Comment sont volés les smartphones

	Comment sont volés les smartphones

Le vol de mobiles en général et de smartphones en particulier reste une plaie, et ce malgré les dispositifs de protection et/ou de de désactivation mis en place par les fabricants et les opérateurs.

Une étude menée par IDG pour Lookout auprès de 2403 personnes tente de détailler le phénomène. Ainsi, parmi les utilisateurs détroussés, 32% des interrogés européens l'ont été par des pickpockets. Evidemment, le ton résolument alarmiste de l'étude doit être relativisé dans le sens où Lookout propose des solutions de sécurité pour les mobiles…
Le vol à l'arraché ou par ruse reste donc et de loin, le principal moyen de voir son précieux portable disparaître. L'oubli ne représente que 18% des pertes tandis que le vol à la maison ou dans sa voiture représente 11% des larcins.

Le lieu du délit varie selon les régions. Les Anglais constatent plus souvent des vols au bar, au pub ou en discothèque (23%). En France en revanche, les transports en commun semblent être le lieu de prédilection des voleurs (17%).

Prêts à payer pour récupérer leurs données
L'étude nous apprend également qu'il y a des heures « plus propices » aux vols. « Que ce soit au Royaume-Uni, en France ou Allemagne, la tranche horaire comprise entre midi et dix-sept heures semble être la plus courue des malfrats », peut-on lire.
Et le smartphone est désormais tellement une extension de sa personne que les utilisateurs sont prêts à prendre des risques pour le récupérer. Les Allemands semblent être les moins timides et les plus téméraires, 89% d'entre eux (71% au Royaume-Uni et 68% en France) étant prêts à se mettre en situation relativement dangereuse pour récupérer leur smartphone volé.
Pire, une victime sur 5 serait prête à payer 750 euros pour récupérer ses données perdues ! De quoi donner des idées, pas forcément très légales.
Les victimes françaises qui passent à l'action en cas de vol de leur téléphone procèdent de manière très organisée, la majorité d'entre eux déposant plainte auprès de la police locale (71%) et informant leur opérateur (74%). En Allemagne en revanche, seulement 58% des victimes signalent le vol à leur opérateur et 63% portent plainte auprès de la police.
Au lieu de cela, 26% des Allemands tendent à utiliser une application de localisation de mobiles (contre 17% de Français et 19% de Britanniques) lorsque leur téléphone est volé.

Avec des smartphones de plus en plus puissants et chers, il faudra encore renforcer les mesures anti-vol ce qui semble être le cas avec la généralisation de la fonction 'kill switch'.
La Californie vient ainsi de passer une loi qui contraindra les constructeurs à proposer ce 'kill switch' à l'utilisateur sur tous les portables vendus en Californie à compter du 1er juillet 2015. Ce n'est pas une première : le Minnesota avait ainsi déjà fait passer une loi comparable en mai.
De plus, les constructeurs ont déjà pris les devants. C'est notamment le cas d'Apple, qui propose à ses clients un 'kill switch' permettant de désactiver à distance les fonctionnalités de l'iPhone. Au mois de juin, le procureur général de la ville de New York avait ainsi plaidé en faveur de la mise en place de cette fonction, expliquant notamment que les vols d'iPhone avaient chuté de 38% d'une année sur l'autre, suite au déploiement de cette fonctionnalité au sein d'iOS 7.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/comment-sont-voles-les-smartphones-39805631.htm

L’Internet des objets ne doit pas devenir un cauchemar pour la sécurité des entreprises

L’Internet des objets ne doit pas devenir un cauchemar pour la sécurité des entreprises

En matière d’Internet des objets (IoT), les entreprises sont laissées à elles-mêmes avec des problèmes de sécurité béants. Les objets connectés, les services et les capteurs ont un potentiel important, mais représentent un risque. Heureusement, ce risque peut être géré au niveau de l’API.

