur ces thèmes permettront de renforcer la doctrine naissante.

Les « Binding Corporate Rules » (BCR) : à ce jour, 68 sociétés ont adopté des BCR. Ces dispositifs n'ont fait pour l'heure l'objet d'aucun contrôle ex-post. La réalisation de contrôles de quelques entreprises ayant adopté des BCR fournira un éclairage sur l'impact du dispositif au regard de la protection des données personnelles et du respect de la vie privée au sein des groupes concernés.

Enfin, l'année 2015 sera l'occasion pour la CNIL de continuer le travail de coopération internationale entre autorités de protection des données. Cette coopération s'effectuera notamment au travers du troisième volet du « Sweep Day » coordonnée par le GPEN (« Global Privacy Enforcement Network » – réseau international d'autorités en charge de la protection de la vie privée) qui concernera le thème de « la vie privée de la jeunesse » (« Youth Privacy »).

Concrètement, l'audit conjoint qui sera réalisé en mai portera sur les services en ligne proposés aux mineurs (sites visant particulièrement les utilisateurs de moins de 12 ans et/ou les adolescents). Les autorités se concentreront notamment sur l'information, et le contrôle de l'âge.

En outre, des contrôles seront menés dans le cadre de la coopération européenne en matière de police (Europol, Schengen, etc.).

Source : http://www.cnil.fr/linstitution/actualite/article/article/programme-des-controles-2015/

Attaque à grande échelle de routeurs | Le Net Expert Informatique

Une attaque à grande échelle utilise les browsers pour détourner les routeurs

Des chercheurs ont découvert un outil d'attaque web qui permet à des pirates de détourner les serveurs DNS des routeurs et de les remplacer par des serveurs voyous.

Des cybercriminels ont développé un outil d'attaque web à grande échelle qui leur permet d'exploiter les vulnérabilités des routeurs et de détourner leurs paramètres DNS quand les utilisateurs visitent des sites web compromis ou sont dirigés vers des publicités malveillantes depuis leurs navigateurs. L'objectif de ces attaques est de remplacer les serveurs DNS configurés sur les routeurs par des serveurs voyous contrôlés par des attaquants. Ainsi, les pirates peuvent intercepter le trafic, le rediriger vers des sites frauduleux, détourner les requêtes de recherche, injecter des publicités malveillantes sur les pages web et plus encore.

L'adresse DNS, qui est comparable à un annuaire de l'Internet, a un rôle essentiel. Elle traduit les noms de domaine, plus faciles à mémoriser, en adresses IP indispensables pour faire communiquer les ordinateurs entre eux. La gestion des adresses DNS se fait en cascade. Quand un utilisateur tape le nom d'un site Web dans un navigateur, la requête est d'abord transmise au système d'exploitation. Et, pour diriger le navigateur vers l'adresse IP demandée, le système d'exploitation doit passer par le routeur local qui est lui-même chargé d'interroger les serveurs DNS généralement configurés et gérés par le fournisseur d'accès internet. La chaîne de commandes se poursuit jusqu'à ce que la demande parvienne au serveur ayant autorité pour le nom de domaine recherché ou jusqu'à ce qu'un serveur fournisse les informations de son cache. Or, si des attaquants d'immiscent dans une des étapes du processus, ils peuvent répondre à la requête en renvoyant une adresse IP frauduleuse. Ils peuvent ainsi tromper le navigateur et l'orienter vers le site d'un serveur différent. Typiquement, ce site pourrait, par exemple, héberger la réplique d'un site réel qui servirait aux pirates à dérober des informations de connexion d'un utilisateur.

