Trois tendances de sécurité informatique à retenir pour 2015 | Le Net Expert Informatique

De nombreuses études placent la sécurité au cœur des TI pour 2015. Retrouvez ci-dessous trois tendances à retenir pour cette année :

Les attaques seront inévitables!
La question n'est plus de se demander si on sera attaqué et quand, mais plutôt de se préparer aux impacts d'une attaque, car cette attaque arrivera de toute façon.
Il faut donc avant tout s'assurer de minimiser les impacts d'une attaque potentielle et être proactif. Pour faire face à ces nombreuses tentatives d'attaques, les organisations doivent mettre en place un SOC (pour Security Operations Manager en anglais) ou du moins constituer des ressources qui vont gérer les opérations de sécurité quotidiennement et en temps réel.
Ces ressources vont être aidées dans leur travail par des outils innovateurs, mais doivent s'appuyer sur une expertise poussée pour analyser la masse d'activités. Par exemple, il ne suffit pas d'avoir un SIEM, mais il faut savoir le gérer.

Impartir sa sécurité
Puisque les attaques sont de plus en plus sophistiquées, l'expertise demandée par les ressources opérationnelles est de plus en plus poussée.
De plus, le temps à consacrer aux activités quotidiennes augmente de manière significative. Il est donc plus logique de faire appel à un fournisseur externe pour assurer ces activités afin que les ressources de l'organisation puissent se consacrer à la portion stratégique de la sécurité.
L'année 2015 verra de plus en plus d'impartition des opérations de sécurité sur la base du mode sécurité à la demande (SaaS).

Priorité à la sécurité applicative
Les réseaux sont de plus en plus protégés, car le cœur de l'infrastructure des organisations est sécurisé grâce aux nombreuses années d'évolution à ce sujet.
Par définition, les attaques ciblent toujours les points faibles d'une organisation et dans bien des cas, les applications Web sont les plus vulnérables : code non sécuritaire, failles non corrigées, mises à jour non appliquées… De nombreuses raisons peuvent s'ajouter à la liste.
Or, les applications Web représentent l'image de l'organisation et constituent bien souvent un accès privilégié aux données sensibles. La protection ciblée des applications Web sera mise de l'avant en 2015.

Source : http://www.directioninformatique.com/blogue/securite-informatique-trois-tendances-2015/36154
Par Matthieu Demoor

iOS 9 impose un code d’accès à 6 chiffres – Le Monde Informatique | Le Net Expert Informatique

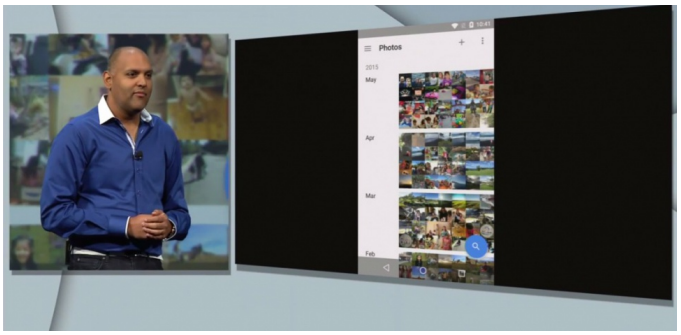
iOS 9 impose un code d’accès à 6 chiffres

Sous iOS 9, le verrouillage des terminaux se fera avec un code à six chiffres. « En passant d'une clef de 4 chiffres à une clef de 6 chiffres, le nombre de combinaisons possibles passe de 10 000 à 1 million », a déclaré Apple.

