Les « Vrais faux » avis des consommateurs : quand e-réputation rime avec compétition

	Les « Vrais faux » avis des consommateurs : quand e-réputation rime avec compétition

En tentant de chiffrer les enjeux commerciaux associés aux avis de consommateurs, deux études permettent d'entrevoir l'intérêt bien compris des acteurs de l'e-réputation tentés de s'engager sur le marché des services de rédaction et de publication de commentaires, ainsi que le bénéfice que leurs clients sont susceptibles d'en retirer. Attention à ne pas tomber dans la manipulation…

Réputation, la nouvelle donne du Web 2.0

La réputation d'une entreprise constitue un actif immatériel essentiel. Elle participe au dynamisme et à la bonne santé d'une activité économique. Sa maîtrise est un enjeu de compétitivité qui, de la PME au groupe international, mobilise des investissements d'image et de positionnement substantiels. Au-delà des opportunités qu'elle génère, force est de constater que l'émergence du Web 2.0, dont la caractéristique essentielle consiste en la possibilité pour les internautes de réagir et de commenter les contenus postés sur diverses plateformes, a changé la donne pour l'entreprise.

En plus des canaux traditionnels, l'e-réputation résulte désormais de nouveaux acteurs – consommateurs, concurrents, salariés, etc. – et de nouveaux supports : réseaux sociaux, blogs, sites d'avis de consommateurs. Si les atteintes à l'e-réputation prennent des formes variées, le phénomène des « vrais faux » avis sur les plateformes communautaires revêt aujourd'hui une ampleur préjudiciable pour la confiance dans l'économie numérique.

Il vise deux finalités principales :

La première consiste à gonfler artificiellement la notoriété d'une entreprise, sa notation et la visibilité sur Internet qui en résulte auprès des consommateurs ; il s'agit dans ce cas de figure d'avis positifs postés par l'entreprise elle-même ou son prestataire.

La seconde consiste à dénigrer les produits ou prestations d'une entreprise, son image ou sa réputation ; il s'agit là de commentaires négatifs postés par un concurrent ou son prestataire.

Dans les deux cas, l'objectif est double : promouvoir de manière non transparente ses propres produits et discréditer ceux d'un concurrent.

Au-delà de l'atteinte à la (e)-réputation, quel enjeu commercial ?

L'enjeu commercial associé aux avis de consommateurs, à la notation et à la visibilité qui en résulte, est souligné dans deux études réalisées par la Harvard Business School sur le site Yelp. La première étude constate que la progression d'une « étoile » peut permettre au professionnel noté d'accroître son revenu de 5 à 9 %.

Appréciés au regard des conclusions d'une seconde étude, selon laquelle environ 16 % des avis sont frauduleux, ces chiffres permettent d'entrevoir l'intérêt bien compris d'acteurs de l'e-réputation tentés de s'engager sur le marché des services de rédaction et de publication de commentaires ainsi que le bénéfice commercial que leurs clients sont susceptibles d'en retirer. Il n'en va pas sans risque juridique au regard de la responsabilité des entreprises et des prestataires qui feraient le choix de s'engager sur cette voie.

La DGCCRF dotée de nouveaux pouvoirs par la loi « Hamon ». C'est vers les États-Unis qu'il faut se tourner pour trouver un exemple récent d'action répressive à l'encontre de professionnels des « vrais faux » avis et de clients en mal de notoriété sur Internet. L'avocat général de l'État de New York annonçait en septembre 2013 la conclusion d'un accord avec 39 entreprises s'engageant à cesser d'avoir recours à de tels procédés frauduleux ainsi que le paiement par ces sociétés d'**amendes pour un montant total de 350 000 dollars.**

En France, la Direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF) semble s'être emparée du sujet et a multiplié les contrôles qui feraient suite à des signalements de consommateurs abusés ou de professionnels victimes de concurrents. Ses pouvoirs vis-à-vis des services web ont d'ailleurs été renforcés par la loi du 17 mars 2014 relative à la consommation (dite loi Hamon). Par exemple, en cas de pratiques commerciales déloyales (cf. ci-dessous), l'article L.141-1 du code de la consommation lui donne désormais la faculté de saisir le juge afin de solliciter toute mesure propre à prévenir ou faire cesser un dommage causé par le contenu d'un service de communication au public en ligne.

