Apple condamné à créer un firmware spécial pour le FBI

Apple condamné à créer un firmware spécial pour le FBI

Le tribunal de Californie a ordonné à Apple de fournir au FBI les moyens technologiques pour accéder au contenu en clair d'un téléphone utilisé par l'auteur de la tuerie de San Bernardino. Apple ne devra pas déchiffrer lui-même, mais supprimer une protection d'iOS 8 qui permet d'éviter les tentatives d'accès par force brute.

À la demande du FBI, un tribunal de Californie a ordonné mardi à Apple de fournir une « assistance technique raisonnable » aux enquêteurs de la police fédérale, qui cherchent à accéder au contenu en clair du téléphone de l'auteur de la tuerie de San Bernardino, Syed Rizwan Farook. Cette attaque terroriste avait fait 14 morts le 2 décembre 2015.

Estimant que ses principes de protection de la confidentialité des données de ses clients étaient indérogeables, Apple avait refusé d'apporter son concours actif au déchiffrement de l'iPhone 5C du suspect, dont le contenu est illisible tant qu'il n'est pas débloqué. La firme de Cupertino se dit de toute façon incapable de déchiffrer le contenu, puisque la clé est générée et stockée sur le téléphone lui-même, et qu'il n'a donc pas davantage la main que les experts en cryptologie des services de renseignement américains.

FAIRE SAUTER LA PROTECTION APRÈS 10 TENTATIVES INFRUCTUEUSES

Mais le FBI a obtenu de la justice qu'Apple l'aide autrement. L'entreprise dirigée par Tim Cook devra fournir une mise à jour du firmware, qui fasse sauter la protection du téléphone contre les tentatives abusives d'accès (il n'est pas précisé comment une telle mise à jour pourrait être installée). En effet le suspect avait activé sur son smartphone la fonctionnalité de sécurité d'iOS qui fait qu'après 10 saisies erronées de codes PIN, le contenu du téléphone est automatiquement effacé.

Apple devra fournir au FBI le moyen de modifier le système iOS sur l'iPhone 5c de Farook, pour que la fonction d'effacement du contenu du téléphone ne soit pas activée. Le FBI espère ainsi opérer par force brute pour deviner le mot de passe à force de tentatives répétées, et ainsi gagner l'accès au contenu en clair du téléphone.

APPLE DEVRAIT FAIRE APPEL

Par ailleurs, toujours dans le même objectif, Apple devra fournir au FBI le moyen de tester rapidement plusieurs combinaisons, pour éviter d'avoir à construire un robot qui tape lui-même lentement les codes les uns après les autres. Avec quatre chiffres pour le code PIN, 10 000 combinaisons sont possibles.

Selon la BBC, Apple devrait toutefois faire appel de la décision. L'entreprise craint certainement que sa coopération soit interprétée comme la fourniture d'un backdoor à l'administration américaine, qui minerait la confiance qu'ont les clients dans la protection apportée par Apple.

« Apple n'a jamais collaboré avec une quelconque autorité publique, de quelque pays que ce soit, afin de créer une « porte dérobée » dans ses produits ou services », peut-on lire sur le site officiel d'Apple. « Sur les appareils sous iOS 8 ou ultérieur, vos données personnelles sont protégées par votre code. En effet, pour ces appareils, Apple ne peut répondre aux demandes d'extraction de données iOS émanant des autorités : les fichiers à extraire sont protégés par une clé de chiffrement liée au code de l'utilisateur, auquel Apple n'a pas accès ».

… [Lire la suite]

Réagissez à cet article

Source : *Apple condamné à créer un firmware spécial pour le FBI – Politique – Numerama*

Toutes les versions de Windows touchées par une faille critique

Toutes les versions de Windows touchées par une faille critique

---

Toutes les versions de Windows, dont Windows 10, sont affectées par une faille critique pour laquelle un correctif est disponible. La vulnérabilité permet d'exécuter arbitrairement du code.

Le dernier Patch Tuesday de Microsoft est léger en correctifs critiques, mais une faille majeure cependant affecte l'ensemble des versions supportées de Windows.