Il faudra des mots de passe à six chiffres pour déverrouiller les appareils mobiles d'Apple qui tourneront sous le futur système d'exploitation IOS 9. Et si iOS 8 permet déjà aux utilisateurs de choisir un mot de passe de plus de quatre chiffres, dont des symboles et des lettres, ce mode de codage reste optionnel, ce qui ne sera pas le cas du futur iOS. En exigeant un code d'accès à six chiffres, Apple multiplie par 100 le nombre de combinaisons possibles, « rendant ainsi les terminaux beaucoup plus difficiles à pirater », comme on peut le lire sur le site du constructeur.
Ce saut à un code d'accès plus long risque de ne pas plaire non plus aux autorités américaines qui craignent que le renforcement des mesures de sécurité et du cryptage complique leurs investigations et rende plus difficile l'accès à des informations sensibles où le facteur temps est important, notamment dans le cadre de la lutte antiterroriste. Apple avait déjà renforcé le chiffrement d'iOS 8 afin de protéger les données les plus sensibles, et la firme de Cupertino avait mis en œuvre davantage de protections matérielles pour rendre l'accès aux terminaux plus difficile. Mais les experts en sécurité avaient estimé que l'utilisation d'un mot de passe à quatre chiffres ne suffisait probablement pas à protéger les données malgré les remparts mis en place par Apple. D'autant que, même si les utilisateurs savent qu'ils sont mieux protégés par des mots de passe plus longs, notamment parce que les séquences peuvent être plus personnalisées, ils choisissent rarement les mots de passe les plus compliqués.
Le changement de mots de passe concernera les terminaux équipés de l'ID Touch, le système d'empreintes digitales intégré aux dernières versions d'iPhone et d'iPad. L'ID Touch permet de se passer du déblocage, parfois fastidieux, du mobile avec le code à quatre chiffres, mais Apple oblige l'utilisateur à déverrouiller le mobile avec son code en cas de redémarrage du terminal. Les appareils iOS offrent d'autres fonctions de protection. Par exemple, si l'utilisateur tape un mauvais code de déverrouillage, l'iPhone peut être bloqué pendant une minute et plus, si plusieurs mots de passe sont saisis à la suite. Il est également possible de programmer l'effacement complet des données après 10 tentatives infructueuses. Le passage à un code à six chiffres pourrait grandement compliquer le travail des enquêtes judiciaires, surtout si l'appareil sous iOS 9 est configuré pour effacer les données après plusieurs tentatives erronées.

Source :
http://www.lemondeinformatique.fr/actualites/lire-ios-9-impose-un-code-d-acces-a-6-chiffres-61419.html
Par Jean Elyan

Et maintenant Google veut vos photos. Toutes vos photos… | Le Net Expert Informatique



Ani Sabharwal, responsable de l'application Photos chez Google, lors de sa présentation au Google I/O le 29 mai 2015. Google

Et maintenant Google veut vos photos. Toutes vos photos…

Après les courriers électroniques, Google veut héberger toutes les photos des internautes. Et bien sûr, analyser leur contenu.

A peine quelques jours avant Apple, c'est Google qui a organisé sa grand-messe annuelle à l'attention des développeurs. L'occasion de se faire une idée des prochains développements sur lesquels mise le géant américain. Parmi eux, une application qui a de bonnes chances de faire mouche auprès du grand public : Google Photos. A première vue, rien de révolutionnaire, car il s'agit d'une application de stockage et de partage de ses photos. Mais avec le petit détail dont Google s'est fait une spécialité : le stockage illimité et gratuit. Et la taille du stockage, c'est ce qui avait assuré par le passé le succès de Gmail face aux messageries déjà implantées.

Un stockage gratuit et illimité

Pour la première fois, le grand public a donc une solution gratuite de sauvegarde de l'ensemble de ses photos et même de ses vidéos. Avec une limitation technique qui ne devrait pas poser de problème aux non-professionnels : la qualité des photos est limitée à 16 mégapixels et celle des vidéos à 1080p (limitation dont on peut se défaire pour 10 dollars par mois et par teraoctet de données). L'interface est soignée, très épurée, dans la droite ligne des produits maison. On peut classer les photos, les retoucher, faire des montages. Google a aussi mis à disposition de chacun ses algorithmes de fouille d'image. Ainsi, toutes les photos sont analysées et l'application y reconnaît toute seule les visages ou des éléments comme par exemple de la nourriture. On peut théoriquement ainsi retrouver des photos en tapant des mots-clés dans le moteur de recherche sans jamais avoir « taggé » ses photos. Démonstration sur scène avec une recherche instantanée des photos après avoir dicté « tempête de neige à Toronto ». La recherche combine sans doute les éléments de neige sur l'image avec la géolocalisation de la ville.