Concrètement, ces dispositions semblent ouvrir la voie à des mesures d'injonction de blocage de sites web prononcées à l'encontre de l'hébergeur du site internet litigieux ou des fournisseurs d'accès à internet. Rappelons aussi que la DGCCRF a la possibilité de transmettre le résultat de ses investigations au procureur de la République qui décidera de l'opportunité des poursuites. À ce jour, aucune condamnation pénale ne semble toutefois avoir été prononcée.

Qualifications juridiques, recours et sanctions

La publication de vrais-faux avis n'en est pas moins susceptible de relever de plusieurs qualifications juridiques, pour certaines, pénalement réprimées. La manipulation d'avis, qu'il s'agisse de la rédaction d'avis positifs ou de la suppression d'avis négatifs, est susceptible de constituer une pratique commerciale déloyale telle que définie à l'article L.120-1 du code de la consommation, et plus particulièrement une pratique commerciale trompeuse (article L.121-1 et L.121-1-1 du même code).

Restées jusqu'ici théoriques, les sanctions pénales encourues doivent être rappelées : deux ans d'emprisonnement et 187 500 euros d'amende pour une personne morale. Cette amende peut être portée à 50 % des dépenses affectées à la publicité ou à la pratique constituant le délit et complétée par la publication du jugement et/ou la diffusion d'annonces rectificatives. Sur le plan civil, un premier réflexe pour une entreprise victime de commentaires frauduleux serait de viser la plateforme communautaire afin de solliciter le retrait des avis dont le caractère dénigrant serait démontré.

De plus, la réparation du préjudice subi par un concurrent dénigré pourra résulter d'une action en réparation sur le fondement de l'article 1382 du Code civil. À ce titre la Cour d'appel de Paris, dans un arrêt du 19 mars 2008, a sanctionné une société ayant « jeté le discrédit sur les produits commercialisés » par son concurrent après avoir publié des avis négatifs sur son compte. Lorsque les avis sont publiés sous couvert d'anonymat, une attention particulière devra être portée à la collecte de la preuve de l'identité de l'auteur des avis litigieux. Dans une récente affaire, la seule mention d'une adresse IP correspondant à l'ordinateur d'une société concurrente a été jugée insuffisante pour démontrer la réalité des manœuvres alléguées.

Vers une autorégulation des plateformes communautaires d'avis ?

Pour tenter de prendre le problème à bras le corps, certaines plateformes communautaires d'avis se targuent d'avoir mis en place des systèmes de détection de fraude et des équipes de modérateurs. C'est en matière de normalisation que l'initiative d'autorégulation la plus structurée a récemment émergé. Elle émane de l'Afnor et prend la forme d'une norme, publiée le 4 juillet 2013, encadrant la publication d'avis de consommateurs sur internet. Développée à l'initiative d'acteurs privés, cette norme décrit un certain nombre de bonnes pratiques relatives à la collecte, l'origine des avis, leur modération, l'affichage des avis et la notation qui peut en résulter.

Pour être opposables aux consommateurs, ces recommandations devront pour certaines être intégrées aux conditions générales d'utilisation des plateformes communautaires qui feraient le choix de s'y conformer. Une norme est en effet dépourvue de force contraignante. Par un arrêt du 27 février 2013, la Cour d'appel de Paris a eu l'occasion de rappeler qu'une norme « n'a aucun caractère obligatoire et ne constitue qu'un recueil de recommandations de bonnes pratiques ». Dans cette affaire, la Cour a refusé les demandes de nullité d'un procès-verbal de constat fondées uniquement sur le non-respect de la norme relative au « mode opératoire de procès-verbal de constat sur internet effectué par huissier de justice ».

Jean-Sébastien Mariez / Avocat | Le 25/05 à 08:33

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

Source :
http://www.lesechos.fr/idees-debats/cercle/cercle-90737-vrais-faux-avis-de-consommateurs-quand-e-reputation-rime-avec-competition-1006014.php?fhoIARI38UX5YK2d.99

73% des entreprises ne sont pas prêtes après un sinistre dans le cloud

73% des entreprises ne sont pas prêtes après un sinistre dans le cloud

Avec des applications de plus en plus hébergées dans le cloud, les entreprises doivent faire évoluer leurs plans de reprise d'activité suite à un incident ou une panne. Mais pour Carlos Escapa, SVP chez Unitrends, la prise de conscience est encore incomplète.