Détecter le routeur pour adapter l'attaque

Un chercheur en sécurité indépendant, connu en ligne sous le nom de Kafeine, a récemment observé des attaques dites « drive-by » lancées à partir de sites web compromis qui redirigeaient les utilisateurs vers un kit d'exploits inhabituel basé sur le web, spécifiquement conçu pour compromettre les routeurs. En général, les kits d'exploits vendus sur les forums illégaux et utilisés par les cybercriminels cherchent à exploiter des vulnérabilités dans les plug-ins pour navigateurs comme Flash Player, Java, Adobe Reader ou Silverlight. Leur but est d'installer des logiciels malveillants sur les ordinateurs qui n'auraient pas téléchargé les dernières versions de ces modules populaires. Le plus souvent la stratégie de ces attaques consiste à injecter un code malveillant dans des sites compromis ou de l'inclure dans des publicités malveillantes, code qui redirige automatiquement les navigateurs vers un serveur d'attaque chargé de déterminer l'OS, l'adresse IP, la localisation géographique, le type de navigateur utilisé, les plug-ins installés et d'autres détails techniques. En fonction de ces informations, le serveur d'attaque sélectionne dans son arsenal d'exploits ceux qui ont le plus de change de réussir.
Mais, les attaques observées par Kafeine fonctionnent différemment : cette fois, les utilisateurs de Google Chrome ont bien été redirigés vers un serveur malveillant, mais celui-ci a chargé un code destiné à déterminer le modèle de routeur utilisé afin de remplacer les serveurs DNS configurés sur l'appareil. « Beaucoup d'utilisateurs pensent que si leurs routeurs ne sont pas configurés pour la gestion à distance, les pirates ne peuvent pas exploiter les vulnérabilités de leurs interfaces d'administration web à partir d'Internet, parce que ces interfaces ne sont accessibles qu'à partir des réseaux locaux. Mais, cela est faux », a déclaré le chercheur. De telles attaques sont possibles grâce à une technique appelée Cross-Site Request Forgery (CSRF), laquelle permet à un site web malveillant de forcer le navigateur à exécuter des actions malveillantes sur un site Internet différent. Et le site cible peut justement être l'interface d'administration d'un routeur uniquement accessible via le réseau local. De nombreux sites web ont mis en place des défenses pour se protéger contre ces attaques CSRF, mais les routeurs ne bénéficient généralement pas de ce type de protection.

Les principaux routeurs vulnérables

Le nouveau kit d'exploits drive-by identifié par Kafeine a utilisé la technique du Cross-Site Request Forgery pour détecter plus de 40 modèles de routeur de divers fournisseurs dont Asustek Computer, Belkin, D-Link, Edimax Technology, Linksys, Medialink, Microsoft, Netgear, Shenzhen Tenda Technology, TP-Link Technologies, Netis Systems, Trendnet, ZyXEL Communications et HooToo. Selon le modèle, l'outil essaie de changer les paramètres DNS du routeur en exploitant des vulnérabilités connues par injection de commande ou en utilisant des identifiants d'administration courants. Dans ce cas aussi, il utilise la technique CSRF. Et en cas de succès de l'attaque, le serveur DNS primaire du routeur passe sous contrôle des attaquants et le serveur secondaire, utilisé comme relais en cas de panne, est paramétré en tant que serveur DNS public de Google. De sorte que, si le serveur malveillant est temporairement hors service, le routeur disposera toujours d'un serveur DNS parfaitement fonctionnel pour résoudre les requêtes, et le propriétaire ne pourra pas soupçonner une défaillance, ni être tenté de reconfigurer l'appareil.

Selon Kafeine, l'une des vulnérabilités exploitées par l'attaque affecte les routeurs de divers fournisseurs, et a été rendue publique en février. « Certains fournisseurs ont effectué des mises à jour de firmware sur leurs routeurs, mais le nombre de matériels mis à jour au cours des derniers mois reste probablement très faible », a déclaré le chercheur. Car la plupart des routeurs doivent être mis à jour manuellement et l'opération exige certaines compétences techniques. Voilà pourquoi un grand nombre de routeurs ne sont pas mis à jour. Et les attaquants le savent. En fait, d'autres vulnérabilités sont ciblées par ce kit d'exploits, dont l'une a été identifiée en 2008 et l'autre en 2013.

