Panorama 2015 des menaces informatiques

	**Panorama 2015 des menaces informatiques**

McAfee, filiale d'Intel Security, publie son nouveau rapport annuel, intitulé '2015 Threats Prediction', qui met l'accent sur les principales menaces prévues pour l'année 2015. McAfee présente conjointement son rapport 'November 2014 Threat Report' relatif à l'analyse des menaces informatiques du dernier trimestre 2014.

Les prévisions 2015 de McAfee en matière de menaces :
1. Une fréquence accrue du cyber-espionnage. La fréquence des attaques de cyber-espionnage continuera d'augmenter. Les pirates actifs de longue date mettront en place des techniques de collecte des informations toujours plus furtives, tandis que les nouveaux venus chercheront des solutions pour subtiliser de l'argent et perturber les activités de leurs adversaires.
Les cyber-espions actifs de longue date travailleront à parfaire des méthodes toujours plus efficaces pour demeurer cachés sur les systèmes et les réseaux de leurs victimes. Les cybercriminels continueront à agir davantage comme des cyber-espions, en mettant l'accent sur les systèmes de surveillance et la collecte de renseignements sensibles relatifs aux individus, à la propriété intellectuelle et à l'intelligence opérationnelle. McAfee Labs prévoit que la cyberguerre sera davantage utilisée par les plus petits États et les groupes terroristes.

2. Attaques fréquentes, profitables et sévères envers l'Internet des objets. A moins d'intégrer le contrôle de la sécurité dès la conception des produits, le fort déploiement de l'IdO devrait dépasser les priorités de sécurité et de confidentialité. La valeur croissante des données pouvant être recueillies, traitées et partagées par ces dispositifs devrait attirer leurs premières attaques en 2015.
La prolifération croissante des appareils connectés dans des environnements tels que la santé pourrait également fournir aux logiciels malveillants un accès à des données personnelles plus sensibles que les données relatives aux cartes de crédit. En effet, selon le rapport de McAfee Labs intitulé « Cybercrime Exposed : Cybercrime-as-a-Service », chacune de ces données représenterait un gain d'environ 10 $ pour un cybercriminel, soit 10 à 20 fois la valeur d'un numéro de carte de crédit américaine volé.

3. Les débats autour de la vie privée s'intensifient. La confidentialité des données sera toujours menacée, dans la mesure où les pouvoirs publics et les entreprises peinent à déterminer ce qui constitue un accès équitable et autorisé à des « informations personnelles » mal définies.

En 2015, les discussions vont se poursuivre pour définir ce que sont les « informations personnelles » et dans quelle mesure elles peuvent être accessibles et partagées par des acteurs étatiques ou privés. Nous allons voir une évolution de la portée et du contenu des règles de la protection des données ainsi que des lois de réglementation de l'utilisation de l'ensemble de données préalablement anonymes. L'Union Européenne, les pays d'Amérique latine, ainsi que l'Australie, le Japon, la Corée du Sud, le Canada et bien d'autres pays adopteront des lois et des règlements de protection des données plus strictes.

4. Les ransomwares évoluent dans le Cloud. Les logiciels de demande de rançon (ransomware) connaîtront une évolution dans leurs méthodes de propagation, de chiffrement et de cibles visées. McAfee Labs prévoit également que de plus en plus de terminaux mobiles essuieront des attaques.

Une nouvelle variante de ransomware capable de contourner les logiciels de sécurité devrait aussi faire son apparition. Elle ciblera spécifiquement les terminaux dotés de solutions de stockage dans le Cloud. Une fois l'ordinateur infecté, le ransomware tentera d'exploiter les informations de connexion de l'utilisateur pour ensuite infecter ses données sauvegardées dans le Cloud. La technique de ciblage du ransomware touchera également les terminaux qui s'abonnent à des solutions de stockage dans le Cloud. Après avoir infecté ces terminaux, les logiciels de ransomware tenteront d'exploiter les informations de connexion au Cloud. McAfee Labs s'attend à une hausse continue des ransomwares mobile, utilisant la monnaie virtuelle comme moyen de paiement de la rançon.

5. De nouvelles surfaces d'attaque mobiles. Les attaques mobiles continueront d'augmenter rapidement dans la mesure où les nouvelles technologies mobiles élargissent la surface d'attaque.
L'émergence de kits de génération de logiciels malveillants sur PC et la distribution de code source malveillant pour mobile permettront aux cybercriminels de désormais cibler ces appareils. Les app stores frauduleux continueront d'être une source importante de malwares sur mobile. Le trafic engendré par ces boutiques d'applications sera notamment conduit par le 'malvertising', qui s'est rapidement développé sur les plateformes mobiles.