Dans son bulletin de sécurité mensuel, Microsoft informe les utilisateurs de la nécessité de patcher immédiatement une vulnérabilité sérieuse au niveau de la façon dont le système d'exploitation gère certains fichiers. Toutes les versions de Windows sous support sont concernées, de Windows Vista à Windows 10.

La faille (MS16-013) pourrait permettre à un attaquant d'exécuter arbitrairement du code comme l'utilisateur authentifié sur la session Windows. Les risques sont donc accrus pour les utilisateurs avec un compte doté des droits administrateur.

Autres vulnérabilités dans Office, IE et Edge

Pour réaliser l'attaque, le pirate doit amener l'utilisateur à ouvrir un fichier Journal spécialement forgé. Il pourra ainsi exécuter des programmes, supprimer des données et même créer de nouveaux comptes avec tous les droits sur le poste Windows.

Windows Server 2016 Tech Preview 4 est également affecté par la vulnérabilité et le correctif doit donc aussi être déployé sur ces configurations. Microsoft précise toutefois n'avoir à ce jour détecté aucune exploitation de cette faille Windows.

A noter que l'éditeur a publié trois autres correctifs pour des vulnérabilités critiques de Windows et Office.

MS16-012 corrige une faille permettant à un attaquant d'exécuter du code en exploitant un fichier PDF compromis. Les utilisateurs de Windows 8.1 et Windows 10 sont principalement touchés. Le problème de sécurité a été signalé à l'éditeur par un tiers et ne ferait pas l'objet d'attaques.

MS16-015 remédie à plusieurs failles de corruption mémoire dans Microsoft Office. Elles autorisent des attaques par le biais de fichiers Office malveillants. Leur exploitation permet d'obtenir des droits équivalents à ceux de l'utilisateur de la session ouverte.

MS16-022 corrige enfin de nombreuses vulnérabilités d'Adobe Flash Player dans Windows 8.1 et versions suivantes de l'OS Microsoft.

L'éditeur diffuse par ailleurs un patch cumulatif pour Internet Explorer (MS16-009) et le nouveau navigateur de Windows 10, Microsoft Edge (MS16-011). Les différentes failles ne feraient l'objet d'aucune exploitation avant la diffusion des correctifs, toujours selon la firme de Redmond… [Lire la suite]

Réagissez à cet article

Source : *Toutes les versions de Windows touchées par une faille critique*

Des données personnelles de développeurs trouvés dans des caméras de surveillance

Des données personnelles de développeurs trouvés dans des caméras de surveillance

---

Gmail, Dropbox et comptes FTP, voici ce qu'ont laissé des développeurs dans les entrailles des caméras sur lesquelles ils travaillaient. Des informations personnelles qui montrent le manque de vigilance de ces techniciens, ayant utilisés leurs comptes privés lors du développement de ces caméras… Une affaire qui pourrait faire tâche sur les CV de ces indélicats !

Selon un article de Forbes, des développeurs ayant travaillé sur la création du software pour les caméras Motorola Focus 73 ont fait preuve d'un manque de vigilance flagrant au moment de finaliser leur travail, juste avant la commercialisation de ce modèle. Des experts de « Context Information Security » sont parvenus à accéder aux entrailles des caméras, et on pu en extraire plusieurs informations suprenantes. Les développeurs y avaient laissé trainer leurs identifiants Gmail, Dropbox et FTP d'entreprise.
Les caméra, facilement piratées et contrôlables à distance pour quiconque ayant un minimum de connaissance dans le domaine, ont apporté la preuve de la négligence de ces développeurs, comma l'a expliqué le responsable de Context Information Security :
Les comptes laissés dans le firmware sont apparus comme étant des comptes de développeurs partagés, utilisés pour recevoir les alertes de mouvement et les extraits de vidéo pour leurs tests. Nous n'avons pas accédé à ces comptes pour des raisons légales, mais nous avions tout ce qu'il nous fallait pour le faire. (…) On ne s'attend pas à ce qu'une entreprise de développement utilise ce type de comptes pour ce genre d'activité et ils n'auraient certainement pas du être laissés dans le firmware final.
Un constat d'autant plus affligeant que les mots de passe utilisés pour la sécurité des caméras et ces comptes Gmail sont plus que décevants : « 000000 » ou « 123456 ».

