L’intelligence artificielle, notre futur Terminator?

	L’intelligence artificielle, notre futur Terminator?

L’intelligence artificielle pourrait menacer à terme l’Humanité: il ne s’agit pas d’un film de science-fiction mais de la prédiction du célèbre physicien Stephen Hawking, qui relance le débat sur le risque de voir l’homme dépassé par les technologies qu’il a lui-même créées.

Interrogés par l’AFP, anthropologue, futurologues et experts en intelligence artificielle se montrent partagés sur les craintes d’Hawking.
Les craintes d’un homme apprenti sorcier sont anciennes et elles ont nourri nombre de romans et des films comme « 2001: Odyssée de l’espace » avec son ordinateur meurtrier Hal 9000 et plus récemment « Terminator », le robot exterminateur.
Mais aujourd’hui, c’est un astrophysicien très respecté, le Britannique Stephen Hawking, qui lance un pavé dans la mare. Atteint d’une dystrophie neuromusculaire, il s’exprime grâce à un ordinateur.
« Les formes primitives d’intelligence artificielle que nous avons déjà se sont montrées très utiles », reconnaît-il. « Mais je pense que le développement d’une intelligence artificielle complète pourrait mettre fin à la race humaine », a-t-il déclaré cette semaine à la BBC.
Déjà, le milliardaire Elon Musk avait expliqué avoir investi dans des sociétés d’intelligence artificielle pour « garder un oeil » sur ce qui se passe dans ce domaine. « Nous devons nous assurer que les conséquences sont bonnes et non mauvaises », selon lui.
« Cela me fait plaisir qu’un scientifique des +Sciences dures+ dise cela. Je le dis depuis des années », déclare Daniela Cerqui, anthropologue à l’université de Lausanne.
« Nous déléguons à ces machines de plus en plus de prérogatives de l’humain, afin qu’elles soient plus performantes que nous. On va finir par devenir leur esclave », selon elle.
A l’inverse, Jean-Gabriel Ganascia, philosophe et expert en intelligence artificielle, juge « excessif » le « cri d’alarme » de Hawking.
« Le danger, c’est davantage l’homme qui se servirait de ces technologies pour asservir » d’autres humains, considère ce professeur à l’Université Pierre-et-Marie-Curie à Paris.
– Développer une intelligence artificielle « amicale »-
Nick Bostrom, futurologue à l’Université d’Oxford, pense que « la machine intelligente parviendra à dépasser l’intelligence biologique. Il y aura alors des risques existentiels associés à cette transition ».
« Les machines sont déjà plus fortes que nous. Je pense qu’elles finiront aussi par devenir plus intelligentes, même si ce n’est pas le cas actuellement », ajoute-t-il.
Au cours de ces dernières années, d’énormes progrès ont été réalisés dans le domaine de l’intelligence artificielle, en tant que capacité à traiter, à analyser des données et à répondre à des questions.
Mais on est « encore loin » de l’intelligence artificielle générale « complète », qui inquiète Stephen Hawking, souligne Anthony Cohn, professeur à l’université de Leeds (centre du Royaume-Uni). « Il faudra encore plusieurs décennies. »
Mathieu Lafourcade, spécialiste en intelligence artificielle et en traitement du langage à l’Université de Montpellier (sud de la France), juge « alarmiste » l’avertissement du physicien.
Mais il pense que « dans un futur hypothétique », il faudra peut être « s’en remettre » dans certains domaines aux machines car leurs capacités intellectuelles auront dépassé les nôtres. « La machine nous proposera une solution que nous ne serons pas à même de comprendre mais il faudra lui faire confiance », par exemple si elle nous recommande des mesures contre le réchauffement climatique, considère-t-il.
« Toutefois, si la machine débloque, il faudra se réserver la possibilité de la débrancher », souligne-t-il.
Stuart Armstrong, futurologue à l’université d’Oxford, relève que « les incertitudes sur le développement de l’intelligence artificielle sont extrêmes ».
« Le problème, c’est qu’il est extrêmement difficile de programmer des objectifs compatibles avec la dignité voire la survie de l’Humanité », dit-il.
« Il faudrait programmer presque toutes les valeurs humaines parfaitement dans l’ordinateur afin d’éviter que l’Intelligence artificielle n’interprète +éradique la maladie+ comme +tue tout le monde+ ou bien +garde les humains sains et saufs et contents+ comme +enterre tout le monde dans des bunkers avec de l’héroïne+ ».
« Il faut que les ingénieurs prennent ces problèmes au sérieux et trouvent des solutions pour développer une intelligence artificielle +amicale+, pleinement compatible avec les valeurs humaines », considère-t-il.

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

Source : http://www.leparisien.fr/sciences/l-intelligence-artificielle-notre-futur-terminator-08-12-2014-4355179.php#xtref=https%3A%2F%2Fwww.google.fr%2F

Que deviennent les données stockées sur nos objets connectés ?

