La Cnil met en demeure Apple France, accusé de surveiller en permanence ses salariés…

La Cnil met en demeure Apple France, accusé de surveiller en permanence ses salariés…

La firme à la pomme a été épinglée plusieurs fois par la Commission pour sa pratique abusive des caméras de surveillance, même dans les espaces de repos des salariés.

Il fut un temps où Apple dénonçait à grands coups de publicités la surveillance généralisée d'une société, comme dans 1984. La firme à la pomme semble aujourd'hui avoir zappé ces beaux principes…

La Cnil annonce en effet avoir mis en demeure Apple Retail France pour sa pratique abusive des caméras de surveillance dans ses boutiques et pour le manque d'information des salariés. Les caméras « ne sont pas orientées uniquement vers les zones sensibles (apporte d'accès ou coffre-fort) mais filment de manière directe et constante les postes de travail » mais aussi la salle de repos d'une des boutiques.

Cette surveillance, « est disproportionnée au regard de la finalité de prévention des atteintes aux personnes et aux biens. Si la surveillance de zones sensibles est justifiée par des impératifs de sécurité, le placement sous surveillance permanente de salariés, attentatoire à leur vie privée, ne peut intervenir que dans des circonstances exceptionnelle », assène la Commission.

Surveillance disproportionnée

Ce n'est en fait pas la première fois que la firme est épinglée par la Commission informatique et Libertés. En décembre 2013, elle faisait déjà l'objet d'une mise en demeure portant sur le dispositif de vidéosurveillance des salariés installé au sein de l'Apple Store d'Opéra à Paris. « Il était notamment demandé à la société de réorienter certaines caméras qui filmaient en permanence des salariés et de leur délivrer une information complète », explique la Cnil.

En février 2014, la société a justifié s'être mise en conformité avec ses obligations pour le magasin, entraînant la clôture de la mise en demeure. Mais des contrôles menés en mai et juin derniers dans d'autres magasins français du géant « ont révélé que la société n'avait pas adopté des mesures de conformité similaires à l'ensemble de ses magasins. L'information des salariés sur le dispositif demeurait lacunaire et certaines caméras continuaient à filmer des salariés à leur poste de travail sans justification particulière ».

« La persistance de ces manquements » a conduit la Commission à mettre à nouveau en demeure la société « de modifier l'intégralité des dispositifs de vidéosurveillance de ses 16 magasins sur le territoire national ».

« Aucune suite ne sera donnée à cette procédure si Apple France se conforme à la loi dans le délai de deux mois qui lui est imparti », ajoute la Cnil. Dans le cas contraire, la firme pourrait écoper de sanctions financières.

Voila de quoi tendre encore un peu plus les relations entre Apple et ses salariés français. En 2012 déjà, ces derniers s'étaient mis en grève. En cause, des revendications sur les salaires et les conditions de travail. Les syndicats négociaient avec la direction la mise en place de différents dispositifs, dont l'attribution de tickets restaurant et d'un 13e mois. Les salariés ont finalement obtenu une concession : des tickets restaurant d'un montant de 8,50 euros…

Par Olivier Chicheportiche

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

Source :

http://www.zdnet.fr/actualites/la-cnil-met-en-demeure-apple-france-accuse-de-surveiller-en-permanence-ses-salaries-39808739.htm

Certains sites facturent jusqu’à 80€ de plus l’achat depuis un mobile

Certains sites factureraient jusqu’à 80€ de plus l’achat depuis un mobile

Une étude dénonce l’absence de transparence des sites de e-commerce et de réservation d’hôtels pratiquant la tarification dynamique. Plus de la moitié des services analysés applique des prix différents en fonction des acheteurs.

Dans les souks, il n’est pas rare d’avoir des prix à la tête du client. Mais au moins, on peut négocier. Sur Internet, on apprend que les prix peuvent varier selon le type de terminal utilisé, le système d’exploitation ou les données personnelles des Internautes. C’est ce que démontre une équipe de chercheurs du College of Computer and information Science de l’université du Nord-Est à Boston (USA).

