Sécurité des données : les entreprises récoltent une mauvaise note

Les entreprises récoltent une mauvaise note en matière de sécurité de données

Une étude internationale a interrogé 450 décideurs informatiques et révèle que de nombreuses sociétés se heurtent aux exigences de gouvernance et de sécurité des échanges de données.

« Les entreprises doivent respecter des exigences réglementaires toujours plus strictes en termes de conformité et de sécurité des données… »

23% des entreprises ont récemment échoué à un audit de sécurité, tandis que 17 % doutent de leur capacité à réussir un audit de conformité des échanges de données. C'est ce que révèle l'étude publiée par Axway, éditeur de logiciels spécialisé dans la gouvernance des flux de données ainsi que par le cabinet d'analyse Ovum. « Un audit de sécurité contrôle les systèmes et analyse leur perméabilité, précise Jean-Claude Bellando, directeur solution marketing pour Axway. Le but est de savoir si les données de l'entreprise sont exposées ou pas. »

Car pour se développer, les échanges entre partenaires nécessitent l'établissement d'une relation de confiance. Mais à l'heure de l'économie numérique, la confiance est relative à la sécurité, l'intégrité et la confidentialité des données échangées. Une relation d'autant plus difficile à établir que les partenaires n'ont pas forcément conscience du parcours et des étapes suivis par ces données. « Les partenaires décident alors d'un niveau d'exigence à atteindre, sur la base des règles et des bonnes pratiques de sécurité disponibles, ajoute Jean-Claude Bellando. Une règle communément admise consiste par exemple à proscrire les échanges via le protocole FTP. »
Coût de l'exposition. Pour préparer l'application de ces règles et bonnes pratiques mais aussi pour vérifier leur bonne application, les entreprises ont recours à des audits de sécurité. Ainsi récemment, Google, le géant de l'Internet, anticipant les craintes de ses clients entreprises, a décidé de publier unilatéralement les résultats d'audit de sécurité réalisés par deux cabinets indépendants. Ce type d'audit est de plus en plus souvent réalisé à la demande des clients de l'entreprise. Si celle-ci n'est pas en mesure de démontrer le respect des règles de sécurité, considérées comme nécessaires au bon déroulement de la relation commerciale, ses clients pourraient arrêter de travailler avec elle. L'enquête ajoute ainsi que le coût total moyen d'une atteinte à l'intégrité des données s'élève à 2,4 millions d'euros. « Les répercussions des cyberattaques sont sérieuses sur le plan économique et pour l'image de l'entreprise », explique Jean-Claude Bellando.

Pour répondre à ces problématiques, Axway préconise une gestion groupée de l'intégration informatique et de la gouvernance d'entreprise. Or, dans la majorité des entreprises (71%), la stratégie d'intégration n'est pas alignée avec les structures et les politiques de gouvernance, de confidentialité et de sécurité des données. « Les entreprises doivent respecter des exigences réglementaires toujours plus strictes en termes de conformité et de sécurité des données, indique Dean Hidalgo, vice-président exécutif en charge du marketing d'Axway. En s'appuyant sur des technologies éprouvées de gestion de transfert de fichier (MFT) et de gestion d'interfaces de type API (Application Programming Interface), sur site ou dans le cloud, et en développant une stratégie d'intégration plus globale et unifiée, les organisations sont en mesure de gouverner leurs flux de données à travers l'ensemble de leur écosystème, en interne comme en externe. »
Par Caroline Albenois

Premier type de risque : Les attaques venant de l'extérieur.
Solution : Demandez un test de pénétration (PENTEST) de votre système informatique à Denis JACOPINI

Second type de risque : Les actes malveillants, illicites ou défaillances internes à votre entreprise.
Solution : Demandez un audit de sécurité infomatique à Denis JACOPINI

Troisième type de risque : Votre système de traitement de données informatiques n'est pas réglementaire selon la loi Informatique et Libertés et des déclaration ou complémentats de déclaration à la CNIL doivent être effectuées.
Solution : Demandez un audit de mise en conformité CNIL à Denis JACOPINI

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

Source :
http://www.info.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,I1602,Zoom-ce92e8de85306f8f94bb572e6ec6d325.htm

Juniper Networks présente ses prédictions réseau, cloud et sécurité pour l’année 2015

Juniper Networks présente ses prédictions réseau, cloud et sécurité pour l’année 2015

Bientôt, nous allons atteindre et même dépasser la barre des 5 milliards d'utilisateurs connectés. Il y a trente ans, l'innovation était un concept à sens unique, une démarche clairement orientée entreprises, où les consommateurs passaient au second plan. Depuis, les choses ont changé. Alors que près de la moitié de la population mondiale est connectée à Internet, les consommateurs ont désormais leur mot à dire et exigent des applications et services innovants pour la qualité de leur vie, à leur rythme et à leurs conditions.

L'environnent de l'entreprise est contraint d'évoluer au rythme des innovations, chaque année, plus nombreuses. Bruno Durand, vice-président TCC, EMEA, chez Juniper Networks a analysé les tendances 2015 dans les réseaux, le cloud et la sécurité. Il partage aujourd'hui ses conclusions avec vous.

Réseaux intelligents : La diffusion de contenu sème la confusion chez les câblo-opérateurs
Si la tendance est au numérique depuis plusieurs années, l'industrie du câble n'a pour ainsi dire pas évolué. Mais 2015 sera l'année du changement. Avec l'avènement et l'essor de la diffusion de contenu en streaming, les abonnés, qui se tournent vers différents fournisseurs de contenu comme Netflix, commencent à demander de nouveaux services à leurs câblo-opérateurs. Selon le rapport « U.S. Digital Video Benchmark » publié cette année par Adobe, le nombre des consommateurs de contenu en streaming a augmenté de près de 400 % depuis l'an dernier. Cette tendance devrait se poursuivre, et pour rester dans la course et gérer l'augmentation du trafic IP, les câblo-opérateurs devraient miser sur les réseaux virtualisés en 2015. Même si la transition durera plusieurs années, ils vont d'ores et déjà examiner les possibilités qui s'offrent à eux et commencer à lancer des appels d'offres pour trouver des fournisseurs partageant leur vision.