La mort de Google+

Cette nouvelle application marque le premier signe du repositionnement de Google sur les réseaux sociaux. En effet, elle découle du début de démantèlement de Google+, qui n'a jamais su s'imposer face à Facebook. En séparant la partie photos de son réseau social, Google va essayer de reprendre du terrain sur les images. D'autant que l'application n'existe pas que sur le web ou les appareils Android : elle est aussi disponible sur iOS (le système d'exploitation d'Apple), ce qui en fait un grand concurrent du stockage des photos sur le cloud d'Apple, qui lui est facturé au prix fort : de 0,99 € par mois pour 20 Go à 19,99 € pour 1 To. Avec ce nouveau service, Google semble bien armé pour réussir ce qu'il a fait avec Gmail : garder l'internaute dans son propre univers en hébergeant ses données personnelles, afin de pouvoir par la suite se rémunérer avec la publicité. En sachant en plus cette fois tout ce qu'il y a dans ses photos et où et quand elles ont été prises.

La conférence est à revoir en intégralité ici :

Source : http://www.sciencesetavenir.fr/high-tech/20150529.OBS9810/et-maintenant-google-veut-vos-photos-toutes-vos-photos.html?cm_mmc=EMV-_-SEA-_-20150531_NLSEAACTU-_-et-maintenant-google-veut-vos-photos-toutes-vos-photos##xtor=EPR-6-ActuSciences17h-20150531

L'analyse comportementale, la

nouvelle cyber-arme ? | Le Net Expert Informatique

IdentityGRC 2015 est la dernière offre de détection comportementale de la fraude et de la fuite de données de Brainwave, co-fondée par Sébastien Faivre. (crédit : D.R.)

L’analyse comportementale, la nouvelle cyber-arme ?

C’est bien connu, en matière de sécurité les risques ne proviennent pas seulement de l’extérieur du périmètre de l’entreprise mais bien de l’intérieur. Téléchargement de fichiers non autorisés, vol de données confidentielles ou encore accès à des informations par un collaborateur ayant quitté depuis des mois l’entreprise sont, malheureusement, une réalité qui dépasse – parfois – de loin la fiction. Et bien souvent, à la base de cette problématique, on trouve une gestion et/ou une politique de gestion des droits d’accès défaillante ou en tout cas plus en mesure de répondre à une évolution malsaine des comportements.
« Le constat que l’on fait aujourd’hui est que d’une façon générale la sécurité des accès et la configuration des droits d’accès pour accéder à des applications ou données sont souvent les parents pauvres de la sécurité informatique », explique Sébastien Faivre, co-fondateur de Brainwave. « En général, le département informatique et les métiers se renvoient la balle en termes de responsabilités dans les cas où on se rend compte que des personnes qui ont quitté l’entreprise ou changé de département ont toujours accès à des informations sensibles ou que d’autres encore ont des droits d’accès excessifs à des données critiques ».

Des jeux d’API couplés à des algorithmes d’analyse
Pour faire face à ce type de menace, le jeune éditeur francilien Brainwave (créé en 2010) a développé IdentityGRC qui permet de récupérer toutes les informations de configurations de l’ensemble des systèmes de l’entreprise afin de proposer une cartographie de l’ensemble des droits d’accès aux applications. Et ce, des systèmes CRM, ERP, gestion financière (SAP, Salesforce.com, Microsoft Dynamics CRM…) que des solutions cloud de sauvegarde et de partages documentaires (Google Drive, Dropbox…) ou encore des grands systèmes (AS400, RACF, CA Top Secret…). Pour y parvenir, plusieurs jeux d’API ont été développés, couplés à des algorithmes d’analyse, brevetés depuis fin 2010, afin de pouvoir poser des questions en langage naturel de type « Quelles sont les personnes ne faisant pas partie des ressources humaines qui ont accès aux fiches de paye des salariés ? ».
Aujourd’hui, Brainwave va plus loin en matière de détection mais surtout de prévention de la fraude et de fuite des données. « La version 2015 d’IdentityGRC propose de l’analyse comportementale permettant de mettre sous surveillance des comportements anormaux comme par exemple identifier une personne qui récupère bien plus de fichiers que ses collègues, mais également d’automatiser le diagnostic et la résolution des comportements suspects », fait savoir Sébastien Faivre. Une approche différente selon Brainwave des traditionnelles offres de sécurité centrées davantage sur les flux de comportements au niveau des postes de travail que sur le comportement du point de vue des applications, indépendamment du reste de tout terminal.