Que deviennent les données stockées sur nos objets connectés ?

Une équipe de France 2 a enquêté sur ces objets connectés qui ont envahi notre quotidien et conservent nos données personnelles.

Chaque jour, 5 millions de Français prennent le pouls de leur santé à l'aide de leurs objets connectés qui engloutissent des informations sur leurs utilisateurs. Ces données sont envoyées via Internet sur un serveur stocké dans un lieu ultra-sécurisé, le data-center, constitué de millier d'ordinateurs. La protection de ces données dépend de la législation du pays où elles sont conservées. « Si vous avez de la chance, vos données atterriront en France dans un data-center comme celui-là, dans la réglementation française qui est très protectrice. Si vous n'avez pas de chances, elles atterriront aux États-Unis ou ailleurs », commente Arnaud de Bermingham, directeur des services d'hébergement Online.

Les internautes exposés à la publicité ciblée

Aux États-Unis, l'administration peut librement accéder à vos données personnelles sous couvert de sécurité nationale. En France, les fabricants d'objets connectés doivent obtenir le consentement des utilisateurs et garantir leur sécurité contre le piratage. Subsiste toutefois le risque de voir ses données vendues à des fins mercantiles. La loi interdit toutefois l'utilisation de ces données par la sécurité sociale ou les assurances.

La vidéo de FranceTV Info pour mieux comprendre le phénomène

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

Source : http://www.francetvinfo.fr/economie/medias/video-que-deviennent-les-donnees-stockees-sur-nos-objets-connectes_757247.html
Par France 2

74% des réseaux domestiques français sont fortement exposés à la cybercriminalité

74% des réseaux domestiques français sont fortement exposés à la cybercriminalité

Près de trois ménages français sur quatre connectés à internet sont susceptibles d'être victimes d'une cyberattaque via leur routeur sans fil, estime Avast Software, qui vient de publier une étude sur ce domaine. La vulnérabilité des routeurs et la faiblesse des mots de passe permettent aux pirates informatiques d'accéder facilement aux réseaux domestiques.

« Les routeurs non-sécurisés sont des points d'entrée très faciles d'accès pour les hackeurs, qui sont dès lors capables de pirater des millions de réseaux domestiques en France, déclare Vince Steckler, Directeur Général d'Avast. Notre enquête révèle que la vaste majorité des routeurs domestiques en France ne sont pas sécurisés. Et si un routeur n'est pas correctement sécurisé, un cybercriminel pourra facilement accéder aux informations personnelles d'un particulier, comme par exemple à ses données financières, ses identifiants et mots de passe, ses photos et son historique de navigation. »

D'après l'étude, plus de la moitié des routeurs seraient mal sécurisés par défaut ou ne seraient équipés d'aucune protection, avec des combinaisons login/mot de passe beaucoup trop évidentes telles que admin/admin ou admin/mot de passe, voire admin/. Au terme de cette enquête réalisée auprès de plus de 20 000 ménages en France, Avast met également en avant que 24% des consommateurs utilisent comme mot de passe leur adresse, leur nom, leur numéro de téléphone, le nom de leur rue ou d'autres mots faciles à deviner.

L'un des principaux risques auxquels un réseau Wi-Fi est exposé est le piratage du système de noms de domaine (DNS). Les logiciels malveillants sont utilisés pour exploiter les failles de sécurité d'un routeur insuffisamment protégé et pour rediriger subrepticement l'utilisateur depuis un site connu, comme par exemple un site web bancaire, vers une fausse page identique à l'original. Lorsque l'utilisateur s'y connecte, le pirate peut ainsi capturer ses identifiants et les utiliser pour accéder à son compte sur le véritable site.

« Le manque de sécurisation actuel au niveau des routeurs rappelle fortement la situation des PC dans les années 1990, où les tendances laxistes des utilisateurs en matière de sécurité et l'explosion du nombre de menaces avaient rendu les environnements informatiques largement exploitables. La grande différence, c'est que les utilisateurs stockent aujourd'hui bien plus d'informations personnelles sur leurs appareils qu'ils n'en avaient auparavant. Les consommateurs ont besoin d'outils à la fois simples d'utilisation et capables de prévenir toute cyberattaque ciblant leurs données », explique Vince Steckler.

Toujours selon le sondage, moins de la moitié des français interrogés sont persuadés que leur réseau privé est sécurisé, tandis que 20% d'entre eux déclarent avoir déjà été victimes d'un pirate informatique. Les participants précisent être pleinement conscients de la gravité des conséquences d'une faille de sécurité, et confient que leurs principales craintes concernent le vol de leurs données bancaires ou financières (34%), la perte de leurs informations personnelles (34%), le piratage de leurs photos (17%) et le vol de leur historique de navigation (13%).