Le trading hypercontextuel (HCT) supplante le trading à haute fréquence
Passé de 7 milliards de dollars en 2008 à 1,4 milliard de dollars en 2013, le trading à haute fréquence est sur le déclin. Il représente à l'heure actuelle moins de 50 % des volumes d'activité des marchés financiers, contre 70 % en 2008. Le trading HCT (hypercontextuel) constitue le nouveau mouvement de dérèglement du marché. Il repose sur l'assimilation en temps réel des fils d'actualités classiques (Bloomberg, Thomson-Reuters, AP, CNN) et des flux des réseaux sociaux (Twitter, Facebook, LinkedIn, Blogs, etc.) en vue d'exploiter les informations du marché et d'acquérir un avantage concurrentiel en termes de transactions boursières. Le tout est piloté par des analyses permettant le chargement, le traitement et l'extraction rapides des données dans le but de tirer parti des discontinuités du marché. Le trading HCT relève de l'informatique distribuée et de la performance. La latence est le principal enjeu et ne constitue plus un facteur de différenciation. Un système extrêmement intelligent s'impose. Les entreprises et leur environnement informatique vont devoir pré-assimiler plusieurs centaines de flux d'informations en temps réel, ce qui nécessitera une programmation et un équipement réseau extrêmement pointus.

Big Data et réseaux : un bien ou un mal ?
Face à l'« Internet des objets », dont les tentacules (les terminaux) continuent de se déployer dans nos vies, les données générées vont être beaucoup plus nombreuses. Ainsi une simple connexion entre un téléphone et un système de sécurité résidentiel produira des données qu'il faudra bien stocker quelque part. En 2015, il s'agira à la fois d'analyser ces données, de les interpréter via une infrastructure réseau appropriée et de les sécuriser au moyen de technologies dédiées. Les entreprises et opérateurs de télécommunications revoyant leurs méthodes de développement de réseaux pour gérer la déferlante de données, la demande de spécialistes des données va atteindre des niveaux record.

Cloud : Des clouds privés d'un nouveau genre vont apparaître
Les entreprises hors de la sphère informatique habituelle exploiteront le cloud autrement pour proposer leurs produits et services. L'essor des paiements mobiles, la multiplication des équipements connectés et les questions de sécurité qui en découlent vont transformer les marchés verticaux de manière radicale. À l'instar de Nike, autrefois spécialisé dans les vêtements de sport et désormais marque lifestyle connectée avec ses dispositifs de suivi, ou de Starbucks, devenu un grand adepte des paiements mobiles et de la diffusion de contenu, nombre d'entreprises vont créer des clouds privés pour répondre aux exigences de leurs clients. Si le cloud, comme toute nouvelle technologie, était au départ l'apanage des chefs de file du secteur des hautes technologies (sites web, services financiers), les entreprises du monde entier et de tous horizons – par exemple, les compagnies pétrolières et gazières comme Hess – vont, elles aussi, pouvoir s'y mettre. En 2015, la création de clouds permettra de se démarquer dans tous les secteurs.

Les solutions SDN en 2015
Les réseaux SDN (Software-Defined Network) vont se multiplier, à mesure que le marché et la technologie gagnent en maturité et que de plus en plus d'entreprises prennent conscience de la valeur de ces solutions. Les entreprises françaises commencent à voir les avantages du SDN selon une étude publiée cette année par Juniper : automatisation accrue, sécurité renforcée et centralisation dans la gestion des ressources. Si, en théorie, ils peuvent faciliter la gestion des réseaux et réduire les coûts, qu'est-ce que les entreprises vont réellement en faire ? Le SDN (couplé aux analyses) procure l'agilité nécessaire pour fournir des services avant que les clients ne les réclament.

Sécurité : Le marché noir continue de gagner en maturité
Selon une étude réalisée par RAND Corporation et Juniper Networks, les marchés noirs de la cybercriminalité ont atteint un niveau de maturité significatif. Et, cette tendance devrait se poursuivre en 2015. Face à la vulnérabilité persistante des systèmes de point de vente et l'afflux de services cloud, les pirates motivés par l'argent ont de beaux jours devant eux.

De nouveaux outils de piratage et kits d'exploitation des vulnérabilités des systèmes informatiques devraient voir le jour. Par ailleurs, malgré les mesures de répression prises par les services de police à l'encontre des sites web frauduleux tels que Silk Road, de nouveaux marchés devraient se développer pour répondre à la forte demande d'enregistrements volés et autres biens illicites. Les principaux fournisseurs de cloud et sites marchands étant la cible d'attaques à grande échelle, le nombre de cartes bancaires et autres identifiants proposés à la vente sur le marché noir devrait demeurer significatif.

L'analyse des données s'étend à la sécurité
Face à la volonté permanente de fournir des renseignements mieux exploitables et de meilleure qualité sur les menaces, on peut s'attendre à une hausse de la demande de spécialistes des données dans le domaine de la sécurité (« Data Scientists »). Déjà fortement sollicités dans d'autres secteurs, les professionnels capables de fournir des données plus précises sur les menaces seront extrêmement recherchés. C'est en appliquant les meilleures pratiques de la science des données à la sécurité que les entreprises disposeront de renseignements fiables et utiles sur les pirates et leurs attaques, et parviendront à se démarquer.

Sécuriser l'Internet des objets
Face à la multiplication des équipements connectés à Internet, le nombre de pirates et d'attaques a de fortes chances d'augmenter. À l'ère de l'Internet des objets, les entreprises qui ne s'étaient jamais soucié de la sécurité de leurs logiciels ne vont plus pouvoir se voiler la face, sous peine de s'exposer à de lourdes conséquences. Les pirates capables de prendre le contrôle à distance d'équipements médicaux, de voitures, de thermostats et autres systèmes physiques représentent une menace de taille pour la société. Les sociétés qui développent ces technologies doivent désormais intégrer la sécurité dans leur processus et mettre au point des outils permettant de corriger rapidement les systèmes concernés. À défaut, les risques de piratage logiciel des environnements et systèmes physiques stratégiques seront bien plus nombreux.