C’est ce que dit en substance Mark O’Neill, vice-président de l’innovation chez Axway. Dans un récent article publié dans le Science Technology Magazine, il presse les responsables IT de commencer à s’intéresser de plus près à la sécurité de l’IoT.
« Chaque appareil intelligent, chaque application connectée récolte des données et chaque appareil intelligent, chaque application connectée risque d’exposer ces données. Les entreprises promettant une expérience exceptionnelle avec leurs produits et services connectés à l’Internet des objets doivent tenir cette promesse avec une sécurité sans précédent. »
Il estime qu’il faut prendre en compte les implications d’une chaîne d’approvisionnement bien équipée en capteurs et appareils intelligents. « Les entreprises laissent des données sensibles dans la nature et risquent une perturbation de leur chaîne d’approvisionnement si elles ne s’inquiètent pas de la sécurité quand elles utilisent codes barres, RFID ou GPS pour surveiller le fonctionnement de leur chaîne, et quand elles connectent à Internet des fonctionnalités traditionnellement gérées derrière le pare-feu de l’entreprise. »
Le temps où « les fabricants pouvaient masquer leurs API et espérer que les hackers ne les localisent et ne les manipulent pas » est révolu, ajoute Mark O’Neill.
Il y a diverses façons de mitiger ces risques. Les portails et passerelles de déploiement d’API [« API portals » et « API gateways », NdT] sont des mesures pro-actives qui peuvent aider à sécuriser un objet connecté. « La sécurité doit être pensée au niveau de l’API », affirme-t-il [sans étonnement, puisque c’est la solution que propose Axway, NdT]. Cela permet de donner « un contrôle complet de la sécurité des appareils aux vendeurs et aux fabricants, qui est dans le monde de l’Internet des objets l’endroit le plus sûr pour gérer la sécurité… Les API peuvent être le point à partir duquel les entreprises imposent leurs politiques de protection des données et de sécurité. »
Les API Gateways « permettent aux API de recevoir des patchs virtuels, une forme de sécurité montante qui évite que le trafic malicieux puisse atteindre l’API sans modifier le fonctionnement de l’appareil. Les patchs virtuels fonctionnent sans modifier le code source de l’API et permettent de gérer les risques rapidement. »
Les API Portals « permettent aux développeurs de voir comment les appareils utilisent les API dans le temps. » Ce qui permet aux entreprises de produire des audits, utiles pour « aider à enquêter sur les attaques d’API et assurer la conformité avec les réglementations de l’industrie. » Ces données sont une nécessité absolue dans certains domaines comme la santé, ajoute O’Neill. De plus, « les entreprises utilisent de plus en plus les API pour la collaboration B2B et l’échange de données ; dans ces cas précis les enregistrements d’audits pour les API peuvent être utilisés comme des méthodes de traçage sur la façon dont les gens accèdent à l’information ».

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.zdnet.fr/actualites/l-internet-des-objets-ne-doit-pas-devenir-un-cauchemar-pour-la-securite-des-entreprises-39805409.htm

Rendre n’importe quel objet connecté : la « mother » est là

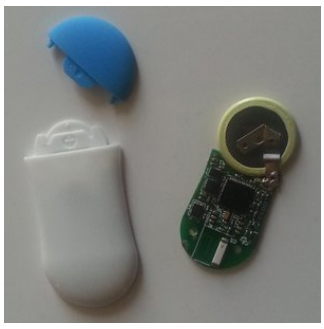
Rendre n’importe quel objet connecté : la « mother » est là

La Mother. « Une maman, mais en mieux » qui s'accompagne d'une ambitieuse promesse : rendre n'importe quel objet connecté.

Si le lapin connecté Nabaztag n'a pas rencontré le succès escompté, l'Internet des objets est, lui en pleine expansion. Malgré l'échec de son premier poulain, Rafi Haladjian, cofondateur de Violet – racheté en 2011 par Aldebaran Robotics – est resté convaincu du potentiel des objets connectés.
Depuis la fondation de sa nouvelle société Sen.se en 2010, il travaille avec une douzaine de personnes sur Sense Mother, un nouvel objet connecté autour duquel gravitent des Motion Cookies. La Mother, pivot central du système, se connecte à Internet à l'aide d'un port Ethernet, et au secteur. Elle est en charge de récupérer les informations transmises par les Motion Cookies à l'aide d'un système de transmission fonctionnant en 868 MHz développé par Sen.se. Les Cookies font tout le reste du travail.