A partir de 75 000 euros la licence perpétuelle
Distingué par le Gartner dans la catégorie des « cool vendors » dans son rapport Magic Quadrant 2013 en Identity Analytics and Intelligence, Brainwave n’a pas attendu pareille reconnaissance pour se tailler une place dans les entreprises. Surtout les grandes, avec des clients comme PSA Peugeot-Citroën, Natixis, Crédit Agricole, BNP Paribas, ou encore Aéroports de Paris et Eutelsat qui utilisent ses solutions. En tout, l’éditeur revendique une cinquantaine de références en France mais également au Bénélux, en Suisse, au Royaume-Uni, au Magrehb ou encore au Canada où il a ouvert récemment un bureau commercial. Autofinancée jusqu’en 2014, la société a levé 2,5 millions d’euros fin 2014 afin de donner un nouvel élan à sa croissance internationale mais également renforcer ses équipes R&D (une dizaine de personnes sur 30 collaborateurs au total). Brainwave a réalisé l’année dernière un chiffre d’affaires de 2 millions d’euros et indique être rentable.
IdentityGRC 2015 est proposée à partir de 75 000 euros en licence perpétuelle, auquel vient s’ajouter près de 20 000 euros de maintenance annuelle. Deux modes de tarification sont proposées : nombre de personnes sur lequel un audit sécurité est réalisé ou bien en fonction du nombre d’applications. Quant à la disponibilité de l’offre, elle est pour le moment uniquement en on-premise. « Nous ne proposons pas d’offre en mode cloud public. Nos clients considèrent que ce type de données est sensible et préfèrent donc un déploiement sur site. Cependant, certains clients ont choisi un déploiement dans un cloud privé chez un infogéreur », explique Sébastien Faivre.

Source : http://www.lemondeinformatique.fr/actualites/lire-avec-identitygrc-2015-brainwave-s-ouvre-a-l-analyse-comportementale-61157.html
Par Dominique Filippone

Les cyber-attaques changent de forme…| Le Net Expert Informatique

	Les cyber-attaques changent de forme…

Akamai constate une évolution du profil des attaques informatiques par déni de service distribué (DDoS), mais aussi des assauts contre les services Web.

Le profil des attaques informatiques par déni de service distribué (DDoS, visant à rendre des ressources indisponibles en les saturant de requêtes) a fortement évolué en un an, tandis que de nouvelles menaces sont nées de l'adoption du protocole IPv6.
Telles sont les principales conclusions émises par Akamai dans la dernière édition de son baromètre Internet Security – document PDF, 93 pages – portant sur le 1er trimestre 2015.
Sur le volet DDoS, le constat est sans appel : les assauts se multiplient (+ 116,5 % d'une année sur l'autre). Les attaques sur la couche applicative (Layer 7) augmentent de 60 %, mais ne représentent encore qu'un cas sur dix.
Le reste des offensives se concentre sur l'infrastructure (Layers 3 & 4 ; + 125 %), qui permet de maximiser plus facilement la puissance des attaques tout en nécessitant moins de ressources.
Alors qu'un DDoS s'échelonnait en moyenne sur 17 heures au 1er trimestre 2014, la durée a avoisiné les 25 heures un an plus tard (+ 43 %). Des attaques plus longues, donc, mais aussi moins virulentes : 5,95 Gbit/s de bande passante moyenne, contre 9,7 Gbit/s un an plus tôt ; quant au nombre moyen de paquets envoyés par seconde, il baisse de 89 % (2,21 millions).
Akamai a tout de même relevé 8 attaques d'un volume supérieur à 100 Gbit/s.
Encore quasiment inexploité début 2014, le SSDP (« Simple Service Discovery Protocol ») est devenu, en l'espace d'un an, le principal facteur déclencheur des attaques DDoS (plus d'un cas sur cinq). Implémenté et activé par défaut sur des millions d'équipements (routeurs, webcams, imprimantes, TV connectées) pour leur permettre d'interagir sur un réseau local, ce protocole est souvent mal – ou pas du tout – sécurisé.
L'industrie du jeu vidéo concentre à elle seule 35 % des dénis de services répertoriés entre le 1er janvier et le 31 mars. Suivent le secteur IT (25 %), les télécoms (14 %), la finance (8,4 %), les médias (7,5 %), l'éducation (5 %), la distribution (2,3 %) et le secteur public (2 %).
Pour la première fois, Akamai inclut dans son baromètre les attaques contre les applications Web. Les analyses réalisées sur environ 180 millions d'échantillons ont permis de dégager 7 vecteurs de piratage.
Dans les deux tiers des cas, les cybercriminels ont exploité une faille de type LFI (« Local File Inclusion ») leur permettant d'accéder, en lecture, à des fichiers hébergés sur un serveur Web. On notera cette campagne massive venue d'Allemagne contre deux grands noms du secteur de la distribution via une vulnérabilité dans le plugin WordPress RevSlider.