Afin de répondre à ces problèmes, Avast a récemment lancé Avast 2015, qui inclut la première solution de sécurisation de réseaux privés (Home Network Security), capable de protéger les utilisateurs face au piratage des réseaux domestiques, tant au niveau du système de noms de domaine que dans le cas de mots de passe trop simples. Avast 2015 est disponible gratuitement et en version payante via www.avast.com.
L' « internet des objets » est présent dans les ménages français : 96% des ménages français possèdent six appareils ou plus connectés à un réseau Wi-Fi. En marge des ordinateurs de bureau et portables, les utilisateurs possèdent des appareils mobiles (28%), des imprimantes et scanners (18%), des Smart TV (5%), et des lecteurs DVD ou Blu-ray (3%) connectés à leur réseau Wi-Fi.
Les utilisateurs craignent que des « espions » ne se cachent dans leur voisinage, mais certains aiment aussi épier les autres : 60% des répondants seraient très mal à l'aise s'ils apprenaient qu'un voisin ou une tierce personne se connecte en cachette à leur réseau Wi-Fi privé. 5% indiquent avoir eux-mêmes déjà utilisé le réseau Wi-Fi d'un voisin sans le lui avoir signalé ou lui en avoir demandé la permission…

Malgré leurs inquiétudes, les utilisateurs manquent de clairvoyance en matière de protection : 23% des répondants ignorent s'ils disposent d'une solution de protection sur leur réseau domestique, alors que 12% sont sûrs de ne pas en posséder une seule. 25% des personnes interrogées utilisent toujours le même nom d'utilisateur et le même mot de passe, aussi bien pour leur routeur que sur les sites web protégés par mot de passe. 34% ont conservé le mot de passe par défaut de leur routeur, tandis que 6% des utilisateurs sont incapables de répondre à cette question. Seuls 38% ont pris des mesures supplémentaires pour protéger leur réseau, en marge de leur pare-feu de base.

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

Source : http://www.lavienumerique.com/articles/152544/74-reseaux-domestiques-francais-sont-fortement-exposes-cybercriminalite.html

Les Français demandent des boutiques et des vendeurs connectés

	Les Français demandent des boutiques et des vendeurs connectés

Les magasins doivent-ils accélérer leur transformation numérique ? Selon cette étude d'OpinionWay, les Français sont agacés par le manque de connaissance client et les lacunes des vendeurs sur le conseil.

Le b.a.-ba de la relation-client est de reconnaître les personnes qui ont déjà acheté dans sa boutique, et quels produits. La pratique est répandue dans les petits commerces auprès de la clientèle la plus fidèle. Elle l'est aussi, de façon moins chaleureuse, sur les sites e-commerce, notamment grâce aux cookies. Toujours est-il que lorsqu'on fait une moyenne, les consommateurs regrettent de ne pas être reconnus en boutique.

Extrait du film Minority Report

Ce constat est fait par OpinionWay au travers d'une étude auprès d'un millier de personnes pour le vendeur de meubles en ligne Miliboo – précisons que ce dernier a lancé cet automne une boutique ultra-connectée à Paris. Selon cette étude, tout juste 13% des consommateurs interrogés ont ainsi le sentiment que les magasins se souviennent des problèmes qu'ils ont rencontrés lors de leurs derniers achats, 22% pensent que les magasins se rappellent de la dernière fois qu'ils sont venus et 24% ont l'impression que les magasins les connaissent.

« Les Français attendent des vendeurs plus d'implication. Il est important pour eux qu'ils puissent répondre à leurs questions immédiatement, sans hésitation ni délais », argumente Aline Buscemi, co-fondatrice de miliboo.com. Les consommateurs attendent également « un service toujours plus poussé et personnalisé ».

Avoir un meilleur conseil

Autre constat : six Français sur dix veulent gagner du temps en boutique – cet argument est souvent avancé par les personnes préférant acheter sur Internet. Plus de six personnes sur dix demandent une accélération du passage en caisse, et près de huit sur dix aimeraient récupérer en boutique un achat effectué en ligne.

Les trois quarts, enfin, voudraient connaître l'état des stocks des magasins en temps réel afin d'éviter de se déplacer pour rien. C'est dans cette optique que des sites de Web-to-store comme Socloz se développent.

Dernier constat accablant – et sévère, disons-le – pour les commerçants en dur : les deux tiers des Français interrogés déclarent que les vendeurs ne savent pas donner de conseils en boutique. Ils sont, du reste, 57% à en appeler à un équipement des vendeurs en smartphones ou tablettes afin de pêcher des informations à même de les renseigner. Si bien qu'un Français sur cinq serait même prêt à payer un peu plus cher pour cela.

Visite de la boutique du futur par Cegid

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire…

Source : http://pro.clubic.com/actualite-e-business/actualite-743139-magasins-connectes-etude.html

Quand les objets connectés contrôlent nos vies…

Quand les objets connectés contrôlent nos vies…

La sécurité est un enjeu majeur pour les objets connectés. Que ce soit dans le Quantified Self où les données relatives à la santé sont sensibles ou dans la domotique où les pirates peuvent prendre contrôle de la maison, les failles sont multiples.