Rendre n'importe quel objet connecté
Un Motion Cookie est un petit galet plat qui pèse quelques grammes et qui embarque un accéléromètre, un thermomètre, un processeur et une pile. Son autonomie varie selon son utilisation – de 4 à 17 mois – et il faut ensuite changer la pile. L'usage qui en est fait dépend de son utilisateur : chaque Cookie intègre les mêmes fonctionnalités, il ne reste qu'à l'assigner à une tâche précise via le tableau de commande disponible en ligne.
Attaché à une bouteille d'eau, le Cookie va pouvoir mesure la quantité de boisson bue dans la journée par une personne. Fixé sur une brosse à dent, il va chronométrer la durée du brossage. Installé entre le matelas et le drap-housse du lit, il va surveiller vos cycles de sommeil. Dans votre poche de pantalon, il va servir de podomètre, mais il va également enregistrer les heures où vous sortez et rentrez chez vous. Fixé à votre porte d'entrée, il va effectuer un suivi des allers et venues, pour éventuellement vous alerter en cas d'intrusion suspecte… ces possibilités comptent parmi la quinzaine de fonctions qui seront proposées au lancement de la Mother et des Motion Cookies.
Les dispositifs seront fournis avec des accessoires permettant de fixer les Cookies aux objets pour les rendre aussi discrets et peu encombrants que possible. La promesse est de rendre les objets de la vie quotidienne connectés par ce biais, l'autonomie élevée des Cookies permettant également de ne pas s'inquiéter en permanence de la possibilité d'utiliser les fonctions connectées.
« On veut que vous viviez votre vie normalement » explique Rafi Haladjian, pour qui il est important que l'utilisateur, une fois ses choix de fonctionnalités effectués, n'ait plus à se soucier de rien. « Nous sommes nombreux à avoir déjà utilisé une application smartphone pour surveiller notre sommeil, mais il faut effectuer des manipulations contraignantes pour la faire fonctionner, ou utiliser un accessoire spécial. Si bien qu'au bout de quelques jours, on arrête de s'en servir. Là, il suffit d'installer le Cookie une bonne fois pour toute, et de l'oublier » ajoute-t-il.
Toutes les données récoltées sont ensuite disponibles dans un journal en ligne, qui hiérarchise les informations selon leur importance.

Des Cookies, et après ?
La Sense Mother et ses Motions Cookies seront disponibles au printemps prochain, au tarif de 199 euros le pack comprenant la Mother et 4 Cookies, 88 euros les 4 Cookies supplémentaires et 111 euros la Mother seule. Mais ces dispositifs ne sont que l'amorce d'un écosystème dans lequel le PDG de Sen.se fonde de grandes ambitions : des partenariats avec de nombreuses entreprises ont été signés pour proposer rapidement des objets compatibles avec les Cookies. Sen.se prévoit également de proposer des accessoires supplémentaires, sans préciser leur nature et de délai de sortie.



A gauche, une brosse à dent équipée d'un Cookie. A droite, un Cookie décortiqué.

« Si l'Internet des objets est intéressant, c'est parce qu'il peut toucher toutes les industries, quelles qu'elles soient. Ça n'a de sens uniquement si c'est le cas » conclut Rafi Haladjian. Les précommandes de la Mother et des Motion Cookies débute aujourd'hui sur le site dédié : reste donc à savoir si le grand public adhérera à cette maman connectée qui sait tout.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Source :
http://www.clubic.com/mobilite-et-telephonie/objets-connectes/actualite-605330-sen-sense-mother-promesse-connecte.html

Internet des objets – L’industrie va être bousculée | Alliancy, le mag

	Les objets connectés vont bousculer nos vies

Les objets connectés vont se multiplier dans les années qui viennent. Dès aujourd'hui, tous les industriels doivent intégrer cette nouvelle dimension, tant dans leur façon de concevoir et de fabriquer leurs produits que dans leur business model.80 milliards, c'est le chiffre choc publié par l'Idate, voici quelques mois. Il s'agit du nombre d'objets connectés qui auront été vendus à l'horizon 2020. Mais Idate, Gartner ou IDC… toutes les analyses prévoient une progression fulgurante de l'Internet des objets, un phénomène qui impactera toute l'industrie. D'une part, il y a aura des terminaux connectés à Internet, c'est-à-dire les smartphones, les tablettes et autres « phablettes »…, et, d'autre part, des objets intelligents, balances, bracelets, brosses à dents, montres connectés… Tous ces objets grand public bénéficient d'une très large couverture médiatique et connaîtront une forte croissance dans les années à venir. La généralisation du bouton d'appel d'urgence eCall, obligatoire dans toutes les voitures neuves vendues en Europe à partir de 2015, va imposer la voiture connectée sur nos routes. De même, tous les Français vont, tôt ou tard, disposer d'un compteur intelligent (Linky) et pourront suivre sur le Net l'évolution de leur consommation électrique ou de gaz quasi en temps réel.

