Que fait Auchan avec notre ticket de caisse ?

Que fait Auchan avec notre ticket de caisse ?

Anticipation de pénurie, état des stocks, performance des zones commerciales… rien n'échappe aux caisses connectées du groupe nordiste.
Nos tickets de caisse sont des mines d'informations! Si on imagine d'emblée qu'une connaissance précise de notre consommation individuelle, destinée à proposer des offres ciblées, constitue un graal pour les Carrefour, Leclerc et consorts, ce n'est pas forcément l'intérêt premier qu'y voient les professionnels de la grande distribution.
Ainsi, pour le groupe Auchan, c'est d'abord à un juste réapprovisionnement des rayons que servent les informations enregistrées par les 7.000 caisses connectées de ses hypermarchés. Remontées en temps réel vers la base de données installée par l'Américain Teradata en région lyonnaise, les données de nos facturettes nourrissent ensuite une appli développée en interne par les services informatiques du groupe détenu par la famille Mulliez. Dès lors, les salariés peuvent connaître en temps réel l'état de leur rayon par produit, au sein de chaque magasin. Ainsi, le responsable du rayon boissons non-alcoolisées peut, grâce à une icône, savoir si son rayon manque partiellement d'une référence ou, selon le jargon maison, s'il est « fantôme », c'est-à-dire vide.
« Pour certains rayons, tels que les sandwiches entre 12h et 14h, c'est anticipable. L'intérêt est donc pour nous de détecter d'autres comportements du consommateur qu'on ne peut prévoir… Un rayon peut être dévalisé en un rien de temps par une personne ou un groupe de personnes, de façon imprévisible ou bien en fonction d'une promotion. En ce sens, l'application peut fournir une information utile au chef de gondole », estime Eric Dewilde, directeur architecture et données au sein du groupe Auchan. Parce que rien ne vaut l'œil humain, les salariés utilisateurs de l'appli sont amenés à faire un retour d'expérience pour dire si le réassort est en cours ou s'il s'agit d'une fausse alerte. *« Nous sommes en phase de rodage. En outre, on n'envoie pas de « push » pour signifier que le rayon se vide. Le principe est de délivrer une information, pas un ordre »,* précise-t-on au sein d'Auchan…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité Contactez-nous

Réagissez à cet article

Source : *Ce qu’Auchan fait vraiment de nos tickets de caisse – Challenges.fr*

Est-ce que Linky aspire nos données personnelles ?

	**Est-ce que Linky aspire nos données personnelles ?**

Linky, un compteur qui ne vous veut pas que du bien ! Ce boitier qui doit être installé dans tous les foyers relèvera en direct et à distance vos habitudes de consommation d'électricité.

Par ailleurs, des incidents ont lieu lors de la pose de ces compteurs, notamment lorsque des personnes s'y opposent : à Plouha et dans sa région récemment, plusieurs incidents ont été constatés, avec notamment une dame de 73 ans bousculée par un installateur alors qu'elle s'opposait à l'installation.
Avec le prétexte d'établir une facture plus précise, EDF prévoit de remplacer 90% des anciens compteurs en 4 ans. Un changement qui suscite de vives polémiques. En effet, de nombreuses communes s'opposent à l'installation de ce compteur dit intelligent. Si l'efficacité et le risque de surcoût sont remis en question, la menace d'intrusion dans la vie privée est également pointée du doigt.
En effet, par son système de collecte de données à distance, le compteur Linky est un véritable concentré d'informations personnelles. Il est techniquement capable de recueillir les index journaliers et la courbe de charge, c'est-à-dire un relevé précis de la consommation électrique de l'utilisateur. Ces données permettent de déduire des informations sur les habitudes de vie des consommateurs.
Des millions de Français seront concernés et des millions de données personnelles seront stockées par ERDF, qui souhaite entrer dans la danse du commerce d'informations, le Big Data. Pas étonnant, car cette mine d'or peut rapporter très gros. En effet, elle fait l'objet d'un véritable business, estimé à plusieurs milliers de milliards d'euros…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Linky, vendeur de données personnelles –*

Comment bien nettoyer sa réputation sur Internet ?

	Comment bien nettoyer sa réputation sur Internet ?