L'utilisation massive du cloud pour héberger les applications critiques des entreprises multiplie les risques en cas de sinistre sur les équipements. Or, les entreprises ne semblent pas prêtes dans ce scénario à restaurer rapidement l'activité. Telle est la conclusion d'une étude mondiale menée pour Unitrends, un spécialiste des plans de reprise d'activité.
Les chiffres sont assez parlants : 78% des personnes interrogées ont connu des coupures des applications critiques, dont 63% estiment que les pertes ainsi engendrées vont de quelques centaines de dollars à plus de 5 millions. 28% des entreprises touchées par un incident estiment que leurs entreprises ont été privées de fonctions clés de leurs datacenters pendant des périodes pouvant aller jusqu'à plusieurs semaines.
« Le phénomène est particulièrement prégnant en Amérique du Nord où les ruptures d'alimentation énergétique des datacenters sont fréquentes. Mais on peut aussi évoquer la complexité de la cartographie applicative et les erreurs humaines », explique à ZDNet.fr, Carlos Escapa, SVP chez Unitrends.
Or, 73% des entreprises déclarent ne pas prêtes pour la restauration après sinistre. 64% des personnes interrogées estiment que le budget alloué par l'entreprise au plan de restauration après sinistre est inadapté et insuffisant. Et plus de 60% estiment qu'elles n'ont pas complètement documenté leur plan de reprise d'activité. Parmi la minorité qui dit l'avoir correctement renseigné, 23% n'ont jamais testé ces plans de reprise d'activité.

78% des entreprises interrogées ont subi des coupures dans les applications critiques
Evidemment, ces chiffres alarmants sont à relativiser étant donné que la source de cette étude n'est autre qu'un fournisseur de solutions dédiées aux PRA (plans de reprise d'activité) issus d'environnements virtualisés. Mais ils illustrent une tendance : le passage des applications critiques dans le cloud n'a pas été suivi d'un adaptation des PRA.
« Les pannes de service ne sont pas tolérables, encore moins aujourd'hui avec des processus qui s'appuient sur des applications, notamment mobiles », ajoute le responsable. « La protection des données ne suffit pas et les directions prennent conscience de l'importance de PRA adaptés ».
Cette prise de conscience est désormais en progressions dans les directions et les DSI « car les applications mobiles sont au coeur du business », résume prosaïquement Carlos Escapa. « Et puis, il y a la pression des contraintes légales comme Bâle 2 qui impose à certains secteurs des politiques précises en matière de panne ».
Pour autant, le chiffre de 73% d'entreprises pas prêtes paraît colossal. « Cela ne nous étonne pas. La plupart des PME estime que les PRA sont trop coûteux et estiment mal le risque financier de sinistre dans les datacenters. Notre discours est de dire qu'avec le cloud, le ticket d'entrée est moins élevé, ce qui permet d'adresser les entreprises plus petites ».
L'argumentaire est d'autant plus complexe à tenir qu »il n'y pas moyen de calculer le ROI d'un projet PRA », reconnaît notre interlocuteur. Tout en précisant « qu'en France, la prise de conscience est forte ».
Unitrends, qui affiche un chiffre d'affaires de 65 millions de dollars (+57% sur un an) indique protéger 1 exabyte de données dans le monde, et ses technologies de backup permettent de garantir un rétablissement après sinistre de une heure.
Par Olivier Chicheportiche | Lundi 01 Septembre 2014

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

Source :
http://www.zdnet.fr/actualites/reprise-d-activite-73-des-entreprises-ne-sont-pas-pretes-apres-un-sinistre-dans-le-cloud-39805553.htm

5 conseils pour protéger ses photos et données perso dans le cloud

5 conseils pour protéger ses photos et données perso dans le cloud

Chiffrement, mot de passe et bon sens commun sont les meilleures armes pour protéger ses données dans le cloud. Même si le risque zéro n'existe pas.

Avec le piratage des photos nues de stars féminines, le problème de la sécurité des services cloud se rappelle à notre bon souvenir. Externaliser le stockage de ses données auprès d'un service en ligne peut être très pratique, mais cela présente aussi des risques, et même de plus en plus. Lors des dernières conférences de sécurité BlackHat et Defcon à Las Vegas, les experts en sécurité sont d'ailleurs unanimes à ce sujet : à force d'interconnecter de plus en plus de services en ligne et d'objets, on augmente la surface d'attaque, et donc le risque de se faire pirater. « Un bon hacker suffisamment motivé peut pirater presque n'importe quoi aujourd'hui », estime même Dan Geer, un expert américain reconnu en sécurité informatique.
Mais alors, le combat est-il perdu d'avance ? Par forcément, car il existe un certain nombre de règles de bons sens qui permettent quand même de limiter le risque.