6. Les attaques dirigées contre les points de vente augmentent et évoluent avec les paiements en ligne. Les attaques dirigées contre les points de vente demeureront lucratives et l'adoption croissante par le grand public des systèmes de paiement numérique sur appareils mobiles offrira aux cybercriminels de nouvelles surfaces d'attaque à exploiter.

Malgré les efforts des commerçants de déployer des cartes à puce et à code PIN, McAfee Labs prévoit pour 2015 une hausse significative des failles de sécurité liés aux points de vente. Cette prédiction est notamment basée sur le nombre de dispositifs de points de vente devant être upgradés en Amérique du Nord. La technologie de paiement sans contact (NFC) devrait devenir un nouveau terrain propice à de nouveaux types d'attaques, à moins que les utilisateurs ne soient formés au contrôle des fonctions NFC sur leurs appareils mobiles.

7. Logiciels malveillants au-delà de Windows. Les attaques de logiciels malveillants ciblant des systèmes d'exploitation autres que Windows exploseront en 2015, stimulées par la vulnérabilité Shellshock.

McAfee Labs prévoit que les conséquences de la vulnérabilité Shellshock seront ressenties au cours des années à venir par les environnements Unix, Linux et OS X, notamment exécutés par des routeurs, des téléviseurs, des systèmes de contrôle industriels, des systèmes de vol et des infrastructures critiques. En 2015, McAfee Labs s'attend à une hausse significative des logiciels malveillants non-Windows dans la mesure où les hackers chercheront à exploiter cette vulnérabilité.

8. Exploitation croissante des failles logicielles. Le nombre de failles décelées dans des logiciels populaires continuant d'augmenter, les vulnérabilités enregistreront une forte hausse.

McAfee Labs prévoit que l'utilisation de nouvelles techniques d'exploitation telles que la falsification de pile (stack pivoting), la programmation orientée retour (ROP, Return Oriented Programming) et la programmation orientée saut (JOP, Jump-Oriented Programming), combinées à une meilleure connaissance des logiciels 64 bits, favorisera l'augmentation du nombre de vulnérabilités détectées, suivi en cela par le nombre de logiciels malveillants exploitant ces nouvelles fonctionnalités.

9. De nouvelles tactiques d'évasion pour le sandboxing. Le contournement du sandbox deviendra un problème de sécurité informatique majeur.

Des vulnérabilités ont été identifiées dans les technologies d'analyse en environnement restreint (sandboxing) mises en œuvre avec les applications critiques et populaires. McAfee Labs prévoit une croissance du nombre de techniques visant à l'exploitation de ces vulnérabilités ainsi que le contournement des applications de sandboxing. Aujourd'hui, un nombre significatif de familles de logiciels malveillants parviennent à identifier les systèmes de détection de type sandbox et à les contourner. A ce jour, aucun logiciel malveillant en circulation n'est parvenu à exploiter des vulnérabilités de l'hyperviseur pour échapper à un système de sandbox indépendant. Il pourrait en être autrement en 2015.

Pour lire le rapport 'McAfee Labs – Threat Report' dans son intégralité, cliquez ici : http://mcaf.ee/ojbsz

Retour sur 2014
Durant le troisième trimestre 2014, McAfee Labs a détecté plus de 307 nouvelles menaces par minute, soit plus de 5 chaque seconde, avec une croissance des logiciels malveillants sur mobile en hausse de 16 % sur le trimestre, soit une croissance annuelle de 76 %. Les chercheurs de McAfee Labs ont également identifié de nouvelles tentatives visant à tirer profit des protocoles de sécurité Internet, notamment les vulnérabilités de protocoles SSL tels que Heartbleed et BERserk, ainsi que l'abus répété des signatures numériques pour masquer les malwares comme étant légitimes.

Pour 2015, McAfee Labs alerte sur les techniques de cyber-espionnage des pirates informatiques et prévoit que les hackers actifs de longue date mettront en place des techniques de collecte de données confidentielles toujours plus furtives au travers d'attaques ciblées étendues. Les chercheurs du Labs prévoient ainsi de mettre davantage d'efforts sur les vulnérabilités liées à l'identification d'applications, de systèmes d'exploitation et au réseau, ainsi que sur les limites technologiques du sandboxing, dans la mesure où les hackers tentent de se soustraire à l'application de détection par hyperviseur.