Quand on se lance dans une recherche d'emploi, on regrette parfois des écrits maladroits ou des photos peu flatteuses du passé. Voici comment nettoyer sa réputation sur Internet.
[Lire la suite]

Notre métier : Vous aider à retirer de l'information sur Internet. Que ça soit à l'amiable ou dans le cadre d'une action judiciaire, nous pouvons vous accompagner pour retirer ou rendre moins visibles des informations sur Internet.
contactez-nous

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ;
(Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert
INFORMATIQUE
Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Nettoyer sa réputation sur Internet, c'est possible ? | JDM*

Le Wifi de votre téléphone permettra aussi de vous pister

Le Wifi de votre téléphone permettra aussi de vous pister

Différents projets visent à pister les personnes passant à proximité de capteurs wifi. Ce qui pose notamment la question de l'anonymisation des données.
Marylin Gobert / La Gazette

Beaucoup de villes cherchent aujourd'hui à devenir intelligentes. Elles sont ainsi truffées de capteurs, de compteurs Linky, d'objets connectés, qui permettent de relever et de communiquer les données. Les smart cities sont devenues de véritables pompes à informations. Mais il ne faudrait pas oublier que la data est au service des citoyens. Elle vise à répondre à leurs besoins en améliorant, par exemple, la qualité du service public. Elle ne doit donc être ni intrusive, ni devenir un moyen de contrôle de la vie privée.
D'où l'importance de la protection des données à caractère personnel, définie par l'article 2 de la loi n° 78-17 du 6 janvier 1978 dite « informatique et libertés » comme « toute information relative à une personne physique identifiée ou qui peut être identifiée directement ou indirectement ».

Des capteurs d'habitudes

La récente loi du 7 octobre 2016 pour une République numérique a encore renforcé ces principes, en affirmant la nécessaire maîtrise de l'individu sur ses données. La Commission nationale de l'informatique et des libertés (Cnil) veille notamment à leur anonymisation.
L'une des tentations actuelles est de mesurer les flux des passants, de cartographier leurs déplacements au moyen de capteurs des signaux wifi de smartphones.
L'exemple du géant de l'affichage publicitaire, JCDecaux, qui voulait placer des boîtiers dans son mobilier publicitaire, sur l'esplanade de La Défense à Paris, afin de capter les téléphones dans un rayon de 25 mètres, illustre cette tendance. Cela lui aurait permis d'estimer la fréquentation de ce quartier parisien.
Situation semblable à Rennes pour lutter contre la désertification du centre-ville. Une association de commerçants a voulu mettre en place des capteurs de signaux wifi. Le but ? Assurer un maillage de cette zone pour connaître les habitudes des consommateurs et en tirer des moyens de dynamiser le quartier…[lire la suite]

Réagissez à cet article

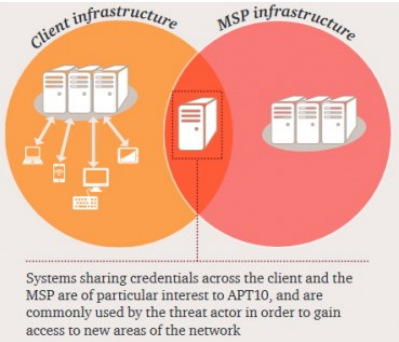
Source : *L’indispensable anonymisation des données personnelles des passants*

Les services Cloud au centre d’attaques d’entreprises par APT10

Les services Cloud au centre d’attaques d’entreprises par APT10

Le groupe de pirates chinois APT10 a infiltré des services Cloud managés pour remonter aux serveurs des entreprises qui les utilisent.

La maturité des attaques ciblées contre les entreprises est montée d'un cran. *« Un groupe de piratage a mené l'une des campagnes d'espionnage les plus prolifiques depuis l'APT1 en 2013, employant de nouvelles tactiques pour atteindre une large audience »*, a alerté PwC (Pricewaterhouse Coopers) lundi 3 avril. En collaboration avec BAE Systems et le National Cyber Security Centre (NCSC) britannique, la branche réseau du cabinet d'audit a découvert ce qu'il considère comme *« l'une des plus importantes campagnes mondiales de cyber-espionnage jamais organisées »*. Pas moins.



De quoi s'agit-il ? Du piratage des infrastructures de fournisseurs de services managés à partir desquelles les cyber-attaquants remontent aux serveurs des organisations qui y ont recours. Une opération que PwC a baptisé 'Cloud Hopper'. Les cyber-criminels derrière ces agissements seraient le groupe de hackers chinois APT10. *« PwC et BAE Systems croient que le groupe de piratage largement connu sous le nom 'APT10' a mené la campagne d'espionnage en ciblant les fournisseurs de services informatiques externalisés comme une façon d'accéder aux organisations de leurs clients à travers le monde, leur conférant un accès sans précédent à la propriété intellectuelle et aux données sensibles »*, indique PwC dans son communiqué. APT10 est le nom donné par FireEye à un groupe de pirates chinois également référencé sous les appellations Red Apollo (par PwC UK), CVNX (par BAE), Stone Panda (par CrowdStrike), et menuPass Team (plus globalement).