Nous vous avions déjà parlé du hack du thermostat Nest lors de la Blackhat Conference, voici maintenant 5 autres cas avérés de piratage d'objets connectés. L'objectif n'est pas de vous faire peur, mais de simplement montrer que de nouveaux défis émergent pour toutes les sociétés qui s'y lancent.

Le compteur électrique qui coupe le courant
Une étude réalisée par deux experts en sécurité a montré de sérieuses lacunes dans les derniers compteurs d'électricités intelligents mis sur le marché pour répondre aux nouvelles normes du gouvernement espagnol. Les deux spécialistes ont ainsi démontré qu'il était possible de couper le courant chez les propriétaires (potentiellement pour créer un gros black out) ou trafiquer les compteurs pour fausser les factures. Grâce à un système d'infection en cascades, il serait même possible de remonter jusqu'aux centrales électriques. Sans donner le nom du fournisseur de compteurs chez qui la faille a été découverte, on sait cependant qu'il s'agirait d'un des gros acteurs du marché en Espagne que sont Endesa, Iberdrola ou E.ON.
L'Union Européenne a lancé un programme pour inciter les habitants à développer l'usage du compteur d'électricité intelligent, dans l'objectif d'économiser 3% d'énergie supplémentaires d'ici à 2020. A cette date, ce sont deux tiers des européens qui devraient en avoir installé un (sous condition qu'ils ne représentent pas de faille aussi importante…).

L'ampoule connectée qui découvre les mots de passe Wi-Fi
La société Context a exposé une faille de sécurité dans une ampoule connectée : la Lifx Wi-Fi. En parvenant à accéder à l'ampoule, elle a réussi à récupérer et décrypter les informations de configuration du réseau. L'équipe qui avait déjà trouvé des failles dans des imprimantes ou des moniteurs pour bébés a accédé au firmware de l'ampoule en étudiant le microcontrôleur afin de comprendre le mécanisme de cryptage de l'ampoule.
Le responsable recherche chez Context a déclaré « Pirater l'ampoule n'est pas simple, mais ne nécessite pas non plus d'avoir des connaissances trop complexes en matière de hack ». Il précise que ces vulnérabilités peuvent facilement être comblées en travaillant avec les développeurs Lifx. Il a déjà vu des cas plus complexes…

Le moniteur vidéo qui insulte bébé
Un couple américain habitant de l'Ohio a entendu une voix inconnue dans la chambre de leur bébé en août 2013. Il s'agissait d'un hacker qui avait réussi à prendre le contrôle de la caméra pour surveiller le bébé. Selon ABC News, la voix proférait des insultes au bébé.
Le père du bébé avait pourtant pris des précautions, notamment en donnant des mots de passe à son routeur et la caméra et en utilisant un pare-feu. La caméra était une Foscam. La société a rapidement sorti une mise à jour permettant d'éviter de nouveaux désagréments. Malheureusement, tous les utilisateurs n'ont pas mis à jour leur caméra de surveillance de bébé, à l'instar de la famille Schreck chez qui l'incident s'est reproduit en avril 2014. Les réactions en vidéo :

La box TV qui menace les grands-mères
A croire que cela ne se passe qu'aux Etats-Unis, voici l'histoire d'une grand-mère de la ville d'Indianapolis qui a eu la mauvaise surprise de voir des messages vulgaires apparaître sur sa télévision après que sa box TV AT&T ait été piratée. Alana Meeks a rapidement changé de box en n'espérant plus jamais revoir ces messages menaçants, rien n'y a fait. La police est intervenue et a pris notes des injures proférées à son encontre sur la télévision.
AT&T a immédiatement déclaré rechercher les causes de ce piratage, mais aucune nouvelle information n'a été officialisée depuis. On ne sait finalement pas si Mme Meeks a rallumé une télévision depuis.

Le frigo connecté spammeur
Le premier cas de frigo qui envoi du spam a été découvert en Californie au début de l'année. Il faisait partie d'un parc de plus de 100 000 appareils dont les pirates se servaient pour leur spam, avec des ordinateurs, des smart TV et des médias center. Plus de 750 000 emails ont été envoyés depuis ces appareils, dont 75% par les ordinateurs et le reste par des objets pour la maison reliés à internet.
Bref, autant d'exemple pour montrer que les objets connectés sont aujourd'hui vulnérables à ce genre d'attaques. Evidemment, avec le nombre de ces appareils qui va en s'accroissant, il faudra que les fournisseurs de technologie redoublent de vigilance pour assurer la sécurité de leurs clients. On se rappelle que HP a publié il y a quelques mois une étude qui montrait des résultats éffarant sur les objets connectés : ce ne seraient pas moins de 250 vulnérabilités qui auraient été découvertes dans les 10 objets connectés les plus populaires du moment.