L’étude révèle que, sur les 16 sites américains observés, 9 modifient les prix en fonction du type de visiteur. Ainsi, le service de réservation d’hôtels Travelocity réduit ses tarifs de 15 dollars pour les utilisateurs d’iPhone ou d’iPad. Le distributeur Home Depot facture jusqu’à 100 dollars supplémentaires les internautes naviguant à partir d’un terminal mobile. Cheaptickets et Orbitz, deux sociétés de voyages en ligne, ajoutent 12 dollars en moyenne à la note des clients ne disposant pas de comptes sur leurs sites.
Enfin, Expedia et Hotels.com manipulent les résultats de recherches afin de mettre en avant des hôtels plus chers. Cela dans l’optique de tester l’impact de telles méthodes sur les internautes.

Un manque de transparence
La pratique du « Dynamic pricing », ou tarification dynamique, est bien connue et n’a rien d’illégale. D’ailleurs, elle est antérieure à Internet, puisque des coupons de réduction dans un supermarché constituent également une forme de tarification personnalisée. En revanche, Internet, le Big data et les traceurs ont permis d’affiner la technique en se servant, entre autres, des adresses IP des visiteurs, de leur localisation géographique, de leur historique (navigation et achats), ou encore de la plateforme utilisée.
Ce que les chercheurs pointent du doigt n’est donc pas la pratique en tant que telle, mais le manque de transparence autour de celle-ci. La tarification dynamique peut permettre d’obtenir des produits à de meilleurs prix, à condition d’être au courant de sa mise en œuvre. Autrement, des clients peuvent se retrouver à payer plus cher pour le même produit, sans s’en rendre compte.
Certains e-commerçants, comme Amazon par exemple, gardent secrète leur méthode de calcul des tarifs. En 2011, des consommateurs s’étaient plaints d’avoir payé des prix différents pour le même DVD, livré dans les mêmes conditions. Le géant américain avait alors remboursé la différence. Un an plus tard, Orbitz se retrouvait à son tour sous le feu des projecteurs car le service mettait en avant des hôtels jusqu’à 30% plus cher lorsqu’un visiteur effectuait une recherche à partir d’un Mac. Depuis, la société affirme avoir mis un terme à cette pratique.
Plus récemment, les sociétés de location de voitures Avis, Goldcar, Entreprise, Sixt, Europcar et Hertz se sont fait taper sur les doigts pour avoir appliqué des prix différents selon l’endroit où se trouvait le consommateur. Une différence de traitement injustifiée selon l’Union européenne. Cette dernière avait alors sommé les six sociétés de respecter les lois du marché unique sur le vieux continent.

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

Source :
http://pro.clubic.com/e-commerce/actualite-735329-commerce-etude-prix-utilisateur.html?&svc_mode=M&svc_campaign=NL_ClubicPro_New_28/10/2014&partner=-&svc_position=720502960&svc_misc=-&crmID=639453874_720502960&estat_url=http%3A%2F%2Fpro.clubic.com%2Fe-commerce%2Factualite-735329-commerce-etude-prix-utilisateur.html

---

CyberCercle du 8 octobre 2014 – Décryptage du rapport interministériel sur la lutte contre la cybercriminalité

CyberCercle du 8 octobre 2014 – Décryptage du rapport interministériel sur la lutte contre la cybercriminalité

Le 8 octobre dernier, Denis JACOPINI s'est rendu au Décryptage du rapport interministériel sur la lutte contre la cybercriminalité organisé par le CyberCercle.

Le CyberCercle a reçu mercredi 8 octobre 2014, Myriam QUEMENER, Magistrat, membre du groupe de travail auteur du rapport interministériel sur la lutte contre la cybercriminalité, membre de la Commission Numérique à l'Assemblée Nationale, et Maître Christiane FERAL-SCHUHL, avocat, ancien Bâtonnier du Barreau de Paris, co-présidente de la Commission Numérique à l'Assemblée Nationale, pour un petit-déjeuner-débat sur le thème :
« DECRYPTAGE DU RAPPORT INTERMINISTERIEL SUR LA LUTTE CONTRE LA CYBERCRIMINALITE »