Réagissez à cet article

Source : *Gmail : des données personnelles de développeurs trouvés dans des caméras de surveillance – 1001Web*

Wi-Fi dans les TGV : il faudra finalement attendre 2017

Wi-Fi dans les TGV : il faudra finalement attendre 2017

Une connexion gratuite devait être proposée sur certaines lignes dès le milieu de cette année, mais la SNCF et ses partenaires opérateurs semblent (encore) prendre du retard.

La présence d'un Wi-Fi fonctionnel et rapide dans les TGV relève de plus en plus de l'Arlésienne. En octobre 2014, Axelle Lemaire, la secrétaire d'Etat au Numérique s'agaçait comme beaucoup de l'absence de cette technologie. Alors que de nombreuses compagnies ferroviaires dans le monde proposent ce service, aujourd'hui considéré comme une commodité, le fleuron de la SNCF reste aveugle et muet. Alors bien sûr, il est toujours possible d'accrocher un réseau 3G ou 4G. Mais à grande vitesse, la qualité de service est rarement au rendez-vous et les coupures fréquentes.

Face à la pression, la SNCF annonçait en février 2015 que le Wi-Fi gratuit serait opérationnel dans les trains, à partir de mi-2016. La ligne TGV Paris-Lyon sera équipée fin 2016. La ligne TGV Est et Paris-Bordeaux seront couvertes mi-2017. « Le dispositif sera testé et opéré de manière commerciale dès juin 2015. Il faut ensuite le temps d'équiper toutes les lignes », déclare Frédéric Burtz, responsable de l'innovation à la direction digitale SNCF.

Manque de bol, il faudra encore attendre un peu. « On va mettre en œuvre des systèmes dans les trains pour permettre d'avoir le Wi-Fi, en commençant par les trains à grande vitesse. En 2017, vous allez commencer à avoir ça », a indiqué sur BFM Business, Barbara Dallibard, la directrice générale de la branche SNCF voyageurs. Les lignes classiques suivront.

La 4G à la rescousse

Quelques mois supplémentaires de patience… Rappelons que techniquement, la SNCF n'utilisera plus le satellite pour acheminer les données mais la 4G aujourd'hui largement déployée. Ensuite, le W-Fi prendra le relai à l'intérieur des rames à grande vitesse. « Le choix du satellite, que nous avons fait il y a 5 ans n'était pas le meilleur. Le principal problème est son coût, d'environ 1 million d'euros par rame. Nous avons réalisé des essais notamment dans l'Est de la France mais de l'avis des clients, c'était superbof. Aujourd'hui on en tire les leçons », expliquait il y a quelques mois Guillaume Pépy, p-dg de la SNCF.

Pour mener à bien le projet, la SNCF s'attache donc avec les opérateurs mobiles à améliorer la couverture mobile 2G, 3G, 4G dans les trains classiques mais aussi les TGV. Il s'agit de déterminer quelles sont les zones blanches ou grises qui provoquent coupures et perte de réseau. « C'est la fin du renvoi de balle entre les opérateurs et la SNCF », a promis Guillaume Pépy.

Au total, la SNCF va consacrer un budget de 150 millions d'euros par an, au cours des trois ans qui viennent. Cela coûte « très cher en raison de la vitesse des trains et ce qui est fait sur Thalys (où les TGV sont équipés du Wi-Fi) est difficilement généralisable », précisait Axelle Lemaire. Le coût est évalué à 350.000 euros par rame. Reste la question du modèle économique : ce Wi-Fi gratuit sera-t-il financé par la publicité ?

Rappelons qu'en 2010, la société nationale annonçait fièrement que les usagers du TGV Est (12 millions de voyageurs par an) seraient les premiers à pouvoir disposer (en 1ère et 2ème classe) d'un accès Wi-Fi via le service Box TGV (facturé 4,99 euros par heure ou 9,99 euros pour toute la durée de leur voyage).

« On a fait la bêtise de le faire nous-mêmes », avait indiqué Guillaume Pepy. « Il y a dix ans, on a investi 30 ou 50 millions d'euros pour mettre le wifi dans le TGV Est et Thalys. Aujourd'hui, cet investissement est perdu ».