Mais, pour Samuel Ropert, analyste à l'Idate, la grande majorité de cet Internet des objets sera peuplée de « choses » beaucoup moins technologiques. « La plus grande part de l'Internet des choses se composera d'objets ne disposant pas d'intelligence, mais capable d'interaction. 85 % de ces milliards d'objets connectés à venir seront porteurs d'une puce RFID ou même d'un simple code-barres 2D, et donc porteur d'une information. »

Dans un premier temps, les industriels vont déployer ces technologies pour optimiser leur supply chain. « Si la conjoncture actuelle freine les grands déploiements de puces RFID, les industriels et les grandes enseignes de la distribution peuvent espérer des gains significatifs dans l'efficacité de leur supply chain et dans la réduction de leurs stocks grâce à l'Internet des objets », ajoute l'analyste.

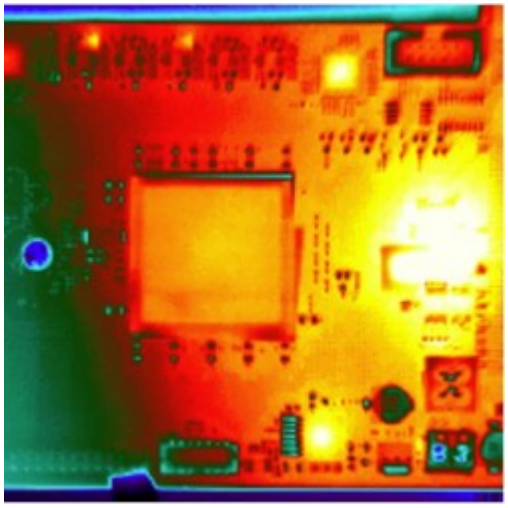
Les industriels de l'automobile préfèrent poser des puces RFID sur les conteneurs et hésitent encore à doter chaque pièce détachée d'une puce pour des raisons de coût.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

Internet des Objets – L'industrie va être bousculée

IBM invente le futur cerveau de nos futurs objets connectés. Un pas de plus vers le robot humain ?



IBM invente le futur cerveau de nos futurs objets connectés. Un pas de plus vers le robot humain ?

La puce TrueNorth d'IBM pourrait peupler l'Internet des objets
Quand elle sera au point, la puce TrueNorth pourrait faire office de capteur basse consommation pour les appareils embarqués et portables.
IBM a franchi une nouvelle étape dans son ambitieux projet de processeur fonctionnant comme un cerveau humain. Big Blue a mis au point une seconde **puce, plus évoluée, qui imite la façon dont fonctionne le cerveau des mammifères**. « C'est une avancée supplémentaire vers les ordinateurs synaptiques », a déclaré Dharmendra Modha, Chief scientist au sein d'IBM Research, spécialisé en informatique synaptique. Des chercheurs de Cornell Tech ont aussi contribué à l'élaboration de la puce. Dans la revue Science de cette semaine qui consacre un article au prototype, Dharmendra Modha déclare que « l'architecture de TrueNorth tend à reproduire la structure et le fonctionnement du cerveau humain au niveau du silicium, tout en étant efficace sur le plan énergétique ». Quand elle sera définitivement au point, cette puce pourrait faire office de capteur basse consommation pour les appareils embarqués et portables. « TrueNorth pourrait devenir le cerveau en silicium de l'internet des Objets et transformer totalement notre expérience mobile », a encore déclaré le directeur scientifique.
La puce pourra également être intégrée dans les superordinateurs pour augmenter leur capacité d'apprentissage automatique et prendre en charge d'autres calculs capables de fonctionner avec les réseaux neuronaux. En 2011, l'équipe d'IBM dirigée par Dharmendra Modha avait déjà sorti une puce imitant le cerveau. Cette seconde puce «TrueNorth » compte 5,4 milliards de transistors entrelacés dans un réseau sur puce de 4096 noyaux neuro-synaptiques. Cela représente l'équivalent de 256 millions de synapses, soit beaucoup plus que la version 2011 qui en comptait 260 000 environ.