« L'année 2014 restera dans les mémoires comme l'année où la confiance en matière de sécurité informatique a été ébranlée », déclare David Grout, directeur Europe du Sud de McAfee, filiale d'Intel Security. « Les nombreux vols et pertes de données ont altéré la confiance de l'industrie envers le modèle d'Internet ainsi que celle des consommateurs dans la capacité des entreprises à protéger leurs données. La confiance des entreprises, ainsi que celle des organisations, ont également étaient impactées et les a poussé à s'interroger sur leur capacité à détecter et à détourner les attaques dont elles ont été la cible », poursuit David Grout. « En 2015, l'industrie d'Internet devra se renforcer pour restaurer cette confiance, mettre en place de nouvelles normes pour s'adapter au nouveau paysage des menaces et adopter de nouvelles stratégies de sécurité qui requièrent de moins en moins de temps dans la détection des menaces. Ainsi, nous devons tendre à un modèle de sécurité intégrée dès la conception de chaque appareil. »

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

Source : http://www.globalsecuritymag.fr/McAfee-Labs-dresse-le-panorama,20141210,49364.html

---

Un « coffre-fort » en ligne pour le stockage des données

Un « coffre-fort » en ligne pour le stockage des données

L’Institut Hasso Plattner (HPI) de Potsdam (Brandebourg) et l’Imprimerie fédérale (Bundesdruckerei) ont convenu d’un partenariat de recherche. Dans le cadre d’un premier projet pilote, un « coffre-fort en ligne » sera développé et mis à la disposition du grand public, de l’administration et des entreprises. Ce système doit permettre à l’utilisateur de stocker et gérer ses données en toute sécurité.

Le HPI, centre de recherche sur les TIC créé et financé par le co-fondateur de l’entreprise SAP, apporte sa technologie « Cloud-RAID » [1]. Les techniques RAID, généralement appliquées aux disques durs, consistent à répartir les données sur plusieurs supports physiques distincts pour améliorer les performances, la sécurité ou la tolérance aux pannes du système. Cette architecture a été adaptée au cloud.

L’Imprimerie fédérale contribue au projet, quant à elle, avec sa plateforme « Trusted Service ». Celle-ci garantit l’identification fiable des utilisateurs du « coffre-fort en ligne » par un document d’identité. La solution, où les données ne doivent être visibles que par l’utilisateur concerné, doit être flexible et facile à utiliser. Plusieurs fournisseurs de cloud sont intégrés au projet, ce qui implique qu’aucun prestataire ne sera, seul, en possession de l’ensemble des données.

Le projet pilote court jusqu’en mars 2015. Afin d’intensifier les recherches en matière de la gestion de l’identité numérique, les deux partenaires prévoient la mise en place d’un laboratoire sur la sécurité au HPI.

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

Source : http://www.bulletins-electroniques.com/actualites/77364.htm

---

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

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

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

---

The European Data Governance Forum – CNIL

European Data Governance Forum – CNIL

Le G29 et la CNIL organisaient le 8 décembre une conférence internationale qui se tenait à l'UNESCO. La conférence avait pour thème : Protection des données, innovation et surveillance : quel cadre éthique pour l'Europe ?

2015 est une année charnière pour la protection de la vie privée, avec l'adoption du règlement de l'Union Européenne sur la protection des données, la poursuite des négociations commerciales internationales et les décisions finales à prendre sur la gouvernance de l'internet. Cette période est cruciale pour l'Europe qui, dans le nouvel environnement numérique, doit promouvoir haut et fort les valeurs sociétales qui sont les siennes et définir des actions prioritaires pour le futur.
Une réponse d'ensemble à ces défis internationaux ne saurait être élaborée par des acteurs agissant en ordre dispersé. La complexité des problèmes posés demande une réflexion collective de la part de l'ensemble des parties prenantes.
La conférence du 8 décembre organisée par le G29 (groupe des autorités européennes de protection des données) et la CNIL était placée sous le patronage de l'UNESCO et de la Délégation permanente française auprès de l'UNESCO. Elle réunssait des représentants et experts d'horizons divers – institutions nationales, européennes et internationales, industrie, ONG et société civile – qui ont présenté leur point de vue sur les défis actuels de la surveillance numérique et sur la manière d'y répondre de manière adéquate dans une société démocratique.
La conférence s'est achevée par la présentation d'une Déclaration adoptée par le G29 qui était endossable par les parties prenantes qui le souhaitaient. Cette Déclaration soulignait la responsabilité collective de toutes les parties prenantes dans la définition et le respect d'un cadre éthique pour la collecte et l'utilisation de données personnelles dans l'économie numérique. Elle a défini les principes essentiels à inclure dans un tel cadre ainsi que les actions clés à entreprendre par toutes les parties prenantes, des secteurs public et privé, pour garantir le respect des règles.

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

Source : http://www.newspress.fr/Communique_FR_284395_1332.aspx