Réagissez à cet article

Source : *Wi-Fi dans les TGV : il faudra finalement attendre*

2017

Astuces pour une meilleure gestion de l’e-réputation – Annuaire +1 Annuaire +1

Astuces pour une meilleure gestion de l’e-réputation – Annuaire +1 Annuaire +1

L’e-réputation ne concerne plus les entreprises et les organisations de marque. Tout le monde peut disposer d’une image sur internet. En effet, avec ou sans permission, des sujets peuvent parler d’une personne notamment via des discussions, des images ou des vidéos. Or, dans ces discours et mauvaises appréhensions ne restent pas dans le monde virtuel. En fait, cela peut impacter la vie quotidienne, détruire des relations et même des carrières professionnelles. Heureusement que ce n’est pas une fatalité. L’e-réputation peut être géré et même utilisé à bon escient. Comment faire ?

Ajouter de l’importance à son image
Quels que soient les documents ou fichiers qu’il faut mettre en ligne, il faut les prendre en conscience. CV, photos ou des commentaires faits sur les plateformes sociales, ils contribuent tous à l’e-réputation d’une personne. Bien que quelque peut inévitable, ces contenus sont les vitrines d’une personne, alors autant qu’elle lui ressemble. La meilleure façon est de ne jamais négliger son e-réputation. Tout ce qui est sur internet reste sur internet ! Telle est la règle.

Avoir un bon aspect de l’état des lieux
Le mieux est d’évaluer son e-réputation le plus tôt possible. C’est très simple, il n’y a pas besoin de faire appel à une agence e-réputation pour avoir une idée de son e-réputation. Pour ce faire, il suffit de taper une requête sur la barre de recherche des moteurs de recherche. De porter une analyse sur au moins les deux premières pages (au lieu de rester sur la première). La suite consiste à vérifier s’ils coïncident avec l’image voulue, s’ils peuvent être lus publiquement…

Penser à son avenir
Les réseaux sociaux constituent en fait une bonne alternative pour constituer un réseau professionnel. Il y a également les sites dédiés avec qui, il faut prendre à l’avance des précautions. En fait, pour une candidature donnée les recruteurs ne s’arrêtent pas sur leur site. Ils peuvent étendre (et c’est bien compréhensible) leur recherche sur les autres plateformes sociales et même sur la totalité des moteurs de recherche.
De même pour les amis Facebook par exemple, ce sont les personnes les plus susceptibles de devenir un danger pour un internaute. La situation n’est pas toujours délibérément provoquée, par contre une identification sur une photo relatant une soirée vertigineuse entre élève et prof employer et employeur ne fait pas bon ménage. Pour éviter cette situation, il est indispensable de bien maitriser les paramètres (ce que peu de gens font également).
Après les constatations, les actions ! Quelle que soit la plateforme, il faut toujours vérifier les paramètres. Entreprendre des petites actions peut permettre à aider des problèmes plus graves. Comme le classement des amis par rapport au lien et relation partagée. Par exemple pour Facebook, cliquer sur rubrique confidentialité et choisir option « examiner les publications dans lesquelles vos amis vous identifient avant qu’elles n’apparaissent sur votre journal ».

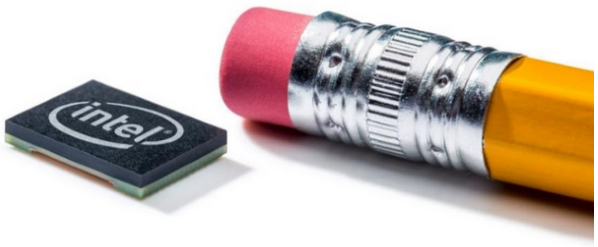
Apparaitre ou ne pas apparaitre ?
Telle est la question ! En premier lieu, demander le droit de ne faire aucune publication sur internet ! C’est toujours possible à faire, mais il faut prendre en compte les autres internautes qui peuvent toujours influer l’e-réputation. L’inconvénient réside alors dans le fait qu’il n’y aura que du mauvais contenu à l’encontre de la personne en question. Un autre inconvénient est que les recruteurs n’aiment pas trop les candidats qui sont trop discrets sur le web.
Du coup, autant prendre le mal par les cornes ! Avoir le pouvoir de supprimer les contenus indésirables en contactant Google ou en faisant appel à une agence e-réputation.