Cette conférence s'est déroulée dans les salons du Bateau MAXIM'S en présence d'une cinquantaine d'auditeurs, notamment des représentants de la magistrature, de la Gendarmerie nationale, de la D2IE, de l'ANSSI, du ministère de la Défense, et des entreprises partenaires des forces de sécurité dans la lutte contre la cybercriminalité.
Retrouvez Myriam QUEMENER par video sur notre chaîne YouTube : « Quels sont selon vous les points forts du rapport interministériel sur la lutte contre la cybercriminalité publié en juillet 2014 ? »

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

Source :
http://www.defense-et-strategie.fr/index.php?option=com_content&view=article&id=567:cybercercle-du-8-octobre-2014-decryptage-du-rapport-interministeriel-sur-la-lutte-contre-la-cybercriminalite

---

Outlook Web App ciblé par des attaques de phishing sophistiquées – Le Monde Informatique

Outlook Web App ciblé par des attaques de phishing sophistiquées

Selon les chercheurs de Trend Micro, un groupe de pirates sévit à l'encontre d'agences militaires, ambassades et d'entreprises liées à la défense nationale et des médias internationaux utilisant Outlook Web App d'Office 365.

Afin de voler les identifiants de messagerie des employés de nombreuses organisations publiques, parapubliques mais également privées, un groupe d'espions a mis en place des techniques de phishing avancées.
Selon des chercheurs de l'entreprise de sécurité Trend Micro, qui ont baptisé cette campagne Operation Pawn Storm dans un document publié la semaine dernière, le groupe à l'origine de ces attaques opèrerait depuis au moins 2007. Au cours de ces années, ils ont utilisé différentes techniques pour atteindre leurs objectifs, notamment des campagnes de phishing pour propager des malwares sous forme de pièces jointes Microsoft Office malveillantes, l'installation de backdoors type SEDNIT ou Sofacy, ou des exploits plus sélectifs pour infecter des sites légitimes.

Dans ses dernières attaques de phishing, le groupe a utilisé une technique particulièrement intéressante, ciblant les organisations qui utilisent Outlook Web App (OWA), une composante du service Office 365 proposé par Microsoft. Pour chaque attaque, le groupe a créé deux faux domaines : un premier, qui reproduit un site Web tiers connu des victimes – par exemple le site d'une conférence dans un secteur de l'industrie qui les intéresse – et un second, similaire au domaine utilisé pour le déploiement d'Outlook Web App par l'organisation visée. Les attaquants ont ensuite créé des courriels contenant un lien vers le faux site tiers sur lequel ils hébergeaient un code JavaScript non malveillant dont le but était double : ouvrir le site légitime dans un nouvel onglet et rediriger l'onglet déjà ouvert du navigateur Outlook Web App vers une page de phishing. « Le code JavaScript faisait croire aux victimes que leur session OWA était close, et la page malveillante leur demandait de se reconnecter en tapant à nouveau leurs identifiants », ont écrit les chercheurs de Trend Micro dans leur document.
« Les attaquants ont réussi à rediriger les victimes vers de fausses pages Outlook Web App en agissant sur les propriétés d'ouverture des pages de leurs navigateurs ».

Une technique de phishing multi-navigateurs
Selon les chercheurs, cette technique n'exploite aucune vulnérabilité et fonctionne avec tous les navigateurs courants dont Internet Explorer, Mozilla Firefox, Google Chrome et Safari d'Apple. Cependant, il faut deux conditions pour que ce mode opératoire fonctionne : « Les victimes doivent utiliser OWA et ils doivent cliquer sur les liens intégrés au volet de prévisualisation OWA », ont-ils expliqué. L'attaque est redoutable parce que l'onglet du navigateur ne permet pas aux victimes de voir que leur session OWA est illégitime et ils ont peu de chance de se rendre compte que l'URL a été usurpée avant de rentrer leurs identifiants. « De plus, les attaquants ont pris soin d'utiliser des noms de domaine très similaires à ceux choisis par les organisations ciblées pour leurs pages de log in OWA, et dans certains cas, ils ont même acheté des certificats SSL légitimes, de sorte que les navigateurs des victimes affichent aussi les indicateurs de connexion sécurisée HTTPS pour les sites de phishing », ont encore ajouté les chercheurs de Trend Micro.