SQL, HTTPS et IPv6
29 % des attaques recensées sont liées à des injections SQL* ; c'est-à-dire à l'exploitation d'une brèche dans une application qui interagit avec une base de données en introduisant une requête SQL non prévue par le système. Illustration avec cette campagne issue essentiellement d'Irlande et visant une société de l'industrie du voyage.
Les autres types d'attaques (inclusion de fichiers distants sur des serveurs Web, injection de code PHP, exécution de commandes shell sur le système visé…) n'ont été repérées que dans environ 5 % des cas. Sachant toutefois qu'au global, près de 10 % ont été menées sur des sites « sécurisés » en HTTPS…
Parmi les grandes tendances de l'année, Akamai pointe la menace grandissante des sites dits « booters » ou « stressers » et qui permettent de simuler des attaques DDoS. Alors qu'il y a encore un an, leur ampleur se limitait à 10 ou 20 Gbit/s, ils peuvent désormais lancer des assauts dévastateurs à plus de 100 Gbit/s, en exploitant notamment des techniques de réflexion du trafic.
Autre enjeu à surveiller : l'adoption du protocole IPv6, qui permet d'élargir l'espace d'adressage réseau… mais dont l'architecture est dite « imparfaite » par Akamai : il est possible de passer outre certaines protections implémentées dans IPv4. Il existe d'ailleurs « plusieurs signes » montrant que les cybercriminels mènent bien des recherches sur le sujet.
* Documentées depuis 1998, les attaques par injection SQL vont désormais bien au-delà du simple vol de données. Elles permettent aussi l'élévation de privilèges, l'exécution de commande, la corruption de systèmes…

Source : http://www.itespresso.fr/securite-it-cyber-attaques-changent-forme-97172.html

Impression 3D : vous n’avez encore rien vu ! | Le Net Expert Informatique

	Impression 3D : vous n’avez encore rien vu !

Voitures, maisons, nourriture et même organes… désormais on peut tout imprimer ou presque. Le début d'une vraie révolution qui va bouleverser notre conception des objets.

Allô Houston ? Nous avons un problème.» Quand on part pour l'ISS, la station spatiale internationale, mieux vaut vérifier que l'on n'a rien oublié. Avant Noël, Barry E. Wilmore, le commandant de l'équipage, s'est aperçu une fois dans l'espace qu'il lui manquait une manivelle. Heureusement, grâce à l'imprimante 3D de la station, capable de fonctionner en apesanteur, la Nasa a pu lui envoyer l'objet… par e-mail ! Un simple fichier contenant les cotes de l'outil a permis de l'imprimer en quelques minutes. L'anecdote montre combien l'imprimante 3D a désormais largement dépassé le stade du gadget.
La technologie n'est pourtant plus si jeune, puisqu'elle est née dans les années 1980, mais elle envahit tous les secteurs à la vitesse de la lumière depuis que des modèles à bas coût sont apparus sur le marché en 2009. Avec une imprimante vendue moins de 200 euros, on peut tous fabriquer des petits objets en plastique. Le principe est simple: l'encre y est remplacée par une sorte de filament de plastique en fusion qui permet de modeler un objet en trois dimensions, couche après couche, à partir d'un fichier numérique. L'utilisation principale est la réalisation rapide de prototypes, mais le plus spectaculaire reste à venir.