Nette amélioration de la confidentialité des données des utilisateurs
La confidentialité des données jouera un rôle majeur dans le développement et l'adoption de nouveaux produits. Suite aux récentes révélations sur les programmes de surveillance à grande échelle des administrations et services de police, les individus sont nettement plus intransigeants sur la confidentialité de leurs données, et les sociétés l'ont bien compris. Apple a, par exemple, renforcé la sécurité de son nouvel iPhone et de son système d'exploitation en mettant au point un système de cryptage par défaut qui va jusqu'à lui interdire l'accès aux données en sa qualité d'éditeur. Résultat : il ne peut pas fournir d'informations sur ses clients à d'autres parties, comme l'administration, et les oblige ainsi à contacter directement l'utilisateur.

Outre la sécurité renforcée des produits grand public, les applications de communication respectueuses de la confidentialité vont commencer à se généraliser. Face à des utilisateurs soucieux de la protection de leurs données, les applications comme Wickr et Silent Circle vont gagner en popularité.

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

Source : http://www.globalsecuritymag.fr/Juniper-Networks-presente-ses,20141210,49338.html
par Juniper Networks

4 bonnes raisons d’aimer Google (par Phil Jeudy)

4 bonnes raisons d’aimer Google (par Phil Jeudy)

Oui, je sais. Je suis fou d'écrire ça. La mode est à l'anti-Googlisme. Partout, on veut se payer la tête de Google, son évasion fiscale, ses commercialisations de données personnelles, son lobbying Bruxellois, ses histoires de coeur, que sais-je.

Je visitais un entrepreneur Français de la Silicon Valley la semaine passée, et il me rappelait a priori des propos échangés il fut un temps : » C'est une boite de merde, Google, hein ?! ». Bon, alors j'ai dit ça, mais là, je vais dire autre chose.
Google souffre d'un problème lié au temps modernes : la technologie est de plus en plus complexe, et passe de moins en moins vis à vis du grand public, parce qu'il faut s'arracher les cheveux pour montrer des choses qui parfois ne peuvent pas se voir facilement, à l'écran ou sur du papier journal.
Et je pense que, à l'image d'une presse politique plus intéressée d'une façon générale par des ronds-de-jambe d'arrière cour que de rendre une image fidèle de la situation du pays, la presse spécialisée se complait à prendre son audience pour des ignares, et tout ceci fait que l'on n'explique jamais assez comment les nouvelles technologies rendent service à leurs utilisateurs. Parler de quincailleries, et du dernier iPhone 12 et du Samsung 28, ça, c'est facile, y a qu'à comparer des chiffres. Mais se creuser la tête pour comprendre ce que fait une startup dans le domaine du cloud computing comme Docker, non Madame, y a trop de travail.

Amis lecteurs, on ne vous explique pas assez comment ça marche, Internet. Et d'ailleurs des sociétés comme Google ne le font pas suffisamment bien, c'est fort possible. Une compagnie mondiale, équipée d'agents commerciaux dans tous les pays, n'est pas la meilleure quand il s'agit de s'adresser aux marchés locaux, loin des « product managers » qui se creusent la tête pour vous servir les produits de demain. Vous ne parlez qu'à des vendeurs de soupe, des marchands de pub.
Je viens de rencontrer une équipe de journalistes français en visite professionnelle à San Francisco pour se poser des questions sur la société de Mountain View, avec des bons éléments de réflexion en tête. Ça nous change. Et franchement ça m'inspire ces quelques petits rappels qui me paraissent importants à garder en tête…

1. Les services de Google sont gratuits.
Si vous utilisez l'application Gmail de messagerie de façon normale, et que vous ne stockez pas trop de fichiers, vous ne payez rien. Vous ne payez pas pour utiliser la carte Google sur votre smarphone, pas plus que les fichier en ligne de Google Drive. Les requêtes sur le moteur de recherche ? Gratuites. Utiliser Blogger pour publier des histoires sur Internet, on ne paye pas. Utiliser un outil de traduction, stocker un nombre raisonnable de photos sur Internet ? Idem. Bloquer son téléphone Android qu'on vient de vous voler ? Service gratuit. Derrière la grande utilisation d'informations que Google opère selon leurs conditions générale d'utilisation, de vente et de tutti quanti, pleins d'outils à votre disposition au prix de 0 la tête à toto.

2. Vos données personnelles servent à améliorer des outils mis à votre disposition d'une façon générale gratuitement.
Internautes, Internautesses, on vous ment, on vous spolie. Derrière beaucoup d'anti-Googler, il y a une Arlette qui sommeille. Et qui oublie de vous dire aussi que l'utilisation de vos données personnelles servent à Google à perfectionner les outils mis à votre disposition. Il n'y a pas que la publicité que l'on vous sert en priorité, il y a toutes ses passerelles entre les produits Google : entre une recherche faite sur un ordinateur qui est mémorisée lorsque vous passez sur le browser de votre téléphone (si vous utilisez Chrome, cela va de soi), pour vous délivrer des informations sur mesure avec Google Now qui cherche à vous simplifier la vie (à défaut de pouvoir bien l'organiser, il y a encore du travail). Lorsque vous travaillez sur votre outil de messagerie, Google travaille à vous apporter le sucre alors que vous allez chercher votre café sur Internet. La meilleures façon de protéger vos données ? Tenez les loin d'Internet, votre meilleur outil de sécurité, ce sont vos doigts.