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

Source : http://www.stuffi.fr/objets-connectes-exemples-piratages-insolites/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed:+Stuffi+(Stuffi+-+L%27actualit%C3%A9+des+objets+connect%C3%A9s

---

Pour la première fois, les

données d’un objet connecté sont utilisées en justice

Pour la première fois, les données d’un objet connecté sont utilisées en justice

Pour la première fois, les données récoltées par un #bracelet connecté sont exploitées dans une affaire judiciaire au Canada. Une démarche réalisée en même temps qu’un procès visant à déterminer les performances physiques d’une jeune femme blessée dans un accident. La première d’une longue lignée ?

Il y a 4 ans, une habitante de la ville de Calgary a été victime d’un accident de voiture qui aurait fortement diminué ses capacités physiques. De très sportive, la jeune femme est désormais limitée à des activités quotidiennes lambda : c’est la principale raison pour laquelle elle réclame aujourd’hui des dommages et intérêts. Et pour démontrer ses dires, ses avocats ont décidé de ne pas se baser uniquement sur une expertise médicale, mais également sur les données récoltées par un bracelet connecté Fitbit.

Une comparaison avec le reste de la population

L’étude des habitudes de la plaignante va durer plusieurs mois, pour avoir une base précise. Un bracelet de type Fitbit, appelé traqueur d’activité, mesure notamment le nombre de pas effectué au quotidien, les escaliers montés, ainsi que le sommeil. Les avocats ne comptent pas utiliser les données de manière brutes : elles seront traitées par Vivametrica, une entreprise spécialisée dans l’analyse d’informations récoltées par le biais d’appareils connectés. L’objectif est de positionner le comportement quotidien de la jeune femme vis-à-vis du reste de la population.

« Jusqu’à présent, nous nous basions uniquement sur l’interprétation clinique » explique l’avocat Simon Muller. « Désormais, nous cherchons à nous baser sur des périodes de temps plus longues qu’une seule journée, pour disposer de plus de données. » Au bout de plusieurs mois, l’avocat espère pouvoir démontrer que « le niveau d’activité de la victime a été revu à la baisse et compromis suite à sa blessure. » L’un des points bloquants de l’affaire se trouve dans le fait qu’il n’existe pas de données enregistrées avant l’accident : difficile, donc, de faire un avant et un après. Mais la démarche pose de tout de même question.

Le premier cas, mais pas le dernier ?

Si, dans le cas présent, la victime de l’accident se prête de bonne grâce à l’expérience, la situation pousse à réfléchir à l’usage des #objets connectés et des données liées dans le cadre d’affaires judiciaires. Selon Forbes, il s’agit de la première affaire en la matière, mais en cas de résultats concluants, la démarche pourrait se généraliser.

On peut notamment imaginer que, dans certains cas, par exemple liés à des litiges avec des assurances, ces dernières demandent à ce que des objets connectés soient utilisés pour fournir des preuves. Rick Hu, PDG de Vivametrica, explique que si les assurances ne peuvent pas elles-mêmes avoir de telles exigences, elles pourraient demander une ordonnance de tribunal pour récupérer des données stockées sur un service tiers. Une démarche qui, selon lui, n’est pas particulièrement différente de celle qui consiste à demander l’accès à des informations stockées sur Facebook, par exemple. D’ailleurs, le réseau social lui-même serait en train de plancher sur des applications en lien avec la santé : ce genre de réflexion n’est donc pas à négliger. (pour aller plus loin : Santé en ligne : Facebook veut-il jouer au docteur ?)

L’autre possibilité, c’est que l’utilisateur d’un dispositif de santé connecté fournisse sciemment l’accès aux données à un organisme d’assurance partenaire. L’exemple d’Apple HealthKit est intéressant sur ce point, puisque l’entreprise serait actuellement en discussion avec des organismes liés à la santé aux Etats-Unis, pour que ces derniers utilisent ses outils. Parmi eux, des compagnies d’assurances.

Des données au service de l’utilisateur… ou pas

Si les données récoltées par les appareils de mesure de soi permettent de se faire une idée sur ses habitudes et son état de santé et avoir un impact positif, elles peuvent également jouer en défaveur du porteur. Dans le cas d’une action en justice, la géolocalisation, les heures de sommeil et autres informations récupérées de manière automatique par un bracelet ou une montre connectée pourraient éventuellement confirmer ou réfuter les déclarations d’une personne.

Mais un tel procédé a également ses limites, car si les données sont évocatrices, il semble aujourd’hui difficile de démontrer qui portait vraiment l’appareil à un instant T. Une situation qui pourrait évoluer à l’avenir, avec le développement de systèmes biométriques plus performants, comme l’analyse de la sueur ou l’obligation d’utiliser une empreinte digitale pour activer un dispositif, par exemple. MasterCard teste depuis peu la reconnaissance du rythme cardiaque comme moyen de valider un paiement. De telles possibilités ne sont donc pas très éloignées de notre quotidien, de plus en plus lié à une collecte intensive de données personnelles.