1) Evitez le cloud pour stocker des données confidentielles. Stocker ses photos sur iCloud ou Google Drive, c'est très pratique, notamment pour les synchroniser et les partager avec vos amis. Mais, de grâce, n'y mettez pas les clichés de vos derniers ébats sexuels. Vous pourriez le regretter.

2) Utilisez un bon mot de passe. Certains experts pensent que le service d'Apple a été victime d'un attaque par force brute, c'est-à-dire le test une par une de toutes les combinaisons possibles (voir ci-dessous). Avec un mot de passe tel que « 0123456 », votre compte explose en quelques secondes. Choisissez, de préférence, une suite aléatoire de chiffres et de lettres. Evidemment, il est impossible de s'en souvenir, c'est pourquoi il faut utiliser un gestionnaire de mots de passe tel que 1pass ou LastPass.

3) Chiffrez vos données. Si vous avez des données confidentielles et que vous voulez quand même utiliser le cloud, il y a une solution : le chiffrement préalable. Les données sont d'abord cryptées par un logiciel tel que TrueCrypt, puis envoyées vers le service de stockage en ligne. Même en cas de vol, les données sont (théoriquement) inutilisables. Certains services en ligne, comme SpiderOak, intègrent d'emblée cette procédure de chiffrement, la rendant plus simple d'usage (technologie Zero-Knowledge). Le revers de la médaille est que le chiffrement n'autorise pas certaines fonctionnalités très pratiques comme le partage ou la modification en ligne. Il faut faire un choix…

4) Analysez la sécurité de votre fournisseur. Tous les fournisseurs cloud ne sont pas au même niveau technologique. Certes, tous utilisent au minimum le chiffrement HTTPS, mais qu'en est-il du chiffrement des communications entre les datacenters (comme l'ont implémenté Google et Yahoo désormais) ? Le fournisseur propose-t-il l'authentification à deux étapes (comme Twitter, Google + ou Apple) ? Utilise-t-il la technologie Perfect Forward Secrecy pour blinder encore plus ses communications chiffrées (comme Microsoft ou Twitter) ? Cette analyse n'est pas aisée à faire, mais elle s'impose dès lors que les données sont sensibles.

5) Ne partagez pas tout avec n'importe qui. Le niveau de sécurité de vos données est égal au plus bas niveau de sécurité mis en place par vos amis avec qui vous les partagez. C'est le principe du maillon faible. Donc, sélectionnez bien les amis avec qui vous partagez vos photos confidentielles. Evitez, par exemple, d'inclure votre ex-petit ami(e) dans la liste…
Gilbert Kallenborn01netle 02/09/14 à 15h09

Pour information, Denis JACOPINI et son équipe proposent des solutions pour protéger vos données :
– protection contre la perte de données
– protection contre la fuite de données
– cryptage de clés usb, d'ordinateurs, d'espace Cloud ou de données
– renforcement des autorisations (sécurité avancée par SMS, biométrie…)
Audit – Conseils – Sensibilisation/Formation des utilisateurs à la sécurité informatique
Contactez-nous

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

Source :
http://www.01net.com/editorial/625810/vol-de-photos-de-nus-5-conseils-pour-proteger-ses-donnees-dans-le-cloud/#?xtor=EPR-1-NL-01net-Actus-20140902

Google aux commandes du droit à l’oubli

Google aux commandes du droit à l’oubli

Par Laurence NEUER

En offrant aux internautes un formulaire pour se faire oublier, Google remplit son « contrat ». Mais il ouvre aussi la boîte de Pandore. Éclairage.

Rien ne prédestinait le premier moteur de recherche du monde à se mêler des contenus qu'il référence. Et pourtant, depuis le 30 mai, Google propose aux citoyens et résidents européens un formulaire gratuit pour faire valoir leur droit à l'oubli numérique. Et ils étaient déjà après une journée plus de 12 000 à l'avoir rempli et posté !