3. Google vous protège, dites lui merci.
Quand on regarde de près le mode connecté d'aujourd'hui, avec tous ces téléphones portables, routeurs, modems, ordinateurs portables, et bientôt votre lunettes, vos T-shirt connectés, le web est une grande passoire trouée. Estimez vous heureux que les hackers soient encore une race à part, organisée mais minoritaires, et essentiellement à but politique. Le jour où ces anonymes vont s'organiser par district et se soulever collectivement, vous allez vite réaliser à quel point vos données les plus fragiles sont accessibles. Mêmes les photocopieurs s'y mettent, des milliards de photocopies stockées sur des mémoires installées sur ces matériels par leurs fabricants se baladent en ce moment sur Internet. Des entreprises plus grosses que Google se font attaquer par des cyber-criminels en permanence, et bien que la nouvelle n'arrive pas à vos oreilles, car tout est fait pour éviter le scandale, la réalité est bien là : devant la grande abime d'un web où rien n'est vraiment caché, nous sommes tous à poil. Et bien Google, avec ses mots de passes, ses serveurs sécurisés, ses procédures, c'est un peu de protection dans un monde de brutes.

4. Google s'améliore. Dites aussi merci.
Je suis, par la force des choses, un « tout-Google ». Je dispose d'un matériel qui ne permet pas d'utiliser simplement des licenses de Microsoft, je me suis déjà fait voler un ordinateur (et perdu au passage des années-photos), et j'utilise les services au quotidien de produits poussés par quelques 50.000 et quelques employés. Google Voice reconnait mon anglais quoique polishé, l'accent est toujours bien là. Les outils de traduction sont encore plus simples à utiliser. Les outils de messagerie demande du temps d'adaptation, les résultats des requêtes sont de plus en plus visuels et agréables à consulter… L'impression générale est là : les outils marchent de mieux en mieux, et en plus de ça quelques acquisitions comme Waze pour le GPS, l'Uber embarqué dans la cartographie, le design, tout ça va dans le bon sens. Les outils de Google sur mobile vont à contre-pied de l'univers surfait des applications mobiles qu'on vous vend à gogo, tel le marchand de poisson pas frais de la BD d'Astérix, et c'est la bonne direction pour les années à venir : de la simplicité, pas de surf sur des écrans jamais assez grands… de l'interactif, du conversationnel. Quoi de plus normal sur un téléphone portable ! Faites dont l'expérience vous-mêmes, parlez lui donc, à votre smartphone, vous verrez bien.

Les problèmes de fonds restent entiers, tant d'un point de vue fiscal que légal, mais tout ce micmac reste bien éloigné des problèmes qu'un utilisateur de base comme moi peut avoir au quotidien.
Alors, verser un peu de rose et une petite dose de bonnes nouvelles dans un monde bleu et froid plein d'effroi, ça n'a jamais fait de mal.

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

Source : http://www.huffingtonpost.fr/phil-jeudy/avantages-google_b_6292352.html
par Phil Jeudy

Les données personnelles solubles dans le livre numérique

Les données personnelles solubles dans le livre numérique

La sécurité des utilisateurs, autant que la confidentialité de leurs données personnelles, a été mise à mal dernièrement. Découvrir que la société Adobe, comme d'autres, collecte des renseignements sur les lecteurs et leurs ouvrages est choquant. Surtout que cet espionnage, et la violation de droits constitutionnels font écho à d'autres révélations de plus vaste ampleur.

opensource.com CC BY SA 2.0

Andrew Roskill, CEO du service BiblioLabs, qui fournit les bibiothèques de prêt en contenus numériques, pose le problème de manière simple. Si l'actualité nous a appris à devenir méfiants, face aux surveillances multiples des réseaux, le contrôle de nos lectures est loin d'être supportable. Et plus encore, le livre numérique emprunté dans un établissement n'a pas vocation à devenir un ensemble de Big Data, que les sociétés pourront stocker et commercialiser.

Bien entendu, note-t-il, le modèle économique d'Amazon repose sur ce traitement des données personnelles. Le moteur de recommandation s'inspire sur les visites faites sur le site de vente, ainsi que les achats, le tout recoupé avec les données des autres clients. « Mais il y a une différence entre le comportement d'achat et celui de lecture, et nous aimons à penser que nos lectures restent confidentielles », poursuit-il.

Le sentiment de sécurité offert par le prêt de livres papier, et qui est garanti dans la législation américaine, devrait être reproduit dans l'univers dématérialisé. Ainsi, les révélations portant sur le comportement du logiciel d'Adobe, Digital Edition ont causé du tort au service de prêt numérique. Non seulement ADE surveillait les lectures, mais, surtout, les diffusait à ses serveurs sans aucun cryptage. Ce dernier point a été reconnu, et corrigé, mais le premier reste d'actualité.

« Certains fournisseurs ont tenté de faire valoir que la collecte de données personnelles est nécessaire pour améliorer l'expérience de l'utilisateur, que les serveurs ont besoin de données spécifiques à l'utilisateur pour synchroniser les ebooks à travers les dispositifs, permettant aux lecteurs de passer d'un lecteur à un autre, sans perdre le fil du récit », rappelle Roskill.

Sauf que pour assurer un suivi des lectures, d'un appareil à l'autre, il n'est pas du tout obligatoire de collecter les données personnelles des utilisateurs, affirme-t-il. Et il n'est pas vrai non plus que les éditeurs ou les libraires ont besoin de données individuelles pour suivre les comportements d'achats – et, éventuellement, orienter leur ligne éditoriale. Une agrégation de données suffirait amplement pour avoir une vue d'ensemble satisfaisante.