1 million de tentatives le 9 mai

Toujours selon le chercheur indépendant, il semble que l'attaque a été menée à grande échelle : au cours de la première semaine du mois de mai, le serveur d'attaque a comptabilisé environ 250 000 visites uniques par jour, avec un pic de près de 1 million de visites le 9 mai. Les pays les plus touchés étaient les États-Unis, la Russie, l'Australie, le Brésil et l'Inde, mais la répartition du trafic a été plus ou moins globale. Pour se protéger, les utilisateurs doivent vérifier régulièrement si de nouvelles mises à jour de firmware pour leurs routeurs sont disponibles sur les sites Web des fabricants et ils doivent les installer, surtout si ces mises à jour concernent des correctifs de sécurité. Si le routeur le permet, les utilisateurs devraient également limiter l'accès à l'interface d'administration à une adresse IP à laquelle aucun terminal n'a normalement accès, mais qu'ils peuvent affecter manuellement à leur ordinateur en cas de besoin de façon à pouvoir modifier les paramètres de leur routeur.

Source : http://www.lemondeinformatique.fr/actualites/lire-une-attaque-a-grande-echelle-utilise-les-browsers-pour-detourner-les-routeurs-61265.html
Par Jean Elyan

Alerte : Des millions de routeurs domestiques peuvent être attaqués à distance | Le Net Expert Informatique

Une faille dans le driver NetUSB permet à un pirate de prendre le contrôle total de l'équipement et d'y installer, par exemple, des malwares. Pour l'instant, seul TP-Link a fourni un correctif.

Netgear, TP-Link, Trendnet, Zyxel… Si vous possédez un routeur domestique de l'une de ces marques, il est probable que vous ayez un problème de sécurité. La plupart de ces routeurs disposent en effet d'une fonctionnalité théoriquement assez pratique, à savoir le partage en réseau d'une connexion USB. Concrètement, vous connectez un équipement en USB sur votre routeur – un disque dur par exemple – et celui-ci devient alors accessible à distance au travers du réseau. Beaucoup de ces routeurs s'appuient pour cela sur un module logiciel nommé « NetUSB », développé par le fournisseur taiwanais KCodes.
Le problème, c'est qu'il existe dans ce module une faille qui permet à une personne mal intentionnée de faire crasher le routeur ou d'y exécuter n'importe quel code. Et donc d'en prendre possession pour, par exemple, y installer des malwares. Cette vulnérabilité a été découverte par les chercheurs en sécurité de la société autrichienne SEC Consult. Elle repose sur une erreur de codage : quand le nom de l'ordinateur qui souhaite se connecter à distance est supérieur à 64 caractères, le module NetUSB génère un dépassement de mémoire tampon et le fait planter. Pire : comme ce module est exécuté au niveau du noyau Linux du routeur, cette faille permet d'accéder au plus haut niveau de privilège. Plutôt pratique pour un pirate.

Exemple de routeur vulnérable.

Attaque par Internet
Certains d'entre vous se diront que ce n'est pas si grave que cela, car il faut déjà pouvoir rentrer dans le réseau domestique pour réaliser cette attaque. Mais cela n'est pas toujours vrai. Les chercheurs de SEC Consult ont trouvé que pour un certain nombre de routeurs, les connexions NetUSB étaient accessibles par Internet, peut-être en raison d'une mauvaise configuration. Par ailleurs, il s'avère que la procédure d'authentification utilisée pour initier une connexion avec NetUSB est totalement inutile : « les clés AES sont statiques et peuvent être trouvées dans le driver », expliquent les chercheurs. En d'autres termes, lorsque le routeur expose sa fonctionnalité NetUSB sur le web, un pirate pourra s'y introduire sans problème.
Une rapide recherche a montré qu'au moins 26 fabricants de routeurs utilisent le logiciel de KCodes dans au moins 92 produits. Ce qui représente certainement plusieurs millions de clients dans le monde. Contacté par les SEC Consult, KCodes n'a fait aucun commentaire. Que faut-il faire pour se protéger ? Seul TP-Link a développé, à ce jour, un correctif qu'il diffusera progressivement dans ses différents modèles. Dans certains équipements, il est possible, par ailleurs, de désactiver le partage de connexion USB. Les clients de Netgear, en revanche, ne pourront rien faire. Le fabricant a indiqué d'emblée ne pas pouvoir produire de patch, et qu'il était impossible de désactiver la fonction de partage. Il ne reste alors qu'une seule solution : la prière.