Formulaire accessible en trois clics

Cette initiative lui a été soufflée par la Cour de justice de l'Union européenne (CJUE) qui, dans une décision du 13 mai 2014, offrait aux internautes la possibilité de s'adresser directement au moteur de recherche pour demander le retrait de certains contenus. Jusqu'à présent, le déréférencement de pages web était ordonné en justice sur le fondement du droit à la vie privée ou des données personnelles. « Le moteur de recherche n'avait pas à arbitrer, le juge remplissait son office », rappelle l'avocat Jean-Sébastien Mariez.

La réactivité quasi immédiate du géant américain peut d'autant plus être saluée que Google est ici aux antipodes de son métier de base. « C'est l'exact opposé de la philosophie sur laquelle le moteur de recherche est construit. C'est comme si vous demandiez à un cuisinier trois étoiles qui concocte des menus pour vingt-cinq couverts de préparer des repas à bas prix pour toute une cantine scolaire, relève Étienne Wéry, avocat aux barreaux de Bruxelles et de Paris. Google aurait pu attendre encore quelques mois, car la Cour n'a fait qu'interpréter le droit européen et a laissé au juge espagnol qui l'a saisie le soin d'en tirer les conséquences dans le cas d'espèce concerné. En théorie, donc, Google pourrait sortir gagnant du procès », note l'avocat.

Mais au lieu de la politique de l'autruche, le géant américain a décidé de prendre les devants. Son formulaire, accessible en trois clics et en français, est très simple d'utilisation. Il suffit de se rendre sur la page d'accueil de Google.fr, de cliquer sur « Confidentialité et conditions d'utilisation » (en bas à droite), puis sur FAQ, et de choisir la troisième question : « Comment puis-je supprimer mes données personnelles des résultats de recherche Google ? »

Mais, attention, prévient Google en amont de la procédure, « supprimer des résultats de la recherche Google n'entraînera pas la suppression des contenus correspondants. Pour que des données n'apparaissent plus sur le Web, vous devez contacter le webmaster du site publiant les informations en question. » Autrement dit, la désindexation d'un contenu n'entraînera pas la disparition de celui-ci des écrans radars du Web. Ainsi, l'internaute qui souhaite voir supprimer son profil sur un réseau social doit contacter directement le webmestre de ce dernier. De Google, il ne pourra obtenir le cas échéant que la suppression du lien vers le site ou vers des pages associées.

Par ailleurs, pour éviter les fraudes, le moteur de recherche exige des requérants la photocopie d'un document prouvant leur identité (carte d'identité, passeport, etc.). Rien de surprenant, selon Me Wery, « le droit d'accès et de rectification des données personnelles étant lui aussi subordonné à la preuve de l'identité de l'intéressé ».

Du « cas par cas »

Reste à convaincre le moteur de recherche du bien-fondé de sa demande. Concrètement, l'internaute doit indiquer « en quoi le lien apparaissant dans les résultats de recherche est non pertinent, obsolète ou inapproprié » conformément aux critères fixés par la CJUE. « L'exercice est d'autant plus délicat que les demandes de déréférencement pourront concerner des contenus qui en soi ne sont pas illicites (photo de vacances postée par un tiers, post sur un blog ou curriculum vitae périmé) et dont le retrait suppose la disparition d'une page web complète (et pas seulement du commentaire faisant référence à la personne concernée ou de l'encart précis) », souligne Me Mariez.

Dans son évaluation, Google devra prendre en compte l'intérêt du public à connaître l'information, en fonction notamment du « rôle joué par le requérant dans la vie publique ». Le moteur de recherche doit notamment veiller à préserver l'équilibre entre le droit individuel à la vie privée et à la protection des données personnelles et le droit à l'information du public, lui aussi protégé par les textes. Autant dire que les experts chargés d'évaluer le bien-fondé des demandes devront chausser des lunettes de fins juristes !

D'autant que, eu égard à la rapidité des recherches, il serait malvenu de laisser patienter trop longtemps les prétendants dans la salle d'attente du droit à l'oubli. Pour l'heure, Google a confié à un comité d'experts indépendants le soin de définir les critères et les moyens à mettre en place pour traiter les demandes au « cas par cas ». Et la question des suites de l'arrêt de la CJUE est à l'ordre du jour du G29 des 3 et 4 juin afin que les « Cnil » européennes adoptent une position commune sur le sujet. « Mais il y aura forcément des erreurs. Google fera des mécontents et se mettra en risque. S'il évalue mal une demande, il pourra faire l'objet de sanctions », pointe Me Wéry.