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

Source :
http://www.clubic.com/mag/sport/actualite-739717-canada-donnees-recoltees-bracelet-connecte-utilisees-proces.html?estat_svc=s%3D223023201608%26crmID%3D639453874_748427012
par Audrey Oeillet

40 % des employés des grandes entreprises américaines utilisent leurs matériels personnels, mais…

40 % des employés des grandes entreprises américaines utilisent leurs matériels personnels, mais…

Selon une récente étude réalisée par Gartner, le BYOD (Bring Your Own Device) serait appliqué par 40 % des employés des grandes entreprises aux États-Unis. Mais un point majeur est à préciser : les entreprises sont loin d'être toutes au courant d'un tel usage.

Le BYOD tiré par les employés, non les employeurs

Dans mes précédents papiers publiés ces derniers mois, je suis souvent revenu sur le risque numéro un de ne pas appliquer de politique de BYOD : que les employés utilisent dans le dos de l'entreprise leurs propres appareils, multipliant ainsi les risques de fuites et de sécurité.

Or dans sa dernière étude, si Gartner montre que 40 % des employés des grandes entreprises sont concernés par le BYOD, il faut bien comprendre que seule une partie minoritaire d'entre eux le font sur demande de la société. Plus précisément, nous apprenons qu'un quart des employés concernés le font suite à un besoin express de leur entreprise.

Cela signifie donc que les 75 % restants le font sans qu'il n'y ait de demande particulière. Or seule la moitié des entreprises sont au courant de ces agissements. L'autre moitié de ces 75 % ignore donc totalement ces utilisations. Non seulement cela prouve et confirme que le BYOD aux États-Unis est plus tiré par les employés que par les entreprises elles-mêmes, mais aussi et surtout qu'une partie importante d'entre elles prennent des risques importants du fait de leur manque de politique de BYOD.

La statistique est un claque terrible dès lors que cela signifie qu'environ 15 % des employés de toutes les grandes entreprises américaines apportent et utilisent leurs smartphones, leurs tablettes ou leurs PC portables dans le dos de leurs dirigeant. Une donnée catastrophique qui doit donner des sueurs froides à bien des DSI.

On se rappellera d'ailleurs qu'en mai dernier, ce même Gartner indiquait qu'un quart des employés américains utilisant leurs propres appareils avaient dû faire face à des problèmes de sécurité en 2013. Et une partie non négligeable d'entre eux (27 %) l'ont précisé à leur hiérarchie… Un cauchemar en puissance pour les entreprises concernées.

L'ignorance, la pire des situations

Toujours du côté des rappels, deux anciennes études ces derniers mois ont montré que de très nombreuses entreprises n'ont toujours aucune politique de BYOD et que bien peu appliquaient un « Full BYOD ». Si l'on cumule ces informations avec le fait que certains employés confondent BYOD et liberté totale, le résultat ne peut mener qu'à des catastrophes.

« La clé pour disposer d'un appareil sécurisé est de vous assurer qu'il est bien géré » notait fort justement Gartner il y a quelques mois. Or comme je l'ai maintes fois répété, manquer de clarté avec ses employés sur le sujet si épineux des appareils mobiles personnels est un danger gigantesque pour l'entreprise. S'il n'y a pas de politique de BYOD, il faut se montrer ferme. Si une politique est mise place, il ne faut pas semer de doute dans l'esprit des employés et leur préciser les meilleurs comportements à avoir.

Notons enfin qu'il est intéressant d'apprendre que les tablettes tactiles, que ce soit en entreprise ou à la maison, servent avant tout… à jouer. Le jeu passe ainsi juste devant les réseaux sociaux et la lecture d'actualité. « L'importance des jeux sur des tablettes va de paire avec la relativement faible utilisation des appareils à des fins de travail » résume Gartner, qui explique donc que globalement, les entreprises ont un besoin encore assez limité de ce type d'appareils, bien plus utilisé à la maison.

Par Nil Sanyas pour Bring it on

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

Source :
http://www.zdnet.fr/actualites/40-des-employes-des-grandes-entreprises-americaines-utilisent-leurs-materiels-personnels-mais-39809253.htm

Une bague connectée pour mieux nous contrôler ?

	Une bague connectée pour mieux nous contrôler ?

Un anneau pour les contrôler tous ? Au Japon, plusieurs sociétés planchent sur le concept de bague connectée, avec l'ambition de proposer reconnaissance de mouvements, clé sans contact, porte-monnaie électronique et système d'alerte au sein d'un seul et même petit appareil en forme de bijou.