Facilement adapté à de grandes mises en oeuvre
IBM a également associé 16 puces « TrueNorth » entre elles par groupe de quatre fois quatre qui offrent collectivement l'équivalent de 16 millions de neurones et de 4 milliards de synapses. L'expérience vise à montrer que le prototype peut être facilement adapté à de grandes mises en oeuvre. Ce projet de puce intelligente avait été lancé en 2008 par le Defense Advanced Research Projects Agency (DARPA) américain sous le nom de Systems of Neuromorphic Adaptive Plastic Scalable Electronics (SyNAPSE). Ces nouvelles puces rompent radicalement avec l'architecture informatique actuelle imaginée par von Neumann, où le traitement des calculs se fait en série. La nouvelle architecture se rapproche du fonctionnement du cerveau humain, dans le sens où chaque « noyau neurosynaptique » possède sa propre mémoire (« les synapses »), son processeur (« le neurone ») et son réseau de communication (« les axones »), et tous travaillent ensemble selon un mode opératoire orienté événement.
Le travail commun de ces noyaux pourrait permettre la reconnaissance des formes et d'autres fonctions de détection, comme dans le cerveau humain. Et de la même manière, la puce d'IBM a besoin de très peu d'énergie pour fonctionner : 70mW en moyenne, soit bien en deçà de ce que consommeraient les processeurs standards pour exécuter les mêmes opérations. Samsung a fabriqué la puce prototype en utilisant un procédé de gravure à 28 nanomètres. Le fait que « TrueNorth » consomme aussi peu d'énergie – moins qu'un appareil auditif – ouvre un vaste champ d'utilisations potentielles, en particulier sur les appareils disposant de ressources énergétiques limitées. Il serait par exemple possible d'intégrer ce processeur à un appareil mobile ou à un capteur, où il pourrait apprendre à reconnaître des objets après avoir analysé des sons, des images ou des sources multi sensorielles. Actuellement, il faudrait recourir au calcul intensif avec serveur dédié pour réaliser ce type d'analyses. Avec la puce, on pourrait facilement effectuer ces tâches sur un périphérique distant, sans avoir besoin de faire remonter les informations vers un centre de calcul. « Le capteur devient l'ordinateur », a déclaré Dharmendra Modha.

Prendre en charge l'apprentissage machine
L'architecture synaptique n'est pas destinée à remplacer les processeurs actuels, mais les deux types de puces pourraient être associées pour réaliser des tâches nécessitant beaucoup de puissance de calcul en parallèle. « Dans le datacenter, les puces pourraient être utilisées dans les cartes d'accélération pour coprocesseur pour faire tourner les réseaux neuronaux qui prennent en charge l'apprentissage machine », a expliqué Dharmendra Modha. « De nombreux algorithmes d'apprentissage machine utilisés actuellement peuvent être facilement adaptés à cette architecture. On pourrait effectuer des opérations de traitement hautement parallèles de façon plus efficace sur le plan énergétique », a-t-il encore déclaré.

IBM continue à explorer différentes applications possible pour son processeur, mais pour l'instant le constructeur ne s'est ni engagé à fabriquer la puce lui-même, ni à en vendre le design sous licence à d'autres fabricants. Dharmendra Modha a aussi précisé que dans le procédé de fabrication, son équipe n'avait n'a pas identifié d'obstacle particulier pour la production en masse. IBM est également en train de développer des compilateurs et des logiciels destinés à faciliter l'usage de ces processeurs.

Article de Jean Elyan avec IDG News Service

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.lemondeinformatique.fr/actualites/lire-la-puce-truenorth-d-ibm-pourrait-peupler-l-internet-des-objets-58299.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

---

Les objets connectés ont de véritables problèmes en matière de sécurité

Les objets connectés ont de véritables problèmes en matière de sécurité

Connexions Bluetooth bavardes, chiffrement de piètre qualité, politiques de protection des données personnelles inexistantes… Les accessoires connectés ont tendance à vous mettre à nu.