Source : http://www.01net.com/editorial/655187/des-millions-de-routeurs-domestiques-peuvent-etre-attaques-a-distance/

Hycopter : Le Supercopter des drones ? | Le Net Expert Informatique

	Hycopter : Le Supercopter des drones ?

Actuellement, les meilleurs drones multirotor ont une autonomie qui ne dépasse pas la demi-heure. Si cela n'est pas vraiment gênant pour les modèles grand public destinés aux loisirs, cette limite est un vrai handicap pour les applications professionnelles. Les opérateurs qui filment avec des drones doivent passer plus de temps sur le terrain pour accomplir leur mission et investir dans des jeux de batteries pour pouvoir décoller à nouveau sans délai.
Augmenter l'autonomie de ces engins est un casse-tête car la puissance des batteries est corrélée à leur taille et à leur poids. Mais Horizon Energy Systems (HES), une entreprise basée à Singapour spécialisée dans les piles à combustible et les systèmes d'alimentation hybrides, pense avoir trouvé la solution.

Elle a développé un drone quadricoptère nommé Hycopter qui pourrait voler jusqu'à quatre heures d'affilée grâce à une pile à combustible. L'originalité du concept est qu'HES est parvenu à intégrer sa technologie dans le châssis du drone. « Nous nous sommes rendu compte que la structure de ces drones était creuse et avons pu utiliser cet espace vide en le remplissant avec un gaz d'hydrogène », explique un des ingénieurs en charge du projet. Ainsi, le châssis tubulaire de l'Hycopter est rempli avec 120 grammes de gaz hydrogène pressurisé à 350 bars. Le gaz est transformé en électricité via une pile à combustible hybride lithium polymère. Le drone complet pèse 5 kilogrammes. Il peut emporter une charge supplémentaire d'un kilogramme, mais alors son autonomie passerait de quatre à un peu moins de deux heures.
Horizon Energy Systems a eu l'idée d'exploiter la structure du drone pour y intégrer son système d'alimentation. Ainsi, les deux parties tubulaires centrales du châssis sont remplies d'un gaz d'hydrogène pressurisé qui est converti en électricité par la pile à combustible lithium polymère (Ultra-light HES Fuel Cell, sur le schéma). Le drone peut emporter une charge d'un kilogramme qui peut être déplacée le long du châssis pour répartir le poids (Flexible positioning of payload). © Horizon Energy Systems

Le premier vol d'essai prévu cette année
Sur la maquette de démonstration présentée à la presse, les tubes du châssis destinés au stockage du gaz d'hydrogène sont en acrylique transparent mais, sur le prototype fonctionnel, ils seront en carbone de 5 millimètres d'épaisseur. Horizon Energy Systems dit être en train de finaliser la conception de son appareil et compte mener les premiers vols d'essai dans le courant de l'année. La viabilité du concept n'est donc pas encore démontrée. Mais l'entreprise, visiblement sûr d'elle, accepte les précommandes, sans toutefois communiquer sur le prix de l'Hycopter. L'engin est destiné à un usage professionnel : cartographie à grande échelle, surveillance des frontières ou d'infrastructures critiques, inspections de bâtiments…
L'autre application citée par HES concerne les futurs drones livreurs qui, grâce à une telle autonomie, pourraient bénéficier d'un rayon d'action beaucoup plus important. Une innovation qui pourrait bien intéresser Amazon, qui compte se servir de drones pour livrer certaines commandes peu volumineuses. Le géant du e-commerce a récemment obtenu un brevet pour un système de guidage grâce auquel le drone pourrait livrer le client là où il se trouve en temps réel, en le suivant grâce à son smartphone.


Ce drone quadricoptère nommé Hycopter est alimenté par une pile à combustible qui lui confère une autonomie de vol théorique de quatre heures. Le prototype est en cours de développement. Un premier vol d'essai est prévu cette année. © Horizon Energy Systems

---

Source :
http://www.futura-sciences.com/magazines/high-tech/infos/actu/d/drone-hycopter-drone-hydrogene-devrait-battre-record-autonomie-58320/
Par Marc Zaffagni, Futura-Sciences

Denis JACOPINI questionné par un journaliste de l’Express | Le Net Expert Informatique

	Denis JACOPINI questionné par un journaliste de l’Express

Le site d'actualité de jeux vidéo Nintendojo.fr a faussement annoncé mercredi 1er avril avoir été bloqué par le ministère de l'Intérieur. Une blague douteuse qui, par l'absurde, révèle néanmoins certains écueils de la loi Cazeneuve. Explications.