Réagissez à cet article

Source : *Astuces pour une meilleure gestion de l’e-réputation – Annuaire +1 Annuaire +1*

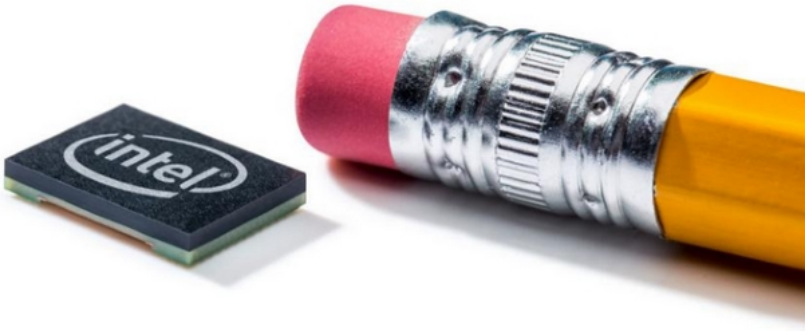
Intel veut encore et toujours que vous enfiliez un

ordinateur

	Intel veut encore et toujours que vous enfiliez un ordinateur

Si les objets connectés connaissent des fortunes variables, Intel creuse le sillon des wearables et met à disposition des constructeur son module Curie, un ordinateur miniature équipé de capteurs de mouvements.

Intel annonce être prêt à livrer Curie, un petit ordinateur qui pourrait aider les wearables dans leur quête de minceur. Le PDG d'Intel Brian Krzanich a annoncé lors de la keynote de la société au CES que Curie serait disponible au premier trimestre de cette année, et couterait moins de 10 dollars l'unité.



L'ordinateur Curie d'Intel, destiné au marché des wearables. (Source : Intel)

Présenté l'an passé à Las Vegas, Curie est un micro ordinateur portable qui tient littéralement dans un bouton de veste. Le PDG d'Intel en avait fait la démonstration lors de la keynote de l'édition précédente. Le tout petit ordinateur Curie est un enjeu capital pour Intel et le secteur des wearables. Protocole de communication Bluetooth, accéléromètre, gyroscope ; Intel assure que Curie possède également une batterie de longue durée de la taille « d'une pièce de monnaie ». De quoi assurer un fonctionnement constant.
Le module Curie est équipé également d'un processeur 32-bit Intel Quark, de 384ko de mémoire flash, de 80ko de SRAM et de capteurs DSP.

Diminuer la taille des équipements

De quoi aussi diminuer sensiblement la taille des équipements électroniques qui équipent montres et bijoux connectés, mais aussi proposer des fonctionnalités de suivi de la santé des utilisateurs sur des vêtements sans les déformer pour autant. Surtout, le coût additionnel de ces produits connectés serait modique.
A titre d'exemple, le PDG d'Intel a présenté sur scène deux cyclistes BMX dont la selle et le guidon de leur vélo sont équipés d'un module Curie rapporte Technology Review. Leurs cascades réalisées en direct étaient ainsi analysées en temps réel et retransmises sur un écran géant. Et si Intel se concentre si fort sur le marché des wearables, c'est qu'il s'agit pour lui d'un enjeu majeur pour enfin trouver grâce aux yeux du marché de la mobilité.

Un marché en croissance et déjà embouteillé

A noter qu'Intel est loin d'être le seul a se positionner sur le segment des composants pour wearables.Samsung vient par exemple de présenter un processeur. Côté marché, la baisse des prix provoque un certain engouement des consommateurs. L'Idate prévoit que 123 millions de wearables seront vendus en 2018.
En France, Cityzen Sciences aurait levé 100 millions d'euros en 2015 pour développer des capteurs à destination des vêtements.