Les tests lors d'un vol parabolique de l'imprimante 3D de la Nasa capable de fonctionner en apesanteur.

UNE PIZZA EN UNE MINUTE.
En effet, le plastique n'est plus la seule matière utilisée par les nouvelles générations d'imprimantes. Et c'est cet emploi d'autres matériaux qui pourrait bien changer la donne, rendant possibles des choses que l'on pensait jusqu'ici inconcevables. Ainsi, en mai 2013, Anjan Contractor, un ingénieur d'Austin, au Texas, a remporté une dotation de 125.000 dollars allouée par la Nasa pour mettre au point une imprimante capable de créer une pizza à partir de cartouches contenant des ingrédients en poudre, lyophilisés. En soixante-dix secondes, sa machine concocte et cuit une pizza composée de pâte, de fromage et de protéines. Le résultat n'est pas très appétissant mais pourrait révolutionner les futurs repas en apesanteur, en particulier lors de voyages vers Mars.

Foodini, imaginé par les Espagnols de Natural Machines, fait entrer la 3D dans la cuisine

Toujours au-dessus de nos têtes, BAE Systems confirmait l'été dernier le succès du vol test d'un Tornado GR4, un avion de chasse contenant certains éléments imprimés en 3D. Il ne s'agissait certes pas d'équipements critiques, mais du système d'arrivée d'air et d'un couvercle de protection pour la radio du cockpit. Le département aviation de General Electric a, lui, investi 50 millions de dollars pour développer un centre consacré à la fabrication de pièces en métal. Leurs injecteurs de carburant, imprimés d'un seul tenant, sans perte de matière et plus légers, équiperont des Airbus et des Boeing dès l'an prochain.

UNE VRAIE VOITURE ÉLECTRIQUE

Du côté de l'industrie, en effet, l'utilisation de métal au lieu de plastique permet d'obtenir des pièces imprimées (réalisées en ajoutant de la matière, couche après couche) d'une qualité proche de celles des objets usinés (obtenus en retirant de la matière). Des machines fonctionnent déjà avec de l'acier, du titane et du nickel. Et d'autres métaux devraient bientôt pouvoir être ajoutés. C'est ainsi que Bentley a pu présenter au dernier Salon de l'automobile de Genève sa nouvelle EXP 10 Speed 6, dont la structure avait été imprimée ! Ford emploie aussi cette technique pour les éléments de certains prototypes – culasses, freins, essieux… – et compte vite proposer à ses clients d'imprimer eux-mêmes leurs pièces de rechange. Le marché est énorme : pour le seul secteur automobile, le cabinet SmarTech prédit une croissance de 25% par an et 1 milliard de dollars de chiffre d'affaires avant 2019. Enfin, l'américain Local Motors a relevé un autre défi : imprimer, en quarante-quatre heures, un véhicule 100% électrique. La Strati, qui n'a pas encore l'autorisation de circuler, ne contient que 40 éléments, contre 20.000 pour un véhicule classique.

Cet immeuble de 6 étages du chinois Winsun a nécessité une imprimante de 40 mètres de long sur 6,5 mètres de haut.

D'autres applications semblent tout droit sorties d'un film de science-fiction : dix pavillons de 200 mètres carrés bâtis en vingt-quatre heures, un immeuble résidentiel de cinq étages, une villa de 1.100 mètres carrés… Ces constructions, signées par le chinois WinSun, ont surgi de terre grâce à des imprimantes 3D de plusieurs dizaines de mètres de long utilisant des déchets issus du bâtiment pour couler une sorte de béton. Les spécialistes du secteur estiment qu'en 2020, on pourra imprimer à la carte des maisons préfabriquées. Plus proche de nous, United Nude propose déjà à ses clients de fabriquer leur paire de chaussures sur mesure grâce à une imprimante 3D installée dans sa boutique de New York. Et Google s'apprête à lancer le Project Ara, un smartphone en kit dont les différents modules seront imprimés par les usagers, qui pourront ainsi les personnaliser à leur guise.