Lunettes, montres ou vêtements, la tentation est grande de conférer des capacités informatiques à tous les objets du quotidien et beaucoup d'acteurs courent après la vision d'un accessoire à tout faire, fonctionnant en adéquation avec un smartphone. Parmi les différentes intégrations possibles, plusieurs se sont déjà intéressés à la bague. Un anneau se fait aisément oublier tout en restant accessible, et le doigt reste encore l'un des meilleurs moyens qu'a trouvés l'homme pour interagir avec son environnement. Jusqu'ici, les premières tentatives en matière d'anneaux connectés se sont toutefois révélées décevantes, en grande partie parce que les interactions proposées étaient à trop faible valeur ajoutée…

La donne va-t-elle changer ? La miniaturisation des composants permet désormais d'aller plus loin, comme en témoigne le projet développé par la start-up japonaise 16Lab. Celle-ci planche sur un anneau de titane qui, à terme, servirait aussi bien à la saisie de texte et de messages qu'à ouvrir la porte de sa voiture, payer ses courses ou alerter lors de la réception d'un message. Dans sa version actuelle, encore en cours de développement, la bague embarque deux petites surfaces tactiles qu'il suffit d'actionner du pouce pour « réveiller » l'appareil, qui émet alors une vibration de confirmation. Au centre de l'anneau, on trouve un composant développé par ALPS, qui propose, au sein d'une enveloppe de seulement 6 mm² une liaison Bluetooth 4.0, un accéléromètre et une boussole. Cette puce permet donc d'assurer la liaison avec le smartphone de l'utilisateur, mais aussi de mesurer la position de sa main dans l'espace ainsi que les mouvements de cette dernière.
D'après son concepteur, le dispositif est suffisamment précis pour envisager sérieusement d'écrire à main levée, en traçant simplement dans les airs les caractères. ALPS propose d'ailleurs des scénarios dans lesquels un démonstrateur contrôle une interface de télévision ou de téléphone grâce à des gestes capturés non pas par une caméra, mais par ce sensor network module.
16Lab admet toutefois sans ambages que la simple reconnaissance de mouvements ne justifierait sans doute pas l'achat et le port d'une telle bague. Il fallait donc chercher à enrichir cette dernière, ce qui passe par l'ajout de composants supplémentaires. Rapidement, le NFC s'est imposé comme une piste à étudier : les communications en champ proche, en plein essor, permettent en effet d'utiliser l'anneau comme une clé, capable d'actionner une serrure compatible, mais aussi comme un porte-monnaie électronique, à l'instar des déploiements en cours dans l'univers de la téléphonie mobile. Plutôt que de sortir son téléphone de sa poche, on n'aurait donc qu'à poser la main sur une surface dédiée au paiement. Dans tous ces scénarios, la bague fonctionne comme une interface rapprochée de la main, l'intelligence et la communication restant gérés au niveau du téléphone.
Alors, la bague sera-t-elle le parfait « raccourci » ? En attendant que le marché en décide, une autre start-up japonaise a justement fait de cette notion son slogan. Logbar Inc. développe également une bague à tout faire, avec une proposition de valeur similaire à celle qu'avance 16Lab. Sa bague s'appelle pour l'instant simplement Ring, et les développements reposent sur des fonds levés grâce au financement participatif. Bouclée en début d'année, la campagne Kickstarter de Logbar a débouché sur une enveloppe globale de 880 000 dollars, alors que la société avait fixé son objectif à 250 000 dollars. Le concept de bague connectée semble donc ne pas laisser indifférent. Reste à voir dans quelle mesure ces premiers essais seront transformés.

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

Source :
http://www.clubic.com/technologies-d-avenir/ceatec/actu-une_bague_connectee_pour_les_controler_tous-731899.html

---

Après le BYOD, voici le WYOD

Après le BYOD (bring your own device), voici le WYOD

En ce mois de septembre, la principale nouvelle dans le secteur high-tech a été de loin l'annonce de l'Apple Watch. Disponible au début de l'année prochaine, la montre pourrait faire exploser le marché des produits vestimentaires connectés. De quoi développer le Wear Your Own Device (WYOD).

Un phénomène qui pourrait bien se généraliser

La future Apple Watch va-t-elle connaître le succès ? Difficile à dire pour le moment. Ce que nous savons par contre, c'est que de nombreux constructeurs et fabricants misent sur les objets vestimentaires connectés / intelligents. Que ce soit les bracelets sportifs de Nike et Fitbit ou encore les montres de Sony, Samsung, Motorola et bientôt Apple, la mode est au connecté.

En entreprise ou encore dans les établissements scolaires, nous connaissions déjà le BYOD (Bring Your Own Device), le BYOS (Bring Your Own Software) ou encore le BYOPC (Bring Your Own PC). Voici donc le WYOD, Wear Your Own Device. Bien entendu, un tel phénomène est loin d'être encore aussi grand que l'utilisation du smartphone en entreprise. Il n'empêche qu'il faut s'y préparer, car les logiques sont les mêmes.