Réagissez à cet article

Source : *Intel veut encore et toujours que vous enfiliez un ordinateur*

Critical Infrastructure Sectors of Nations facing cybercrime

Critical Infrastructure Sectors of Nations facing cybercrime

There are 16 critical infrastructure sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Presidential Policy Directive 21 (PPD-21): Critical Infrastructure Security and Resilience advances a national policy to strengthen and maintain secure, functioning, and resilient critical infrastructure. This directive supersedes Homeland Security Presidential Directive 7.
PPD-21 identifies 16 critical infrastructure sectors:

Chemical Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Chemical Sector.

Commercial Facilities Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Commercial Facilities Sector.

Communications Sector
The Communications Sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government.

Critical Manufacturing Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Critical Manufacturing Sector.

Dams Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Dams Sector. The Dams Sector comprises dam projects, navigation locks, levees, hurricane barriers, mine tailings impoundments, and other similar water retention and/or control facilities.

Defense Industrial Base Sector
The Defense Industrial Base Sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

Emergency Services Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Emergency Services Sector. A system of prevention, preparedness, response, and recovery elements, the Emergency Services Sector represents the nation's first line of defense in the prevention and mitigation of risk from terrorist attacks, manmade incidents, and natural disasters.

Energy Sector
The U.S. energy infrastructure fuels the economy of the 21st century.

Financial Services Sector
The Department of Treasury is designated as the Sector-Specific Agency for the Financial Services Sector.

Food and Agriculture Sector
The Department of Agriculture and the Department of Health and Human Services are designated as the Co-Sector-Specific Agencies for the Food and Agriculture Sector.

Government Facilities Sector
The Department of Homeland Security and the General Services Administration are designated as the Co-Sector-Specific Agencies for the Government Facilities Sector.

Healthcare and Public Health Sector
The Department of Health and Human Services is designated as the Sector-Specific Agency for the Healthcare and Public Health Sector.

Information Technology Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Information Technology Sector.

Nuclear Reactors, Materials, and Waste Sector
The Department of Homeland Security is designated as the Sector-Specific Agency for the Nuclear Reactors, Materials, and Waste Sector.

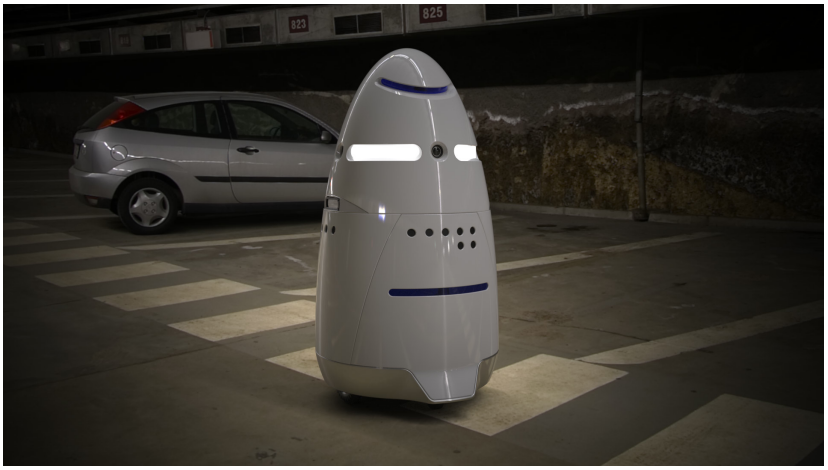
Transportation Systems Sector
The Department of Homeland Security and the Department of Transportation are designated as the Co-Sector-Specific Agencies for the Transportation Systems Sector.

Water and Wastewater Systems Sector
The Environmental Protection Agency is designated as the Sector-Specific Agency for the Water and Wastewater Systems Sector.

Réagissez à cet article

Source : *Critical Infrastructure Sectors | Homeland Security*

Des robots sentinelle contre le crime dans la Silicon Valley



Des robots sentinelle contre le crime dans la Silicon Valley

Une start-up de Palo Alto, Knightscope, déploie dans les rues de la Silicon Valley des robots pour lutter contre le crime.

Non, ce n'est pas le pitch d'un nouveau film d'anticipation ou de science-fiction, mais bien une réalité d'aujourd'hui. Ces robots, les Knightscope K5 Security Robot, sont déjà dans les rues et patrouilles pour dissuader ou récolter des données.