Bien entendu, les services de BiblioLabs proposent un anonymat maximal, promet-il, et garantissent une sécurisation des données transférées. « La confidentialité et la sécurité sont extrêmement importantes pour les bibliothèques et leurs usagers. » Parce que, ce qui prime, c'est la confiance que ces derniers accordent aux établissements, pour que les bibliothèques elles-mêmes puissent avoir envie de recourir aux services les plus respectueux. (via BookBusiness Mag)

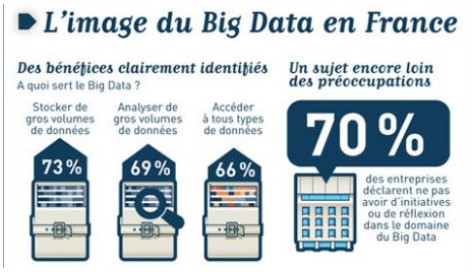
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : https://www.actualitte.com/usages/les-donnees-personnelles-solubles-dans-le-livre-numerique-54229.htm

Comment stocker ses données en toute sécurité

Comment stocker ses données en toute sécurité

L'actualité du piratage et du vol de grandes bases de données, de fichiers de clients, est hélas toujours très riche et risque de ne pas se tarir, au contraire (voir par exemple, cette très instructive « dataviz » des plus grandes bases de données piratées et la très riche collecte d'informations de La Quadrature du Net sur le « privacy nightmare », le cauchemar du respect de la vie privée).



Dernier en date, Domino's Pizza, qui s'est vu dérober une base de 600 000 noms, prénoms, adresses postales, numéros de téléphone, courriels et parfois codes d'entrée d'immeuble. Ou Sony, comme le rapporte Courrier International et l'a raconté Rue89, qui s'est fait pirater des dizaines de milliers de documents…

Grosses données, grosses responsabilités
Dans une interview pour l'édition américaine du Huffington Post, Sandy Pentland, spécialiste des Big Data, ces énormes masses de données que collectent opérateurs et services web (cf. « Big Data, vers l'ingénierie sociale ? »), rappelle une règle de sécurité assez simple à l'intention des entreprises. Les organisations doivent apprendre qu'elles ne peuvent stocker leurs données à un seul et unique endroit.

Capture d'écran de l'interview (HuffingtonPost.com)

Elles doivent les organiser par répartition, en séparant chaque type de données, en utilisant différents systèmes informatiques et différentes techniques de chiffrement. Avec la collecte des Big Data, viennent de grandes responsabilités pour éviter les « Big brèches », les « gros dommages », c'est-à-dire les risques de piratage informatique majeur. La restauration de la confiance du public après les révélations d'Edward Snowden est à ce prix.

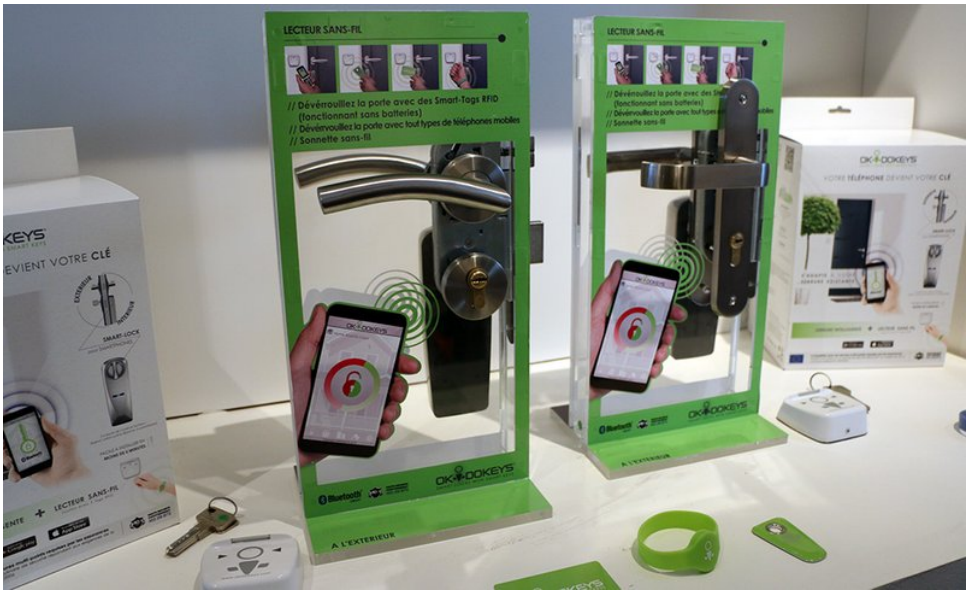
Comme l'explique Sandy Pentland :
« Les ressources informatiques et humaines doivent toujours être redondantes et fragmentées afin d'éviter que des acteurs centraux trop puissants, qui peuvent être corrompus, ne puissent passer outre les précautions de sécurité standards. »

Il y a encore des progrès à faire ! Notamment et avant tout chez les fournisseurs de service de fichiers clients et de bases de données, qui souvent proposent des solutions bien trop centralisées…

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

Source : http://rue89.nouvelobs.com/2014/12/09/repetez-apres-dois-stocker-toutes-donnees-meme-endroit-256466
par Hubert Guillaud

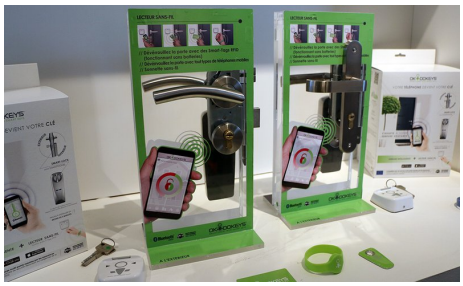
Okidokeys : la serrure connectée à la française bientôt disponible



Okidokeys : la serrure connectée à la française bientôt disponible

En vente depuis 6 mois aux Etats-Unis, la serrure connectée de l'entreprise française Okidokeys s'apprête à être commercialisée en Europe. Que se cache-t-il vraiment derrière ce produit, destiné à être installé très rapidement sur n'importe quelle porte ?