Voici l'écran qui s'affiche ce mercredi lorsque l'on tente de se connecter au site Nintendojo.fr

Ministère de l'Intérieur

Enfin, les détracteurs de la loi Cazeneuve tiennent leur martyr! Jugez donc: Nintendojo.fr, un simple site consacré à l'actualité des jeux Nintendo, est inaccessible ce mercredi. Il renvoie vers une page du ministère de l'Intérieur qui explique que le contenu a été bloqué. Une mesure qui est autorisée depuis le vote de la loi Cazeneuve fin 2014, avec de premiers cas en mars dernier, mais en principe réservée aux sites terroristes ou pédophiles.

Rassurez-vous tout de suite. « Il s'agit d'une blague de mauvais goût et ça nous a bien fait rigoler », explique à L'Express Mortal, l'administrateur du site. Il ne faut donc pas voir la main du ministère de l'Intérieur derrière ce faux blocage, mais un poisson d'avril qui aura trompé des dizaines d'internautes et quelques sites d'information.

Pourquoi ce gag?

« Ce n'est pas un geste politique, mais nous estimons quand même que la loi qui permet le blocage de certains sites internet est mauvaise, justifie Mortal, qui se revendique de la Quadrature du Net, association de défense des libertés sur internet hostile au dispositif. On avait envie de piquer les gens pour que ça éveille un peu les consciences sur le sujet. Cela pourrait arriver pour de vrai à d'autres demain, c'est ça le problème », tranche-t-il.

De la difficulté de distinguer « vrai » et « faux » blocage

Qu'on le juge drôle ou pas, le poisson d'avril de Nintendojo.fr pose de sérieuses questions sur le principe même de bloquer certains sites Internet. Est-il possible pour un internaute face à une page qui affiche le fameux message du ministère de l'Intérieur de savoir avec certitude que le site a été bloqué? « La réponse est simple: c'est non », estime **Denis Jacopini**, consultant en cybersécurité. Point de vue partagé par plusieurs observateurs interrogés ce mercredi.

« **Rien est impossible, poursuit l'analyste. Cela peut être un vrai message, bien sûr. Mais cela peut aussi être une blague de l'administrateur du site, ou l'oeuvre d'un hacker qui a modifié le site**« , avance-t-il.

Qu'en pense l'Intérieur? Contactés par L'Express, les services du ministère n'ont pas donné suite à nos sollicitations. A ce jour, les services de la Place Beauvau n'ont pas mis en place de dispositif pour informer sur de telles situations. Il ne serait pas étonnant, dans ce contexte, de voir fleurir les farces voire de réelles arnaques du même tonneau dans les semaines qui viennent.

Attention, arnaques à prévoir…

Dans le cas de Nintendojo.fr, l'artifice était plutôt élaboré. Le message affiché sur la page d'accueil du site reprenait, aussi bien graphiquement qu'au niveau du contenu, celui affiché en cas de blocage. Ce n'est pas tout. Un utilisateur de Twitter a comparé le code HTML de la page vers laquelle redirigeait Nintendojo.fr avec celui d'une page affichée via un site réellement bloqué par l'Intérieur, et ils étaient bien identiques.

Mais Nintendojo.fr est allé encore plus loin. « Nous avons vraiment procédé à un blocage DNS » (domain name system, nom de domaine) explique Mortal. Ce qui a pu donner l'illusion a certains que le site avait bel et bien été « bloqué ». « Techniquement, le dispositif de censure fait appel à un résolveur DNS menteur, c'est-à-dire qu'il ne renvoie pas le résultat correct, mais un mensonge tel que demandé par le gouvernement », explique nextinpact.com.