Bardés de capteurs

Ces robots ne sont pas armés, ce qui pourrait arriver aux États-Unis vu les lois en vigueur dans certains états. Par contre, ils sont équipés de multiples capteurs qui leur permettent de voir à 360°, d'entendre, de sentir et de ressentir. Le système de guidage et de pilotage est le même que celui des Google Car.

Ils mesurent un peu plus d'un mètre cinquante, pèsent près de 137 kg, sont de forme ovoïde et de couleur blanche. Ils téléchargent en temps réel ce qu'ils voient et entendent et sont conçus pour réagir à des bruits significatifs comme le bris de glace ou des coups de feu. Si cela se produit, le K5 enregistre alors beaucoup d'informations sur son environnement comme la géolocalisation, photos, vidéos, plaques d'immatriculation des véhicules à proximité et même les visages des personnes proches dans l'éventualité d'une reconnaissance faciale.

Les K5 peuvent donner l'alerte aux autorités compétentes en cas de « détection » crime via une plateforme Internet accessibles aux forces de l'ordre.

Le K5 est déjà en fonction dans des centres commerciaux ou des campus universitaires comme assistant de sécurité et, selon Stacy Stephens cofondatrice de Knightscope, ils ont un très bon accueil et reçoivent même des câlins.

Le business model de Knightscope pour les K5 est MaaS, Machine-as-a-Service, et coûte 4 500 dollars par mois, pour un service 24h/24 et 7jr/7 soit 6,25 dollars de l'heure.

Toutes ressemblances avec Dalek de Docteur Who est fortuite…

Réagissez à cet article

Source : *Des robots contre le crime dans la Silicon Valley – Ere Numérique*

Carte de paiement sans contact – Le client n’est pas toujours roi

Carte de paiement sans contact – Le client n’est pas toujours roi

---

Refuser les cartes bancaires équipées du paiement sans contact n’est pas toujours simple. Un client du Crédit agricole l’a appris à ses dépens.

En avril 2015, un adhérent de l’UFC-Que Choisir de Senlis saisit l’association locale de ses difficultés avec son agence du Crédit agricole de Rixheim (68). Celle-ci lui a adressé en renouvellement une carte bancaire Visa munie de la fonction paiement sans contact. Ayant lu dans Que Choisir que cette fonction n’était pas sans faille, ce consommateur demande à sa banque le remplacement de sa carte par une même carte Visa mais sans cette nouvelle fonction. Refus de son agence, puis de la direction régionale du Crédit agricole qui affirme que c’est impossible et lui propose en échange soit une carte Visa avec débit différé, soit un autre type de carte bancaire. Pas d’accord, le particulier fait part de ce blocage à l’association locale de l’UFC-Que Choisir de Senlis.

Client à la porte

L’intervention de cette dernière auprès de la banque n’aura pas plus de succès. Face à un tel refus, elle saisit la Cnil (Commission nationale de l’informatique et des libertés) au motif que le Crédit agricole viole une de ses recommandations qui impose aux banques d’offrir à leurs clients la possibilité de refuser la fonction paiement sans contact.

La Cnil rejette la plainte de l’association locale, déclarant ne pas pouvoir imposer aux banques un changement de carte à l’identique mais rappelle que le particulier a la possibilité de faire désactiver la fonction.

Fort de cette réponse, le consommateur demande à son agence cette désactivation.

Pour toute réponse, la banque a mis son client à la porte, le sommant de restituer tous ses moyens de paiement. La Cnil a été avertie d’un tel comportement.

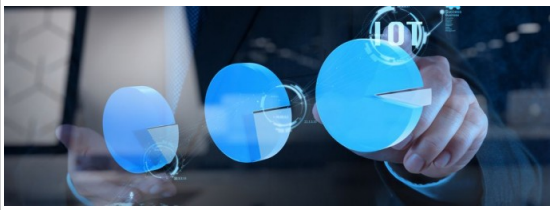
Réagissez à cet article

Source : *Carte de paiement sans contact – Le Crédit agricole a la main leste – UFC Que Choisir*

L’Internet des objets boostera-t-il l’Europe ?

	L’Internet des objets boostera-t-il l’Europe ?

En plein CES de Las Vegas, AT Kearney vient de livrer une version rafraîchie de son étude sectorielle sur la high-tech en Europe avec un focus #IoT.