Les requérants pourront saisir la Cnil comme ils le font déjà après avoir essuyé un refus de la part du site où sont publiés leurs photos, vidéos, textes ou faux profils dont ils ont demandé la suppression. D'ailleurs, les plaintes liées au droit à l'oubli, en hausse de quatre points par rapport à 2012, ont représenté 34 % du nombre total de plaintes en 2013. De plus, les responsables de site qui seraient en désaccord avec la décision du moteur de recherche de supprimer leur page des résultats de recherche pourront aussi se plaindre devant la commission. En dernier ressort, c'est la justice qui tranchera. Et le contentieux promet d'être copieux…

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

Source :

http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/google-aux-commandes-du-droit-a-l-oubli-02-06-2014-1830043_56.php

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

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

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

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

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

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

---

Rendre n’importe quel objet

connecté : la « mother » est là

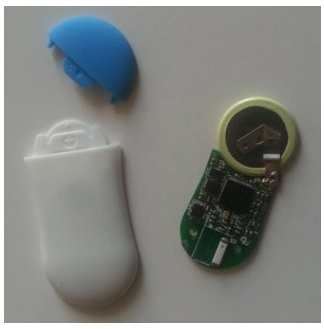
Rendre n'importe quel objet connecté : la « mother » est là

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

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

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

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



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

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

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

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

Microsoft foutu dehors par Pékin sur des doutes d’espionnage…

Microsoft foutu dehors par Pékin sur des doutes d’espionnage…

C’est la première fois que les autorités chinoises pointent officiellement du doigt l’entreprise depuis le lancement d’une enquête antimonopole le mois dernier.

L’étau chinois se resserre lentement mais sûrement sur Microsoft. Après Google, et Qualcomm, spécialiste de la technologie 4G, c’est l’entreprise fondée par Bill Gates qui se retrouve dans le viseur de Pékin. Un haut responsable des autorités de la concurrence chinoise a accusé le géant américain de l’informatique de manque de «transparence» dans ses ventes de logiciels.
Zhang Mao, le chef de la puissante administration d’État de l’industrie et du commerce (SAIC) exige que Microsoft fasse toute la lumière sur ses chiffres de ventes de logiciel «Media Player» et son moteur de recherche. C’est la première fois que les autorités pointent officiellement du doigt l’entreprise depuis le lancement d’une enquête antimonopole le mois dernier. Ces dernières semaines, les enquêteurs ont opéré des raids surprises dans sept bureaux à travers le pays et devraient délivrer leur verdict, «en temps voulu». Avec, à la clé, une possible amende pesant 10 % du revenu chinois de l’entreprise.
Microsoft est pris en otage dans la « cyberguerre » entre Washington et Pékin suite à l’affaire Snowden
Microsoft subit une offensive tous azimuts dans l’empire du Milieu, puisque les autorités viennent d’annoncer le lancement d’un système d’exploitation visant à remplacer Windows en octobre. Depuis le mois de mai, la dernière version du logiciel, Windows 8, est bannie de toutes les administrations publiques, au nom de la lutte contre l’espionnage. Microsoft est pris en otage dans la «cyberguerre» entre Washington et Pékin suite à l’affaire Snowden.
L’interdiction de Windows 8 a été annoncée quelques jours après la mise en cause de cinq militaires chinois pour espionnage par la justice américaine, le 19 mai dernier. «En représailles, la Chine renforce ses contrôles sur les firmes étrangères dans le secteur technologique et va donner la préférence aux entreprises locales dans tous les domaines où il y a des données sensibles», analyse Ian Bremmer, président du cabinet de conseil américain Eurasia Group.
Après la mise au ban de Google, qui avait refusé de collaborer avec le régime en matière de cybersurveillance des citoyens, Microsoft craint à son tour d’être éclipsé du marché chinois. Le moteur de recherche de Google est depuis victime de multiples obstacles techniques ainsi que d’attaques qui ralentissent son fonctionnement et sa part de marché a fondu.
Parallèlement à Microsoft, l’entreprise californienne Qualcomm est également visée par une enquête de l’antitrust. Soupçonné d’imposer des prix trop élevés, son président Derek Aberle a promis des «améliorations», après avoir rencontré les autorités.
Pékin examine cette semaine une nouvelle loi visant à renforcer son arsenal juridique contre le cyberespionnage. Un impératif de sécurité nationale qui fleure le protectionnisme économique et dont les entreprises locales doivent profiter. «La priorité est de développer notre propre système d’exploitation pour mettre nos informations à l’abri.»
Côté industriel, «l’ambition est de briser le monopole étranger en devenant le quatrième système d’opération aux côtés de ceux d’Apple, Google et Microsoft», explique Ni Guangnan, membre de l’Académie chinoise d’ingénierie, dans le Global Times, quotidien proche du Parti.
Ces annonces laissent sceptiques certains experts et de nombreux internautes chinois qui doutent des capacités du secteur public à accoucher d’un système fiable. «Est-on en Corée du Nord?» lance provocateur l’un d’eux sur Weibo.
Au début des années 2000, le régime avait lancé son propre «moteur de recherche du peuple». Un échec retentissant, mais le rival privé Baidu, moteur de recherche chinois, avait lui profité pleinement de l’éclipse de Google pour contrôler aujourd’hui plus de 70 % du plus grand marché du monde en ligne. C’est aujourd’hui le site le plus consulté de Chine.