Votre dernière course en forêt, vos déplacements à l'étranger, vos phases de sommeil, votre consommation en nicotine ou alcool, vos cycles de menstruations (si vous êtes une femme), votre pression artérielle, votre activité sexuelle… Pour toute activité personnelle, il y a désormais une application mobile et un accessoire connecté pour capter ces informations, comme par exemple le Nike Fuel Band. Et les utilisateurs en raffolent, si l'on croit les analystes. Selon Pew Research Center, plus de 60 % des Américains utilisent ces outils pour améliorer leur performances sportives ou préserver leur bonne santé. D'ici à 2018, le nombre de ces accessoires connectés devrait dépasser les 485 millions d'unités. Un marché en plein boom que tous les grands acteurs cherchent à accaparer, à commencer par Google et Apple.

Mais ce marché est encore très balbutiant, et notamment en matière de protection de données personnelles. Symantec vient de publier, il y a quelques jours, un rapport d'analyse qui évalue le niveau de sécurité de tous ces engins. Résultat: la plupart des applications révèlent des failles flagrantes permettant à des tiers de récupérer des données à l'insu des utilisateurs. Une majorité des bracelets peuvent être localisés grâces à leurs puces Bluetooth. Activés en permanence, ils sont plutôt bavards et émettent une adresse physique de type MAC, ainsi que des identifiants divers et variés, qu'il est aisé de capter dans un rayon de 100 mètres.
C'est d'ailleurs ce que les analystes de Symantec ont fait: ils ont créé des sniffeurs Bluetooth basés sur une carte Raspberry Pi, qu'ils ont disséminés aux abords d'une compétition sportive, ou trimballés dans un sac à dos en plein milieu d'un centre commercial. Certes, ces données ne permettent pas d'identifier une personne, mais c'est un premier pas…

Des mots de passe transmis en clair
Autre problème: parmi les applications qui utilisent des services cloud pour stocker ou traiter les données captées, 20 % transmettent les identifiants en clair, sans aucun chiffrement. Parmi les 80 % restantes, certaines appliquent aux identifiants des fonctions de hachage de faible protection comme MD5, qui peut facilement être craqué par les cybercriminels.
Dans un certain nombre de cas, la gestion de sessions laisse également à désirer, permettant par exemple de deviner ou de calculer des identifiants et ainsi d'accéder à des comptes utilisateurs.
Enfin, plus de la moitié des applications (52 %) n'apportent aucune information sur la manière dont toutes ces données sont traitées et stockées, alors que c'est obligatoire dans bon nombre de pays. Et quand il existe un document d'information, celui-ci est souvent très vague. On peut donc douter du sérieux de ces fournisseurs en matière de protection des données personnelles.
En somme: si toutes ces nouveaux appareils et applications semblent bien pratiques, il est conseillé de regarder en détail leur fonctionnement, histoire de pas se faire avoir !

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.01net.com/editorial/624818/les-objets-connectes-sont-des-passoires-en-matiere-de-securite/#?xtor=EPR-1-NL-01net-Actus-20140806

Objets connectés : HP s'inquiète des failles de sécurité

Le danger pourrait aussi bien venir des Objets connectés

Au total, 10 objets ont été passés au crible par les services de Fortify, la division d'HP dédiée à la cybersecurité.

Lesquels ? On ne sait pas exactement, l'entreprise se contente de préciser qu'ils sont de tous types (webcam, domotique, hub

etc…) et font partie des objets les plus vendus. Mais dans un souci diplomatique, le rapport semble préférer la discrétion, afin peut être de laisser le temps aux constructeurs de corriger ces vulnérabilités.

Le problème n'est pas anodin puisque comme le relève l'étude, 9 de ces 10 objets stockent ou utilisent des données personnelles de l'utilisateur. Parmi ceux la, 7 d'entre eux ne chiffrent pas les données qu'ils transfèrent vers le réseau, et 6 objets proposent des interfaces web vulnérables à des attaques de cross-site scripting ainsi qu'à d'autres types d'attaques plus simples basées sur le social engineering. Un exemple criant : 8 objets sur 10 ne posent aucune restriction sur le choix du mot de passe, permettant ainsi à l'utilisateur de choisir un mot de passe du type « 123456 »

L'internet des objets : un gruyère ?

En moyenne, les objets étudiés par Fortify présentaient chacun 25 failles de sécurité, allant des plus obscures à d'autres beaucoup plus connues telles que des vulnérabilités ayant trait à Heartbleed. La générosité gratuite n'étant pas vraiment de ce monde, cette initiative n'est pas innocente de la part d'HP qui en profite pour faire la promotion de son activité de sécurité Fortify et redirige tout au long du rapport le lecteur vers son site Owasp, un site open source dédié à la sécurité des objets connectés.