Concrètement, le gouvernement n'efface pas les sites bloqués: l'internaute qui essaye de s'y connecter est simplement redirigé vers la fameuse page ministérielle. Un mécanisme que Nintendojo.fr a plutôt bien singé ce mercredi.

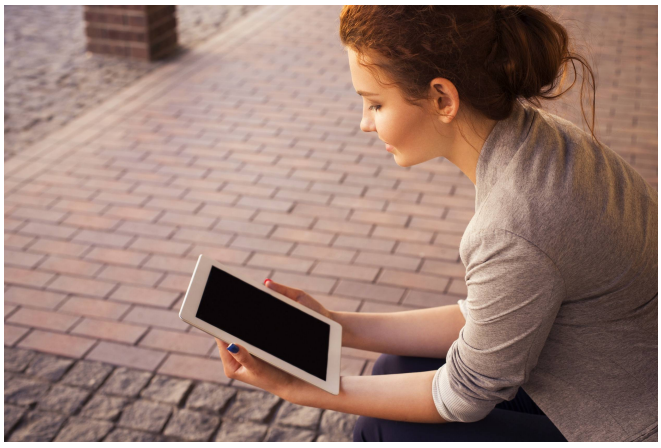
« On aurait pu faire encore plus sophistiqué »

Les bons connaisseurs, eux, ont néanmoins pu déjouer la supercherie en testant d'autres DNS. Ils ont alors observé que tous renvoyaient vers la page du ministère de l'Intérieur, ce qui n'aurait pas été le cas pour un « vrai » blocage gouvernemental. En situation réelle, les fournisseurs d'accès à Internet (FAI) bloquent le site concerné au fur et à mesure, ce qui prend du temps. De plus, il existe des DNS publics, gérés par d'autres acteurs du Web (par exemple, Google), qui peuvent ne pas faire l'objet de blocage. Changer de résolveur DNS est d'ailleurs précisément l'une des solutions pour ceux qui souhaitent contourner la censure.

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

Source : http://lexpansion.lexpress.fr/high-tech/les-vraies-questions-que-pose-le-faux-blocage-de-nintendojo-par-le-gouvernement_1667195.html

Mouchards sur les ebooks : Big brother is reading you ! | Le Net Expert Informatique

	Mouchards sur les ebooks : Big brother is reading you !

Grâce aux « mouchards numériques », il est désormais possible de savoir si un livre a été lu jusqu'au bout. Amazon, Apple, Google et Kobo en savent beaucoup plus sur vos habitudes de lecture que vous ne le pensiez…

Eric Zemmour a vendu plus de 400 000 exemplaires de son essai « Le suicide français ». Mais seulement 7,3 % des lecteurs l'ont lu jusqu'à la fin ! L'économiste Thomas Piketty fait un peu mieux : 9,7 % des lecteurs ont terminé son pavé de près de 1 000 pages (Le capital au XXI ème siècle). Encore mieux, le dernier roman de Patrick Modiano, Prix Nobel 2014 (Pour que tu ne te perdes pas dans le quartier) affiche un honorable taux de 44 %. Quant à Valérie Trierweiller (Merci pour ce moment), son score d'achèvement est, de loin, le meilleur : environ 66 % des lecteurs sont allés au terme des mésaventures sentimentales de l'ex compagne de François Hollande.
Comment connaît-on ces taux de lecture avec une telle précision ? Tout simplement grâce aux « mouchards » numériques installés sur nos liseuses et nos tablettes. Ces instruments dédiés à la traçabilité permettent en effet de collecter une série de données sur le comportement des e-lecteurs : nombre de pages lues, vitesse de lecture, temps passé sur une page, heures de lecture, surlignage…
Ces chiffres proviennent des statistiques collectées par Kobo (partenaire de la Fnac) l'un des leaders de la lecture numérique dans le monde. Autant dire qu'ils ne sont pas passés inaperçus, notamment auprès des lecteurs les plus attentifs aux questions de confidentialité des données. Mais il faut reconnaître à Kobo une qualité : il dit ce qu'il fait. L'un de ses responsables, Nathan Maharaj, a publiquement présenté ce dispositif de mesure de « l'engagement du lecteur » lors du salon du Livre de Francfort qui s'est tenu au mois d'octobre dernier. Selon Kobo, ces données ne seraient exploitées qu'à des fins statistiques ; surtout, elles seraient anonymisées et non rattachées à un compte lecteur. En revanche, elles sont revendues aux éditeurs qui peuvent ainsi accéder à des données inédites sur le comportement réel des lecteurs.
Lire la suite….