BIENTÔT DES TISSUS VIVANTS
Dans le domaine de la santé, on savait reproduire des prothèses auditives ou dentaires en plastique. Depuis peu, on réalise aussi des os artificiels, à base de phosphate de calcium ! Une mâchoire, un morceau de crâne ou une prothèse de trachée imprimés ont ainsi été implantés à des patients. Et il y a déjà une dizaine d'années que les chercheurs remplissent les cartouches de ces imprimantes de cellules humaines pour tenter de fabriquer du vivant. La société californienne Organovo a réussi à produire le tout premier tissu organique fonctionnel : un morceau de foie de quelques millimètres. Des échantillons sont déjà commercialisés, à l'intention de la recherche médicale. Mieux que la téléportation : et si on pouvait, un jour, s'imprimer en 3D sur Mars ? Au moins, cela éviterait de devoir manger des pizzas pendant le voyage…

L'IMPRESSION 3D EN CHIFFRES :
• 70% des objets en 3D sont des prototypes destinés à l'industrie.
• 8,5 milliards d'euros, c'est le marché de l'imprimante 3D ne 2020 d'après Xerfi.
• 250 milliards d'euros, c'est le volume d'activité généré par la 3D en 2025 selon McKinsey

---

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

Source : http://www.capital.fr/enquetes/dossiers/impression-3d-vous-n-avez-encore-rien-vu-1043990
Par Charlotte Laurent

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

Android : vos données personnelles impossibles à effacer ? | Le Net Expert Informatique

Des chercheurs ont mis en lumière les problèmes de sécurité du système d'exploitation mobile de Google.
Grâce à un seul petit bouton « Restaurer les paramètres d'usine », Google promet à ses utilisateurs de supprimer tous les contenus de leur smartphone Android. La mémoire du smartphone serait ainsi totalement effacée. Mais à en croire une étude menée par deux chercheurs de l'université de Cambridge, il n'en est rien : cette fonction de suppression serait inefficace sur plus de 500 millions de smartphones Android. Explications.

Quelles données ont été récupérées ?
Les chercheurs ont examiné 21 smartphones de 5 grandes marques et sous différentes versions d'Android : Samsung Galaxy S2 et S3, LG Optimus L7, Nexus 7, HTC Desire C, Motorola Razr I, etc. Cet échantillon représenterait près de 500 millions de smartphones actuellement en circulation. Sur la totalité des smartphones étudiés, les données personnelles ont pu être récupérées après avoir été effacées. Les deux chercheurs ont ainsi pu mettre la main sur les identifiants Google des utilisateurs sur tous les modèles. Puis, ils ont pu accéder aux informations des services Google associés à ces comptes : Gmail, Calendrier, Drive, etc. Enfin, les chercheurs ont pu récupérer des données de communications (SMS, e-mails, appels, etc.) et des fichiers multimédias (photos et vidéos).

Comment c'est possible ?
Comme l'explique le résultat des recherches, lorsqu'un utilisateur appuie sur le bouton pour effacer ses données, le smartphone supprime en réalité l'accès à ces données et non les informations elles-mêmes. « C'est comme pour un ordinateur : un formatage du disque dur ne suffit pas à effacer les données », explique à Europe 1 Jean-François Beuze, expert en sécurité informatique.

Comment être sûr que toutes les données sont effacées ?
« Il faut chiffrer ses données », conseille le spécialiste en sécurité. C'est à dire ajouter une étape de protection supplémentaire à ces informations personnelles. Pour cela, il faut se rendre dans les réglages du smartphone, puis dans le menu Sécurité et enfin cocher la case « chiffrer les données sur le smartphone ». Si une carte mémoire est utilisée pour étendre le stockage de l'appareil, l'utilisateur devra également chiffrer celle-ci. Pour les données les plus sensibles, « il existe des appareils émettant un champ électromagnétique pour effacer toute donnée sur le smartphone », ajoute Jean-François Beuze. Mais ces appareils restent réservés aux professionnels en raison de leur coût élevé.

Source : http://www.europe1.fr/technologies/android-les-donnees-personnelles-impossibles-a-effacer-970842

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