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

Source :
http://www.lefigaro.fr/secteur/high-tech/2014/08/26/01007-20140826ARTFIG00374-pekin-pousse-microsoft-vers-la-sortie.php

---

Attaque informatique : JPMorgan et plusieurs autres banques ciblées

Attaque informatique : JPMorgan et plusieurs autres banques ciblées

Si au cours des derniers mois, les pirates semblaient avoir comme cibles de prédilection les entreprises des secteurs de la distribution et de la santé, ils n'en oublieraient pas pour autant les acteurs de la finance.

Selon le Wall Street Journal, le FBI enquêterait sur une série d'attaques informatiques visant des établissements financiers, dont JPMorgan, la plus grande banque des Etats-Unis et la sixième dans le monde (source : Forbes).

Une enquête aurait été ouverte début août. Des données auraient en effet été dérobées à la banque par l'intermédiaire de code malveillant injecté par des hackers dans l'ordinateur personnel d'un employé de JPMorgan.

Mais l'entreprise ne serait pas la seule ciblée. Selon des sources proches de l'enquête, deux à cinq autres banques pourraient elles aussi avoir été attaquées. Les établissements bancaires font des proies de choix pour les cybercriminels. Plusieurs d'entre eux ont déjà été visés cette année, dont Wells Fargo, J.P. Morgan Chase, Bank of America, Citigroup, et HSBC.

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

Source :
http://www.zdnet.fr/actualites/jpmorgan-et-plusieurs-autres-banques-attaquees-39805373.htm

---

La dangereuse faille informatique Heartbleed constitue toujours une menace

La dangereuse faille informatique Heartbleed constitue toujours une menace

Près de cinq mois après la révélation de la vulnérabilité Heartbleed, IBM dresse un premier bilan, avec le rapport trimestriel de sa division X-Force, en s'appuyant sur les informations retirées des infrastructures des clients de ses services de sécurité managés. Et celui-ci s'avère contrasté.

La bonne nouvelle, c'est que l'intérêt malveillant pour la vulnérabilité semble s'être sensiblement tassé : si IBM a enregistré jusqu'à plus de 300 000 attaques par jour exploitant Heartbleed le 15 avril dernier, le chiffre est rapidement retombé, à quelques centaines d'incidents par jour fin avril. L'effet de grandes entreprises qui ont été capables de mettre rapidement en œuvre des contre-mesures. De quoi pousser les attaquants à déplacer leurs efforts sur d'autres vulnérabilités. Pour autant, l'activité malveillante liée à Heartbleed se maintient, explique IBM, estimant qu'environ « 50 % des serveurs potentiellement vulnérables ont été laissés sans correctif ». De quoi faire, pour le groupe, de la vulnérabilité « une menace continue et critique ».
Mais pour IBM, le plus important est peut-être à chercher du côté de la gestion de la réaction : « disposer d'un plan de réaction aux incidents – et d'une base de données à jour des actifs – s'est avéré absolument critique pour réduire l'exposition au risque. » En outre, selon le groupe, si les pare-feux ont pu rapidement offrir une protection pour les systèmes concernés, les dispositifs de détection et de prévention des intrusions ont pu « fournir une protection encore plus importante en bloquant les attaques au niveau des paquets ». D'autant plus que les attaquants semblent avoir privilégié la carte de l'exploitation distribuée de la vulnérabilité Heartbleed, rendant plus difficile la protection par des pare-feux.