Parmi les personnes visées, on trouve des employés de l'entreprise militaire privée américaine Academi, anciennement connue sous le nom de Blackwater ; l'Organisation pour la sécurité et la coopération en Europe (OSCE) ; le Département d'État des États-Unis ; le fournisseur du gouvernement américain Science Applications International Corporation (SAIC) ; une société multinationale basée en Allemagne ; l'ambassade du Vatican en Irak ; des médias de radiodiffusions de plusieurs pays ; les ministères de la Défense de la France et de la Hongrie ; des responsables militaires pakistanais ; des employés du gouvernement polonais et des attachés militaires de différents pays. Parmi les appâts utilisés par les assaillants, les chercheurs ont identifié des événements et des conférences bien-connus pour lesquels les victimes pouvaient avoir un intérêt.
« Mais, ce n'est pas tout : les assaillants ont combiné leur tactique de phishing à diverses attaques éprouvées afin de compromettre les systèmes et entrer dans les réseaux pour y voler des données », ont déclaré les chercheurs de Trend Micro.
« Les variantes de SEDNIT utilisées ont été semble-t-il très efficaces car elles ont permis aux pirates de voler des informations sensibles sur les ordinateurs des victimes en évitant de se faire repérer ».

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

Source :
http://www.lemondeinformatique.fr/actualites/lire-outlook-web-app-cible-par-des-attaques-de-phishing-sophistiquees-59081.html

---

Un grand pas vers la détection des fraudes nommé

ArgyleDB

Un grand pas vers la détection des fraudes nommé ArgyleDB

L'éditeur Argyle Data a lancé sa solution de détection des fraudes reposant sur le SGBD Accumulo créé par la NSA ainsi que sur le moteur de requêtes SQL distribué Presto développé par Facebook.

Argyle Data a annoncé le lancement d'ArgyleDB, sa solution de surveillance et de détection des fraudes en temps réel taillé pour les environnements Hadoop et à forte volumétrie de données. La société indique avoir conçu son offre sur la base du système de gestion de base de données Accumulo, initialement développé par la NSA avant d'être récupéré en 2011 par la fondation Apache, mais également de Presto, la technologie Open Source utilisée par Facebook pour permettre d'analyser les données en utilisant des requêtes SQL et d'automatiser les futures requêtes sur les données en direct.
Argyle Data indique par ailleurs que sa solution supporte un ensemble d'algorithmes permettant de détecter une activité frauduleuse, à une échelle pétaflopique, en une quinzaine de minutes seulement contre 24 heures ou plus habituellement. L'année dernière, Argyle Data avait annoncé travailler sur une gamme de produits utilisant le machine learning sur une pile Hadoop afin de créer des applications capables d'ingérer des données et de les analyser en temps réale pour réduire la fenêtre de détection des fraudes et d'intrusion de plusieurs heures ou jours à quelques secondes.

Une levée de fonds de 4,5 millions de dollars
Parallèlement à ce lancement, Argyle Data a annoncé un nouveau tour de table financier qui lui a permis de lever 4,5 millions de dollars, portant à 21 millions de dollars le montant total des fonds levés depuis sa création en 2009. L'équipe de direction est également étoffée avec l'arrivée de Arshak Navruzyan, Ian Howells, Padraig Stapleton et Volkmar Scharf-Katz Navruzyan qui ont tous un solide vécu en matière d'analytique et de machine learning.

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

Source :
http://www.lemondeinformatique.fr/actualites/lire-argyledb-la-detection-des-fraudes-avec-des-technologies-de-facebook-et-la-nsa-59068.html?utm_source=mail&utm_medium=email&utm_campaign=Newsletter

---

Droit au déréférencement sur Google jugé à Paris

Droit au déréférencement sur Google jugé à Paris

Dans une ordonnance de référé datant du 16 septembre 2014, le Président du Tribunal de Grande Instance de Paris a enjoint Google France, de supprimer des liens renvoyant vers des contenus déjà jugés diffamatoires par un jugement du tribunal correctionnel du 13 mars 2014.