Assez peu connue du grand public, l'entreprise française Okidokeys est pourtant l'une des pionnières en matière de serrure connectée. Il s'agit d'une filiale d'OpenWays, dont le cœur de métier cible, à la base, les hotels, dont certains utilisent depuis longtemps déjà des systèmes de clés électroniques pour l'ouverture des portes des chambres.
Okidokeys cible de son côté les particuliers désireux d'utiliser la ou les serrures de leur logement d'une autre manière, principalement avec un smartphone, mais pas seulement. Car la serrure connectée, si elle se présente sous une unique forme de base, peut être complétée par différents éléments qui permettent d'en renforcer l'usage.
La serrure en elle-même s'installe à l'intérieur du logement, sur une serrure déjà existante. La mise en place n'est censée prendre que quelques minutes, et tout le nécessaire, jusqu'au tournevis, est inclus dans la boîte. Certains impératifs doivent être vérifiés avant l'achat : la serrure de base doit notamment disposer impérativement d'un cylindre européen pour être compatible. L'épaisseur de la porte doit également être contrôlée.



Le maître des clés
« Par rapport aux serrures américaines, qui ont souvent de simples loquets, les serrures européennes ont été un défi » explique Pascal Metivier, le PDG d'Okidokeys. « La principale difficulté a été d'adapter le mécanisme qui ouvre la porte aux serrures 3 ou 5 points. » Les assurances demandent généralement la présence d'une serrure 3 points minimum pour la couverture d'un logement. La serrure d'Okiokeys est compatible avec ce type d'installation.
Concrètement, le « robot », une fois installé, agit sur le cylindre de la porte pour l'ouvrir ou la verrouiller. Le reste est essentiellement l'affaire de la connectique Bluetooth, qui permet de connecter un smartphone pour interagir avec la serrure. Tout est chiffré en 256 bits AES, une mesure de protection très répandue et efficace, assure l'entreprise. La clé de chiffrement est différente pour chaque serrure : pas de risque de voir sa porte ouverte par un voisin qui aurait le même modèle.
Différentes clés peuvent être programmées par le biais d'une interface Web, elle aussi sécurisée. L'administrateur peut autoriser, gratuitement, jusqu'à 10 personnes à accéder à jusqu'à 5 serrures. Des plages horaires et des jours peuvent être délimités, pour, par exemple, autoriser une femme de ménage à entrer seulement à certains moments.
Différents paramètres peuvent également être réalisés par le biais de l'application mobile, disponible sur iOS et Android. On peut, par exemple, autoriser temporairement l'ouverture d'une porte quand le smartphone en est proche : pratique quand on a les bras chargés. La serrure peut également se fermer automatiquement.
Bien évidemment, tout ceci n'empêche pas d'utiliser une bonne vieille clé manuelle, qui garde la priorité sur la serrure à l'extérieur. A l'intérieur, un loquet permet de fermer la porte à la main.

RFID, NFC et CAC à la rescousse
La serrure fonctionne à l'aide de 4 piles LR6, pour une autonomie d'un an. Lorsque les piles arrivent en fin de vie, le système le fait savoir 6 semaines à l'avance, et insiste de plus en plus pour qu'on les change, jusqu'à empêcher la fermeture électronique.
Le vrai risque question autonomie concerne davantage le smartphone : si on n'a plus de batterie et pas de vraie clé sur soi, comment faire ? Okidokeys a la réponse : il s'agit d'une sonnette connectée, qui dispose de plusieurs systèmes de lecture. Outre le NFC d'un téléphone, elle peut lire des puces RFID programmées à l'avance pour l'ouverture de la porte. Ces dernières sont disponibles sous la forme de cartes à mettre dans son portefeuille, de porte-clés ou encore de bracelets étanche. Une solution de secours, mais également de nécessité si on ne dispose pas d'un smartphone. En cas de perte, ces éléments peuvent être rapidement désactivés sur le site.
La sonnette connectée intègre également le système CAC, pour « crypto acoustic credential ». Ce dispositif, utilisé dans certains hôtels, permet d'utiliser un téléphone mobile « traditionnel » pour ouvrir une porte à l'aide d'une séquence sonore sécurisée. L'utilisateur reçoit un SMS avec un code, il doit ensuite appeler un numéro vert, qui va jouer un son pour la sonnette. Cette dernière est capable de l'interpréter, de le valider et d'ouvrir la porte si tout est en règle.

Une ouverture à Internet
A ce stade, tout se passe en local. Mais Okidokeys propose également un pack incluant un module, appelé Gateway, qui se connecte à une box et relie donc la serrure à Internet. Il est ainsi possible de savoir, en temps réel sur son smartphone, si la porte a été ouverte, et par quel moyen. La serrure intègre également une alarme, qui va retentir en cas d'entrée forcée. Là encore, l'administrateur est prévenu à distance, à condition de disposer de cette extension Internet.

Okidokeys dongle

On se retrouve donc face à trois solutions : la serrure de base, celle avec la sonnette et les tags, et celle qui permet, en plus du reste, de connecter le site à Internet. Tout ceci a un prix non négligeable : le premier pack est proposé au tarif de 250 euros, le second à 350 et le troisième à 450.

La démonstration d'Okidokeys est efficace et le système est convaincant. Néanmoins, il apparaît également destiné à des personnes qui ont un besoin important d'optimiser l'accès à leur logement. Si la démarche commence à avoir du sens dans un environnement familial – où les parents donneront des bracelets RFID aux enfants, par exemple – il en a presque encore plus dans le cadre d'une location mesurée, pour les adeptes de services de type Airbnb. Ce n'est d'ailleurs pas pour rien si l'interface en ligne passe en mode payant – 35 euros par an – si l'on désire enregistrer plus de 10 utilisateurs et plus de 5 serrures.

Les trois packs seront disponibles en France à partir du mois de janvier 2015.

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

Source : http://www.clubic.com/mag/maison-connectee/actualite-744009-okidokeys-serrure-connectee-francaise-disponible.html?estat_svc=s%3D223023201608%26crmID%3D639453874_775958436

Disparaître du Net, droit ou rêve ?

Disparaître du Net, droit ou rêve ?

Le 13 mai 2014, la Cour de Justice de l'Union Européenne rendait une décision imposant aux moteurs de recherches, le retrait de tout lien des pages de résultats, en cas de demande légitime d'une personne estimant subir un préjudice. Cette décision dite « droit à l'oubli » rend les moteurs de recherches responsables des contenus qu'ils indexent de façon algorithmique, même si ceux-ci sont publiés ailleurs, par une tierce personne. Comment en sommes-nous arrivés là ? Les règles de l'internet évoluent-elles vraiment vers le respect de la vie privée ?