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

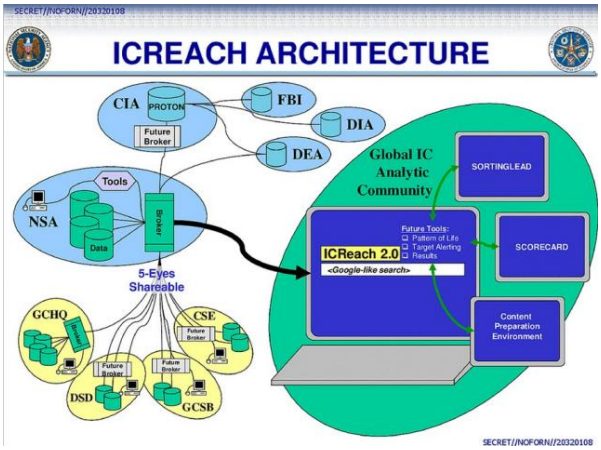
Source :
http://www.lemagit.fr/actualites/2240227500/Heartbleed-constitue-toujours-une-menace?asrc=EM_MDN_33243175&utm_medium=EM&utm_source=MDN&utm_campaign=20140827_L%27essentiel%20IT%20:%20Premi%e8re%20politique%20globale%20de%20s%e9curit%e9%20en%20France%20-%20VMWare%20se%20convertit%20aux%20appli_

ICReach, le moteur de recherche secret «à la Google» de la NSA

ICReach, le moteur de recherche secret «à la Google» de la NSA

Certes, la NSA est une agence secrète, mais entre bons amis, elle concède volontiers de partager des informations. Et même beaucoup d'informations, comme le prouve l'existence d'ICReach.

Révélé par The Intercept, sur la base de documents d'Edward Snowden, ce programme de surveillance compile plus de 850 milliards de métadonnées récoltées dans le monde entier et les rend accessibles au travers d'un moteur de recherche « à la Google » auprès d'une vingtaine d'agences gouvernementales américaines. Comme par exemple la CIA (service secret), le FBI (police fédérale) ou le DEA (agence de lutte anti-drogue).



Plus d'un millier d'agents gouvernementaux américains ont ainsi accès à une véritable mine d'or informationnelle. En effet, ICReach compile non seulement des métadonnées téléphoniques, mais aussi des métadonnées relatives aux communications emails et aux messageries instantanées. Au total, ce moteur de recherche référence plus d'une trentaine de champs : temps et durée d'appel, numéros d'appel, protocole, IMEI (identifiant unique du smartphone), identifiant de la cellule mobile de réception, adresse email, identifiant chat, etc. Les données proviennent d'une multitude de bases de données gérées par la NSA, mais aussi par les partenaires du club « Five Eyes » (Royaume-Uni, Australie, Nouvelle-Zélande, Canada).

Les métadonnées surveillées par ICReach.
Ainsi, l'enquêteur pourra savoir qui communique avec qui et depuis quel endroit. Mais ce n'est qu'un début. En croisant toutes ces données, l'objectif est de pouvoir extraire les habitudes de vie quotidienne d'une cible : quels endroits elle fréquente, avec qui et à quel moment, etc. La NSA appelle cela « pattern of life analysis » (« analyse du mode de vie »).
Il est difficile de savoir combien de personnes peuvent être potentiellement surveillées par cet outil. Il concerne principalement des non-Américains, dans la perspective d'un « renseignement extérieur » (« foreign intelligence »). Ce qui est assez vague et peut aller de la guerre anti-terroriste à l'espionnage économique, en passant par la lutte contre la criminalité organisée.
Comme bon nombre de programmes de surveillance de la NSA, ICReach trouve son origine dans les attentats du 11 septembre, qui avaient révélé un manque de communication entre les différentes agences gouvernementales américaines. Un problème qui, visiblement, a été résolu. Attention, ICReach n'est pas à confondre avec XKeyscore, un autre moteur de recherche célèbre de la NSA. Mais celui-ci est davantage restreint au monde de l'espionnage. Par ailleurs, il ne cible que les données du web.

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

Sources :
http://www.01net.com/editorial/625470/icreach-le-moteur-de-recherche-secret-a-la-google-de-la-nsa/#?xtor=EPR-1-NL-01net-Actus-20140826
https://firstlook.org/theintercept/article/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/