Google France avait tenté de faire valoir qu'elle n'avait qu'une activité de fourniture de prestations de marketing et de démonstration auprès d'une clientèle utilisant des services publicitaires. Cependant, le juge des référés a retenu que si la société Google Inc, sa société-mère, était l'exploitant du moteur de recherche, Google France avait pour activité la promotion et la vente d'espaces publicitaires liés à des termes recherchés au moyen du moteur édité par Google Inc. et assurait donc, le financement de ce moteur de recherche.
Google France avait argué que les demandeurs ne pouvaient contourner les conditions procédurales de la loi du 29 juillet 1881 (notamment l'article 53), dès lors qu'ils agissaient sur le fondement de la diffamation. Toutefois, le juge des référés a retenu qu'en aucun cas les demandeurs ne se fondaient sur la loi du 29 juillet 1881. En effet, ces derniers reprochaient simplement à Google France d'avoir mis à la disposition de ses utilisateurs des données à caractère personnel qui avaient déjà été jugées diffamatoires.. Ainsi, le Président du Tribunal de grande instance de Paris a estimé que les dispositions de la loi du 29 juillet 1881 précitée n'étaient pas applicables à Google France.

Le juge a donc consacré un droit au déréférencement dans les moteurs de recherche sur Internet en s'appuyant sur plusieurs fondements afin d'enjoindre Google France à déréférencer plusieurs liens renvoyant à des contenus diffamatoires :
– la Loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel ;
– la Loi n°78-17 du 6 janvier 1978 selon laquelle : « {Toute personne physique justifiant de son identité peut exiger du responsable d'un traitement que soit, selon les cas, rectifiées, complétées, mises à jour, verrouillées ou effacées les données à caractère personnel la concernant, qui sont inexactes, incomplètes, équivoques, périmées, ou dont la collecte, l'utilisation, la communication ou la conservation est interdites. »}
– l'Arrêt du 13 mai 2014 de la Cour de justice des communautés européennes ;
– et la Directive 95/46/CE du Parlement européen et du Conseil du 24 octobre 1995 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation de ces données. Cette dernière directive européenne vise à assurer « une protection efficace et complète des libertés et des droits fondamentaux des personnes physiques, notamment du droit à la vie privée ».

Le juge des référés ordonna ainsi à la société Google France, sous astreinte, de faire procéder à la suppression des liens référencés litigieux. Cette décision, qui apparait quelques mois après l'arrêt innovant de la CJUE du 13 mai 2014, consacre pour la première fois en France, un droit au recours au juge des référés pour faire respecter ce droit au déréférencement des données à caractère personnel dans les résultats du moteur de recherche Google.

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

Source :
http://www.legavox.fr/blog/e-reputation-et-droit/google-consecration-droit-dereferencement-donnees-16076.htm

---

Les cybercriminels utilisent aussi les Sous-domaines

abandonnés

Les cybercriminels utilisent aussi les Sous-domaines abandonnés

Si la plupart des hackeurs tentent de contourner les mesures de sécurité mises en place sur les serveurs d'une entreprise, il est parfois plus simple de scruter l'architecture d'un site au global et les sous-domaines, notamment.

Spécialisée dans la sécurité, la société Detectify, propose un outil de scan en mode SaaS et annonce avoir mené une enquête concernant la vulnérabilité des sous-domaines. Ces derniers seraient largement laissés à l'abandon et constitueraient un vecteur d'attaques.
Un prestataire de services proposant de créer des comptes utilisateur en leur attribuant un sous-domaine peut lui-même créer son propre sous-domaine pour lancer un service ou une campagne promotionnelle pendant quelques semaines, voire quelques années. Par la suite, à la fin de cette campagne ou à la fermeture du service en question, Detectify explique que le prestataire n'efface pas systématiquement la redirection du sous-domaine pointant vers le service ou la campagne. Or, un internaute peut donc se créer un compte chez ce prestataire de service puis obtenir ce même sous-domaine et orchestrer une attaque de phishing, par exemple.
Cette manipulation est possible lorsque la société en question ne procède pas à la validation du détenteur de chaque sous-domaine. Et il en existerait un certain nombre parmi lesquels nous retrouvons Heroku, Github, Bitbucket, Squarespace, Shopify, Desk, Teamwork, Unbounce, Helpjuice, HelpScout, Pingdom, Tictail, Campaign Monitor, CargoCollective, StatusPage.io ou encore Tumblr.
« Nous avons également identifié 200 organisations qui s'en trouvent affectées. Dans beaucoup de cas, nous parlons de société listées au NASDAQ ou figurant dans le top 100 d'Alexa », ajoute Detectify.
Pour vérifier si une personne est bien le propriétaire d'un domaine ou d'un sous-domaine, quelques sociétés, comme Google demandent de transférer un fichier HTML via FTP ou d'ajouter une CNAME particulière dans le panneau de contrôle du nom de domaine.