Soyons clair…

Le droit à l'oubli n'existe pas et aucune mention de ce terme n'est présente dans le droit. La décision rendue par la CJUE (Cours de Justice de l'Union Européenne) s'appuie sur la protection des données à caractère personnel, le droit au respect de la vie privée, ainsi que le droit de la presse. En l'état actuel, seuls les particuliers dans l'UE, en Islande, en Norvège, en Suisse et dans le Liechtenstein sont concernés. Si la décision implique l'ensemble des moteurs de recherche, Google prend l'affaire très au sérieux, en raison de sa position de leader en Europe (93% du marché) mais aussi des récentes résolutions du Parlement Européen le concernant, pour abus de position dominante. Le Parlement Européen a d'ailleurs voté le 26 novembre dernier le démantèlement de Google, décision qui reste cependant symbolique puisqu'il ne détient aucune compétence en la matière.

Sous la contrainte de la CUJE, tous les moteurs de recherches disposent désormais d'une page avec un formulaire permettant à un internaute de demander la suppression de données personnelles. Toutefois, seules les versions européennes des moteurs sont concernées. Une limitation que le G29 (organisme qui rassemble les CNIL européennes) trouve insuffisante. Des données effacées sur Google France reste accessible sur Google Canada, par exemple…

Une nouvelle directive du G29 vient d'ailleurs de voir le jour pour que le déréférencement soit étendu à toutes les versions géographiques des moteurs. Affaire à suivre !

Etat de la demande

Le droit à l'oubli risque de prendre une dimension politique sur fond de lobbying, mais qu'en est-il des intérêts des internautes ? Qu'advient-il des demandes envoyées via les formulaires des moteurs de recherches ?

Si les Européens communiquent facilement des données en ligne, 75% d'entre eux souhaitent pouvoir exercer un droit à l'oubli. Un paradoxe que les moteurs de recherche doivent prendre en compte dans leur processus de retrait des liens préjudiciables. La question du « droit à l'oubli » se heurte également au « droit à l'information », principe de base de la démocratie. Par conséquent, chaque demande de suppression envoyée à un moteur de recherche, doit être accompagnée d'une explication cohérente, accompagnée de la copie de votre pièce d'identité avec photo en cours de validité. A vous d'être suffisamment clair pour « expliquer en quoi le lien apparaissant dans les résultats de recherche est non pertinent,obsolète ou inapproprié. »

A ce petit jeu, il va de soi que toutes les demandes ne sont pas validées. Google, Bing et Yahoo… jugent le plus souvent les informations vous concernant, d'intérêt public et des milliers de demandes envoyées se heurtent ainsi à un refus. A noter, que les moteurs de recherche ne sont pas tenus de publier la liste de leurs critères, ni de produire les statistiques de leurs décisions.

Le « droit à l'oubli » est donc loin d'être acquis et il faut rester attentif pour garder la maîtrise de son profil web et ne pas en devenir esclave. Si les moteurs de recherche contribuent à cet état de fait, il est certainement plus judicieux de s'interroger sur notre véritable rapport au narcissisme et au voyeurisme sur la toile.

Ego-surfing ou droit à l'oubli ?

Si nos données personnelles sont si peu « personnelles », il faut bien reconnaître que nous contribuons fortement à dévoiler notre vie privée. Un simple regard sur un profil Facebook permet de découvrir, âge, sexe, profession, goûts, désirs… Difficile de prétendre que l'on souhaite protéger sa vie privée, quand notre égo nous pousse à dévoiler sa vie aux autres… Que dire quand l'instinct pousse certains d'entre nous à espionner le profil d'une personne pour en connaître plus sur sa vie, le plus souvent via un faux profil.

Selon une étude Ipsos menée pour Bing, 71% des internautes français ont déjà tapé leur nom sur les moteurs de recherche. Certes, la curiosité est un facteur important mais la fierté de voir son nom sur le web est également bien présente. Quant à l'inquiétude liée à son e-reputation, elle ne semble pas se manifester pour la maîtrise de ses informations, mais bien dans le fait d'être confondu avec un autre.

Dans ce contexte, il devient de plus en plus nécessaire de protéger sa vie privée même quand on n'a rien à cacher.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire…

S o u r c e : http://cursus.edu/dossiers-articles/articles/24648/disparaitre-net/?utm_source=Thot+Cursus+-+Bulletins+hebdomadaires&utm_campaign=2cf8b24b72-UA-5755289-1&utm_medium=email&utm_term=0_3ba118524c-2cf8b24b72-13406077#.VIg_XLK9KSN

Par Vincent Dadin

Twitter : les données des applications mobiles servent à mieux cibler les publicités

Twitter : les données des applications mobiles servent à mieux cibler les publicités

Technologie : Les annonceurs travaillant sur Twitter peuvent désormais exploiter les données d'utilisation des applications mobiles pour affiner leurs campagnes. Mais les usagers ont la possibilité de désactiver le suivi de leurs habitudes.

Il y a quelques semaines, Twitter annonçait qu'il allait commencer à collecter des informations sur l'usage des applications mobiles afin de rendre les contenus plus pertinents. Cela se traduit aujourd'hui par un nouvel outil mis à la disposition des publicitaires qui prend le nom de "tailored audiences" ou "public adapté". Ces derniers vont désormais pouvoir cibler leurs réclames en se basant sur les données issues des applications mobiles : fréquence d'utilisation, nombre d'installations, achats in-app, inscriptions.
Par exemple, un annonceur pourra cibler une personne ayant installé son application mais qui ne s'est pas encore enregistré ou n'a pas fait d'achat. Mais Twitter a pris soin d'offrir à ses membres la possibilité de refuser ce ciblage en désactivant la fonction depuis les paramètres de leur application Android ou iOS. (Eureka Presse)

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

Source : http://www.zdnet.fr/actualites/twitter-les-donnees-des-applications-mobiles-servent-a-mieux-cibler-les-publicites-39811067.htm

---

Les ministres de l'UE reviennent sur le guichet unique pour la protection des données

Les ministres de l'UE reviennent sur le guichet unique pour la protection des données

Deux ans après la proposition de s'adresser à une unique autorité pour gérer les questions de protection de données dans l'Union européenne, les ministres de la Justice de l'UE envisagent une autre solution, impliquant plusieurs autorités. Un abandon qui contrarie la coalition ICDP où l'on retrouve Google, Facebook, Microsoft, Apple et Yahoo.