Dorénavant ou tout du moins d'ici quelques mois ou années, il faudra donc veiller à ce que les montres connectées ne deviennent pas problématiques pour la sécurité des données sensibles de la compagnie. Et nous ne parlons même pas des lunettes connectées de Google qui peuvent être pires encore.

Bientôt invisibles à nos yeux

Les montres connectées ont de cela de spéciales que si l'on n'y prend pas garde, on ne la différenciera pas des autres montres, et donc on ne la remarquera pas. Même logique pour les vêtements connectés ou même les perruques connectées (oui oui). Bien plus difficiles à vérifier qu'un smartphone, une tablette tactile et bien entendu un ordinateur, tous ces nouveaux et futurs produits peuvent devenir le cauchemar des patrons et des DSI s'ils ne prennent pas les dispositions adéquates.

Comme le notait il y a quelques Kevin Noonan, analyste pour Ovum, les produits connectés comme les montres ou les lunettes pouvaient à l'époque paraître bizarres et étaient immédiatement identifiables. Aujourd'hui à force de les voir et de les côtoyer, ils risquent d'être invisibles à nos yeux.

Que faire ? Les interdire ?

Dans certains lieux vraiment sensibles, ce serait peut-être la solution la plus simple. Néanmoins, on a déjà vu que de nombreuses entreprises interdisaient le BYOD, ce qui n'empêchait pas les employés d'apporter leurs propres appareils, en le cachant aux yeux de leurs dirigeants. Une véritable catastrophe qu'il convient d'éviter pour les objets connectés.

Le contrôle avant tout

Plutôt qu'interdire, mieux vaut donc disposer d'une véritable politique propre à tous les appareils, y compris donc les objets et vêtements intelligents et connectés. Mieux vaut ainsi avoir le contrôle et la mainmise sur ce type de produits qu'en ignorer la présence, ce qui est la pire des situations.

Qui plus est, comme pour les smartphones, les entreprises doivent en tirer profit, que ce soit pour communiquer avec leurs employés ou encore trouver un moyen d'exploiter ces objets vis-à-vis des clients. Après tout, il s'agit de produits souvent compatibles avec d'autres appareils, et il n'est pas rare qu'un important espace de stockage en ligne (cloud) l'accompagne. Si cela peut devenir un problème, cela peut donc surtout être un atout.

Il faut de plus comprendre qu'à l'heure actuelle, il n'existe pas de solutions spécifiques de sécurité pour ces objets. Stephen Brown, directeur de la gestion des produits mobiles chez Landesk, expliquait par exemple en avril dernier qu'en réalité, la première préoccupation vis-à-vis de ces produits n'est pas la sécurité mais le respect de la vie privée. C'est en particulier le cas des lunettes connectées, mais pas uniquement. Est-ce que ces appareils enregistrent constamment voire à notre insu ? Répondre à ces questions est déjà un point fondamental.

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

Source :

http://www.zdnet.fr/actualites/apres-le-byod-voici-le-wyod-39806705.htm

Par Nil Sanyas

Baidu va lancer des baguettes mesurant la qualité de la no urriture

Baidu va lancer des baguettes mesurant la qualité de la nourriture

Après les scandales du lait contaminé, de l'huile recyclée ou de la viande de renard, vous n'avez pas confiance dans la sécurité de vos aliments en Chine ? Baidu affirme avoir la réponse.

Le géant chinois des moteurs de recherche a dévoilé mercredi un nouveau dispositif baptisé « baguettes intelligentes », ou Kuaisou en chinois, dont il dit qu'elles peuvent détecter des huiles contenant des niveaux de contamination les rendant insalubres. Lors de la conférence annuelle sur la technologie de l'entreprise, Robin Li, le PDG de Baidu a brièvement présenté le nouveau produit, qu'il a appelé « une nouvelle façon de sentir le monde ».

« Dans l'avenir, grâce à Baidu Kuaisou, vous serez en mesure de connaître l'origine de l'huile et de l'eau et des autres aliments, s'ils sont devenus mauvais et quels nutriments ils contiennent », a déclaré M. Li dans un discours prononcé mercredi.

Une vidéo postée par la société montre comment utiliser le produit, qui est relié à une application smartphone. Dans une expérience, les baguettes ont été présentées en train de tourbillonner dans de l'huile d'olive, avec le smartphone affichant ensuite la mention « bonne ». Dans une autre, les baguettes ont donné une mention « mauvaise » après avoir été plongées dans de l'huile de friture recyclée.
Selon Baidu, les baguettes mesurent la fraîcheur de l'huile de cuisson. Les baguettes seront également en mesure de mesurer les niveaux de pH et de la température et de calories. Le prix de ces baguettes n'a pas encore été annoncé, et la société a ajouté que le produit n'est pas encore prêt pour la production de masse.

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

Source :
http://french.peopledaily.com.cn/n/2014/0905/c31357-8779044.html