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

Source :
http://pro.clubic.com/it-business/securite-et-donnees/actualite-735061-domaine-abandonnes-vecteur-attaques-hackeurs.html?&xvc_mode=M&xvc_campaign=NL_ClubicPro_New_25/10/2014&partner=-&xvc_position=71726460?&xvc_misc=-&crmID=639453874_71726460?&estat_url=http%3A%2F%2Fpro.clubic.com%2Fit-business%2Fsecurite-et-donnees%2Factualite-735061-domaine-abandonnes-vecteur-attaques-hackeurs.html

---

Déclaration à la Cnil d'un dispositif de contrôle et moyen de preuve

Déclaration à la Cnil d'un dispositif de contrôle et moyen de preuve

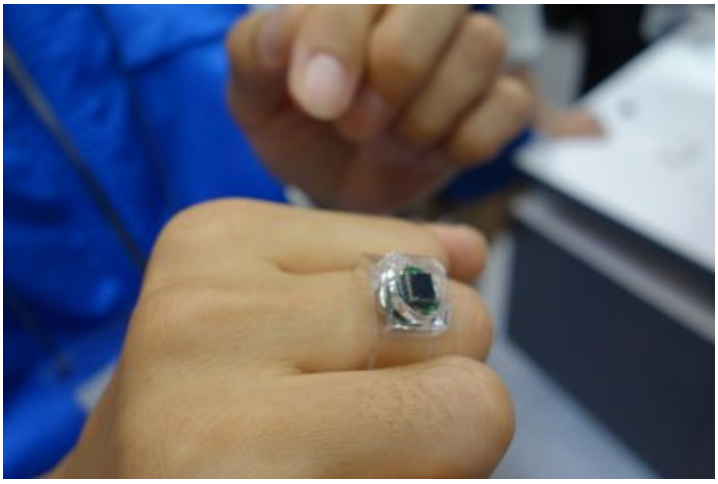
Les informations collectées par un système automatisé de contrôle des données à caractère personnel avant sa déclaration à la Cnil constituent un moyen de preuve illicite.
Une salariée engagée en tant qu'assistante chargée de l'analyse financière des dossiers ayant fait un usage excessif de sa messagerie électronique à des fins personnelles, son employeur l'a licenciée pour cause réelle et sérieuse.
La cour d'appel a rejeté les demandes de dommages et intérêts de la salariée pour licenciement sans cause réelle et sérieuse et pour licenciement vexatoire, au motif que la déclaration tardive à la Cnil de la mise en place d'un dispositif de contrôle individuel des flux de la messagerie électronique ne rend pas ce système de contrôle illicite, alors que la salariée ne faisait pas un usage raisonnable de cet outil à des fins privées, durant son temps de travail.
La Cour de cassation censure cette position, dans un arrêt du 8 octobre 2014, et considère que les informations collectées par un système de traitement automatisé des données personnelles avant sa déclaration à la Cnil, constituent un moyen de preuve illicite. Les éléments de preuve obtenus à l'aide d'un tel système avant sa déclaration à la Cnil ne sont donc pas licites.

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

Source :
http://actualitesdudroit.lamy.fr/Accueil/Articles/tabid/88/articleType/ArticleView/articleId/125297/Declaration-a-la-Cnil-dun-dispositif-de-controle-et-moyen-de-preuve.aspx

---

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.