Les pays membres de l'Union européenne sont revenus la semaine dernière sur une proposition de 2012 visant à diriger les fournisseurs de technologies tels que Google, Facebook, Microsoft ou Apple vers une seule autorité habilitée à gérer les questions de protection de données en Europe. L'objectif de ce projet était d'éviter de devoir s'adresser à chaque autorité de protection de données des 28 pays membres de l'UE. La question avait été débattue par les ministres de la Justice et la proposition élaborée par la Commission européenne constituait l'un des piliers de la réforme de la protection de données dans l'UE.
Mais la semaine dernière, lors d'une nouvelle réunion des ministres de la Justice et de l'Intérieur à Bruxelles, à laquelle ont assisté Christiane Taubira, ministre de la Justice, et Bernard Cazeneuve, ministre de l'Intérieur en France, une majorité s'est dégagée pour une autre proposition, suggérée par les Italiens. Ces derniers occupent jusqu'au 31 décembre la présidence tournante du Conseil européen où se rencontrent les ministres pour coordonner les différentes politiques.

Un processus qui risque d'être très lourd, estime l'ICDP
Cette fois, la proposition suggère un mécanisme qui se déclencherait uniquement dans les cas transfrontaliers les plus importants. Celui-ci consisterait à faire coopérer les différentes autorités de protection de données concernées afin de déboucher sur une décision conjointe. Cette proposition n'emporte évidemment pas les faveurs des fournisseurs de technologie. L'ICDP, Industry Coalition for Data Protection (qui regroupe 18 associations représentant des milliers de sociétés européennes et internationales, dont Google, Facebook, Microsoft, Apple et Yahoo), a exprimé sa déception. Dans une lettre envoyée aux ministres avant leur réunion, elle estime que cela semble créer un mécanisme plus compliqué. Pour elle, cela pourrait conduire à impliquer toutes les autorités de protection de données dans la grande majorité des cas examinés. Couplé à la possibilité que chaque autorité puisse opposer son veto à une décision, cela rendrait le processus très lourd.
Même son de cloche du côté de la CCIA (Computer and Communications Industrie Association) qui représente des sociétés Internet européennes et américaines. L'un des ses porte-parole estime qu'il faut un guichet unique qui permettrait aux grandes entreprises technologiques comme aux PME de ne s'adresser qu'à un seul régulateur, quel que soit le nombre de pays dans lesquels ils interviennent. Ces dispositions seront à nouveau abordées par le Conseil européen dans les prochains mois.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-les-ministres-de-l-ue-reviennent-sur-le-guichet-unique-pour-la-protection-des-donnees-59534.html par Loek Essers / IDG News Service (adapté par Maryse Gros)

La protection des données personnelles, un « droit fondamental »

La protection des données personnelles, un « droit fondamental »

Les régulateurs européens, réunis au sein du G29, rappellent la nécessité de ne pas traiter les données personnelles comme un seul « objet de commerce ».

Les autorités européennes de régulation des données ont affirmé lundi dans une déclaration commune au ton très politique que la protection des données personnelles était un « droit fondamental » sur lequel l'Union européenne ne pouvait transiger. Un an et demi après les révélations d'Edward Snowden, les régulateurs européens réunis au sein du G29 ont rappelé lors d'un colloque la nécessité de ne pas traiter les données personnelles comme un seul « objet de commerce ».
Faisant référence au traité de libre-échange transatlantique, les « Cnil » (Commission nationale de l'informatique et des libertés, NDLR) soulignent que « le niveau européen de protection des données ne peut être érodé (…) par des accords bilatéraux ou internationaux ». Elles demandent ainsi l'application stricte des nouvelles règles de protection des données de l'Union, en cours de négociation, qui doivent être considérées « comme des principes internationaux impératifs en droit international public et privé ».
« Tous les corpus de protection des données doivent être considérés comme des lois de police », a affirmé Isabelle Falque-Pierrotin, présidente de la Cnil française, qui appelle également à la mise en place d'actions judiciaires collectives sur le modèle des class actions. Le G29 juge par ailleurs « inacceptable sur le plan éthique (…) la surveillance secrète, massive et indiscriminée de personnes en Europe ».

« Le pétrole de demain »
« La conservation, l'accès et l'utilisation de données par les autorités nationales compétentes doivent être limités à ce qui est strictement nécessaire et proportionné dans une société démocratique », soulignent les « Cnil ». Le Premier ministre Manuel Valls a promis à ce sujet qu'un projet de loi « garantira un contrôle effectif et indépendant de l'intégralité des actes dérogatoires au droit commun accomplis par les services de renseignement ». Il a appelé également à une simplification des conditions générales d'utilisation et à un droit à l'oubli renforcé pour les mineurs.
Le stockage des données personnelles collectées par des entreprises privées doit enfin, selon les régulateurs, pouvoir être contrôlé par une autorité européenne indépendante. « Les données européennes doivent être stockées en Europe », a indiqué Thierry Breton, P-DG d'Atos et ancien ministre de l'Économie. « Il est temps de protéger ces mines d'or (…), ce sera le pétrole de demain », a-t-il ajouté.

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

Source : http://www.lepoint.fr/societe/la-protection-des-donnees-personnelles-un-droit-fondamental-08-12-2014-1887990_23.php