Source : http://www.archimag.com/bibliotheque-edition/2015/05/22/mouchards-ebooks-big-brother-reading-you

L’impression 3D de la peau humaine est presque une réalité | Le Net Expert Informatique

	L’impression 3D de la peau humaine est presque une réalité

L'Oréal, géant de la cosmétique, s'associe avec Organovo, une entreprise de bio-impression 3D cotée en bourse. Cette nouvelle technologie allie l'impression 3D et des tissus vivants dans le but d'imprimer de la peau humaine.
Dans son annonce de ce projet de collaboration, L'Oréal a utilisé un terme propre à la Silicon Valley en le présentant comme une technologie dite "de rupture". Aujourd'hui, toutes les grandes sociétés sont des incubateurs d'entreprises technologiques.

(Source)
Guive Balooch, directeur de l'Incubateur de la beauté connectée à L'Oréal, a déclaré : "Nous avons développé notre incubateur de technologie pour dévoiler des innovations de rupture à travers les industries ayant le potentiel de transformer le marché de la beauté". L'Oréal ajoute :
Notre partenariat ne va pas seulement créer de nouvelles méthodes de pointe in vitro pour évaluer la sécurité et la performance du produit. Le potentiel de ce nouveau secteur de technologie et de recherche est sans limites.

Des "tissus humains vivants" au service de la beauté
Comme l'a souligné L'Oréal, les méthodes de bio-impression 3D d'Organovo permettent l'automatisation et la reproductibilité de la "création" de "tissus humains vivants" qui pourraient "imiter la forme et la fonction des tissus originels du corps."

Dans la vidéo ci-dessous, Organovo explique (en anglais) comment cette peau est produite :

Keith Murphy, le PDG d'Organovo, décrit "ce partenariat [comme] une nouvelle étape considérable pour l'extension des fonctions des technologies de ."
En parlant de "modélisation de la peau", L'Oréal tente de créer un nouveau marché. L'avenir nous dira si cette technologie s'appliquera au niveau de la chirurgie réparatrice, et éventuellement soigner les grands brûlés.

Une innovation pour la santé et la recherche
Bien que L'Oréal investisse dans cette nouvelle technologie, son utilisation première est pharmaceutique. Dans un article paru dans Le Monde, Fabien Guillemot, chercheur à l'Inserm, énumère les usages possibles de ces tissus humains créés par bio-impression : "Ce procédé permet de reproduire la physiologie de tissus humains afin de tester de manière plus prédictive des molécules, ingrédients et candidats médicaments." De quoi réduire considérablement l'expérimentation animale.
Ainsi, la bio-impression pourrait également permettre le développement de la médecine individualisée, de produire des greffons et d'en finir avec les problèmes de rejet car la peau en question est réalisée à partir des cellules mêmes du patient. La bio-impression permettrait aussi d'accélérer la recherche contre le cancer.

Un marché en expansion
Ces nouvelles technologies représentent des enjeux socio-économiques majeurs qui affolent les investisseurs. Selon une étude du MedMarket Diligence relayée par Le Monde, le marché de l'ingénierie tissulaire était évalué à 15 milliards de dollars en 2014 et devrait doubler d'ici 2018. Ses utilisations multiples et limitations jusqu'à présent indéfinies suscitent de grandes attentes.
En janvier 2014, Organovo avait déjà imprimé un bout de foie produisant de l'albumine et capable de synthétiser le cholestérol. Cependant, l'impression totale d'organes, leur commercialisation et leur utilisation n'est pas prête de devenir monnaie courante dans les hôpitaux. De plus, la création et la commercialisation de tissus humains reste un marché éthiquement discutable.

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

Source : http://www.konbini.com/fr/tendances-2/impression-3d-peau-humaine/
Article co-écrit et traduit par Marie Fabre