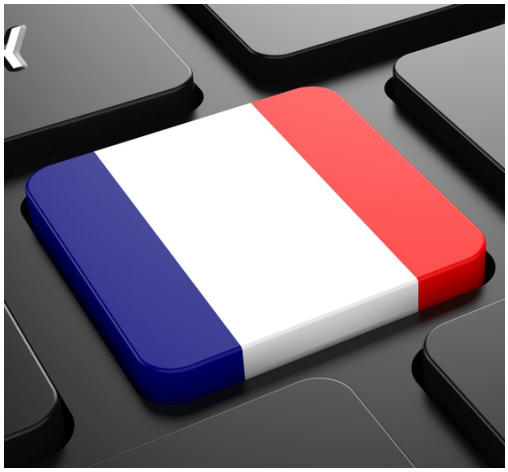
Cet article vous à plu ? Laissez-nous un commentaire (Source de progrès)

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

---

France Connect, pour simplifier l'administration

numérique



France Connect, pour simplifier l'administration numérique

Les administrations et les collectivités locales qui bénéficieront à court terme d'un support d'identification unifié.

Thierry Mandon, le secrétaire d'Etat chargé de la réforme de l'Etat et de la simplification, s'est rendu le 2 octobre dans les locaux de la Dila pour visiter le plateau de développement du projet « France Connect ». France Connect est la « marque de fabrique » du futur système numérique national d'identification et d'authentification des usagers des services de l'administration.
Le dispositif, développé par le Secrétariat général pour la modernisation de l'action publique (SGMAP), cible les services publics de l'Etat, les administrations et les collectivités locales qui bénéficieront à court terme d'un support d'identification unifié, bon marché et relativement facile à implémenter dans leur propre système d'information.
Ce programme, qui sera déployé dès 2015 avec la bascule sur France Connect des trois millions de comptes du site portail « mon.service-public.fr », doit permettre à l'usager de fédérer tous ses comptes publics existants, puis d'établir ensuite de nouvelles connexions avec des administrations non encore dotées de leur propre système d'authentification, à condition d'adopter directement celui de France Connect.

La solution annule et remplace la carte d'identité électronique
La procédure qui s'apparente à celle déjà pratiquée par les réseaux sociaux comme « Facebook Connect » ou « Google+ Sign in » restera relativement simple à déployer. L'usager n'ayant pas encore de compte pourra s'enregistrer à partir d'une administration reconnue par le label et à laquelle il est numériquement affilié. Après avoir saisi ses identifiants d'origine, le site lui proposera en retour de fédérer son compte avec France Connect.
Après avoir donné son consentement, il disposera d'un compte national réutilisable sur de nombreux sites. Cette simplicité dans le mode d'enregistrement a d'ailleurs incité la DGFIP à proposer aux contribuables, dès la campagne 2016 de déclaration de revenus en ligne, de fédérer leur compte « impôts.gouv.fr » avec France Connect afin d'étendre rapidement le dispositif aux 10 millions d'utilisateurs dotés d'un compte fiscal.
France Connect ne se limite pas au seul composant unifié d'identification. A terme, il devrait permettre aux administrations et notamment aux collectivités d'effectuer des requêtes sur le niveau d'imposition ou sur la domiciliation de l'usager afin d'éviter l'étape coûteuse des demandes de justificatifs. Selon un expert ayant participé à la définition du projet, la nouvelle solution répondrait à 95% des besoins justifiant la création d'une carte d'identité électronique (CNIE) et l'économie réalisée sur la « non création » de cette carte avoisinerait le milliard d'euros.
France Connect devrait ainsi accélérer le développement de portails de téléservices couvrant la totalité des besoins transactionnels des collectivités avec les usagers et constituer également une brique essentielle de la mise en œuvre du programme « dites-le nous une fois » dans toutes les administrations. Autant dire qu'il constitue déjà à lui seul un levier essentiel pour les prochaine conquêtes de l'administration numérique.
Philippe Parmantier / EVS

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

Source :
http://www.localtis.info/cs/ContentServer?pagename=Localtis/LOCActu/ArticleActualite&cid=1250267813817