Peu de chiffres, pas de noms, HP ne se mouille donc pas trop mais on peut rappeler que l'objet du rapport n'en reste pas moins pertinent : la sécurité des objets connectés est un enjeu de taille que les constructeurs ne peuvent se permettre de traiter à la légère.

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :
http://www.zdnet.fr/actualites/objets-connectes-hp-s-inquiete-des-failles-de-securite-39804463.htm

---

Les Objets connectés et leurs failles de sécurité ont de quoi nous inquiéter

Les Objets connectés et leurs failles de sécurité ont de quoi nous inquiéter
Dans une étude, HP s’est penché sur les failles de sécurité au sein de 10 objets connectés parmi les plus populaires. L’entreprise relève que ces nouveaux objets présentent de nombreuses vulnérabilités et incite les constructeurs à en tenir compte.

Les objets connectés à notre e-santé dévoilent nos données

personnelles

Les objets connectés à notre e-santé dévoilent nos données personnelles

Alors que la présence du wearable (ensemble des vêtements et accessoires comportant des éléments informatiques et électroniques avancés) croît rapidement et avec elle, la collecte d'informations de santé, la Commission fédérale du commerce américain s'inquiète de ce que peuvent devenir ces données très personnelles.

Samsung a SAMI, Apple a Healthkit Google a Google Fit.

Trois grands noms des smartphones et trois approches de l'e-santé qui ont pour point commun de recueillir, formaliser et stocker vos données de santé sur votre téléphone ou sur des serveurs.

Quoi de plus personnel que votre état de santé et ses indicateurs ? Quoi de plus précieux et éventuellement de plus valorisés pour fournir des services complémentaires ?

Julie Brill, commissaire au sein de la Commission fédérale du commerce (FTC) s'inquiétait en tout cas de l'accélération de cette tendance qui va prendre encore plus d'importance avec la multiplication des montres et bracelets connectés. Pour elle, la façon dont les données sont « siphonnées » par ces applications est préoccupante. « Nous ne savons pas où ces informations vont en définitive », indiquait-t-elle devant un groupe de discussion organisé par le site politique The Hill. « Cela met les consommateurs dans une situation inconfortable », continuait-elle. La Commissaire a souligné devant le Congrès l'importance de voter une loi pour interdire la collecte d'informations personnelles sous de faux prétextes.

Le besoin de régulation ?

En mai dernier, la FTC rendait un rapport dans lequel elle indiquait qu'une bonne part des développeurs d'applications d'e-santé donnait accès aux données de santé collectées à des sociétés extérieures. Ainsi, l'étude menée sur douze applications de fitness et e-santé démontrait que ces informations électriques étaient partagées avec 76 entreprises différentes, y compris pour du marketing.

Face à un paysage si inquiétant et totalement dépourvu de cadre légal, la commissaire de la FTC s'inquiète que « personne ne parle de nouvelle réglementation ».

L'ACT, Association for Competitive Technology, lobby qui défend les intérêts des développeurs d'applications, craint évidemment qu'une quelconque réglementation nuise à l'innovation. Morgan Reed, directeur exécutif de l'ACT, déclarait ainsi à l'occasion de ce groupe de discussion : « L'industrie de la santé mobile a besoin d'éduquer la FTC sur les apports positifs que peut avoir la collecte d'informations sur la santé. […] Si nous échouons dans ce rôle, la commission pourrait prendre des décisions qui pourraient dévaster les

développeurs d’applications ».

Ci-dessous à la 34ème minute, Julie Brill, commissaire au sein de la Commission fédérale du commerce.

http://www.ustream.tv/recorded/50427445

Si les bénéfices de la surveillance régulière de notre santé sont indéniables, il va une fois encore faire attention à ne pas devenir un produit dans la stratégie marketing d’acteurs peu soucieux de nos vies privées. Pour éviter ces pièges, Julie Brill préconise qu’un gros effort pédagogique soit fourni, d’une part et d’autre part que les utilisateurs soient toujours informés des informations recueillies et partagées. Un effort de transparence pour les plus personnelles de nos données…

Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

Références :

http://www.01net.com/editorial/624302/e-sante-debut-de-la-bataille-pour-nos-donnees-entre-la-ftc-et-les-lobbies/#?xtor=EPR-1-NL-01net-Actus-20140724