L'Internet des objets donnera-t-il un nouveau souffle au secteur high-tech en Europe ? AT Kearney a publié un focus dans ce sens qui montre tout le potentiel…s'il est bien exploité.

En pleine effervescence du CES organisé à Las Vegas, le cabinet de consulting d'origine américaine vient de présenter à Paris la troisième version de son étude sur les nouvelles technologies en Europe sous l'angle de l'IoT

C'est une véritable opportunité de croissance sur les 10 prochaines années, estime Hervé Collignon, Partner d'AT Kearney, expert en TMT (télécoms, médias et technologies) et co-auteur du rapport.

Ce potentiel économique est estimé à près de mille milliards d'euros d'ici 2025. Il pourrait correspondre à 7 points de PIB à cet horizon.

Et les start-up comme Sigfox, Netatmo ou Withings et les groupes industriels français ont une carte à jouer. Ils ont pris position sur le marché des objets connectés dans le BtoC et le BtoB (historiquement via le M2M).

Dressons d'abord le tableau des perspectives présumées gigantesques de cet Internet des objets, qui va permettre « l'interconnexion du monde physique en facteur 10 par rapport à l'Internet phase 1 ».

Entre les technologies exponentielles (capteurs, bande passante, hardware, stockage & cloud), la population connectée (3 milliards de personnes en 2015), les effets réseaux (peering, IPv6, plateformes, interopérabilité…) et l'essor du big data, tous les ingrédients sont réunis pour assister à une « nouvelle révolution » qui va toucher tous les secteurs d'activité, estime Hervé Collignon.

A l'horizon 2025, le marché des solutions IoT en Europe (hors fabrication des objects connectés) est évalué à 80 milliards d'euros. Les intégrateurs de systèmes (IBM, Accenture, Atos…) remporteraient la plus grosse part du gâteau : plus d'un quart du business généré (22 milliards d'euros), devant les fournisseurs de services et de plateformes (le club GAFA et les opérateurs télécoms) qui pourraient en tirer un business de 18 milliards d'euros….

On retrouverait les opérateurs dans une autre catégorie : les spécialistes de la connectivité pour l'IoT. Un segment qui pourrait peser 15 milliards d'euros à l'horizon 2025 et qui comporte des pure players comme Sigfox.

Toujours selon le cabinet en stratégie qui a présenté mardi midi les résultats de son étude à Paris, on devrait recenser dans dix ans une base installée de 26 milliards d'objets connectés (correspondant à un marché de 10 milliards d'euros pour les fournisseurs de composants et modules comme Sierra Networks, Telit ou Gemalto).

L'essor de la dimension Internet des objets devraient avoir un impact sur 5 secteurs principalement : le transport et l'hôtellerie (250 milliards d'euros), la santé (235 milliards d'euros), la domotique domestique (160 milliards d'euros), le matériel industriel (pour un montant similaire), et la distribution, commerce (hors commerce électronique) et vente en gros (60 milliards d'euros).

Divers paramètres pourraient modifier cette perspective apportée par AT Kearney : le niveau d'adoption des objets connectés par les consommateurs, la politique industrielle associée à l'IoT en Europe (balbutiante en l'état actuel malgré une certaine prise de conscience par la Commission européenne), la guerre d'influence des plateformes (Google, Apple, Samsung…), la rationalisation des standards IoT sur fond de consortiums puissants (Open Interconnect, Allseen Alliance, Industrial Internet Consortium…), l'avancée de la 5G en Europe, l'impact de l'IoT sur l'emploi et la juste appréciation du traitement des données.

Etude « The Internet of Things : a new path to European Prosperity », ATKearney, janvier 2016, co-auteurs : Thomas Kratzert et Michael Broquist (respectivement Partner et Principal à Stockholm), Hervé Collignon et Julien Vincent (respectivement Partner et Principal à Paris)

En savoir plus sur http://www.itespresso.fr/europe-vraie-puissance-internet-objets-117702.html#2t626JMWackx6u04.99

Réagissez à cet article

Source : *L'Europe, une vraie puissance de l'Internet des objets ? | ITespresso.fr*