Un grand volume de données exfiltrées

Les méthodes d'infection restent relativement classiques et s'appuient sur le spear-phishing, ou harponnage. Cette méthode de phishing ciblé fait appel à des techniques d'ingénierie sociale qui visent à tromper le destinataire d'un e-mail pour l'inciter à installer, à son insu, un malware ou visiter une page infectieuse, à partir desquels les pirates ouvrent une porte d'entrée sur le réseau. Objectif ici : prendre le contrôle des accès d'employés de prestataires Cloud, afin d'exploiter les canaux de communication existant entre les services managés de ces derniers et les serveurs des entreprises clientes. De la grande distribution aux technologies en passant par l'énergie, l'industrie manufacturière, le secteur public ou l'industrie pharmaceutique, tous les grands secteurs sont touchés par cette campagne…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.

Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)

Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle…) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *Les services Cloud au centre d'attaques d'entreprises par APT10*

Big data. Comment les entreprises recueillent et utilisent nos données ?

Big data. Comment les entreprises recueillent et utilisent nos données ?

En 2015, 11 % des entreprises françaises ont traité des big data, selon l'Insee. Les sources de données les plus utilisées sont la géolocalisation, les médias sociaux et les objets connectés ou capteurs. Les grosses entreprises sont les plus à l'aise pour traiter ces données nombreuses et complexes.
Par Julie DURAND

1 % des entreprises françaises ont traité des big data en 2015. Selon l'Insee, qui a réalisé cette enquête, la big data est constituée de **» données complexes, dont le volume important et l'actualisation constante rendent difficile l'exploitation par les outils classiques «** .

7 % des entreprises traitent des données de géolocalisation

Sans surprise, les grosses entreprises sont plus nombreuses à en utiliser que les petites (24 % contre 9 %). Les barrières à l'utilisation de la data sont plus difficiles à franchir pour elles : mauvaise compréhension du sujet et de son intérêt, manque de compétences, coût trop élevé et législation contraignante.

La donnée la plus recueillie et la plus utilisée est la géolocalisation (pour 62 % des entreprises qui utilisent des data, soit 7 % de l'ensemble des entreprises françaises). Cette donnée intéresse surtout les entreprises de transports (92 %) et la construction (89 %).
Deuxième source : les médias sociaux (pour 32 % des entreprises qui utilisent des data, soit 4 % de l'ensemble). Ces données intéressent surtout l'hébergement-restauration (76 %) et l'information-communication (64 %).
Enfin, les objets connectés et capteurs sont la troisième source de data (29 % des entreprises qui en utilisent, soit 3 % de l'ensemble), utilisés principalement par l'industrie (46 %).

Traitement en interne ou externalisée des données ?

74 % des entreprises qui traitent des données le font en interne et 42 % par des prestataires extérieurs, 16 % utilisent donc ces deux méthodes. Le choix entre traitement interne ou externe dépend du secteur et de la taille de l'entreprise. 90 % des entreprises de l'infomation-communication et 84 % des activités scientifiques et techniques le font en interne, **» car les employés sont probablement mieux formés pour cela que dans d'autres secteurs »**. Tous secteurs confondus, 83 % des entreprises de plus de 250 personnes traitent les data en interne, contre 73 % pour les moins de 250 salariés.
Selon l'Insee, les entreprises utilisent toutes ces données pour optimiser leurs processus internes, améliorer leurs produits ou services et/ou rendre plus efficace leur marketing ou leur gestion des ventes.

Réagissez à cet article

Source : *Big data. Comment les entreprises recueillent et utilisent nos données ?*

Wikileaks révèle comment la CIA a piraté des MacBook et iPhone neufs

Wikileaks révèle comment la CIA a piraté des MacBook et iPhone neufs

---

L'organisation fondée par Julian Assange publie un second corpus de documents présentés comme émanant de la CIA qui décrivent les méthodes de l'agence pour pirater des ordinateurs Apple et des iPhone.

Wikileaks remet le couvert. Près de deux semaines après avoir mis en ligne « Vault 7, Year Zero », un ensemble de plusieurs milliers de documents internes détaillant des dizaines de programmes d'espionnage électronique et informatique de la CIA, l'organisation fondée par Julian Assange a publié une deuxième vague d'archives décrivant les techniques utilisées par l'agence du renseignement extérieur américain pour pirater des produits Apple. Baptisé « Dark Matter », ce second volet explique comment la CIA peut pirater un ordinateur Apple, même si son propriétaire y installe un nouveau système d'exploitation, ou un iPhone neuf en pénétrant le réseau d'approvisionnement et de distribution de la marque à la pomme.
• Wikileaks : 5 questions pour comprendre les dernières révélations

Un logiciel indétectable et impossible à effacer

Selon les documents dévoilés par Wikileaks, la CIA a développé un outil en 2012 nommé « Sonic Screwdriver » permettant de passer outre le processus de démarrage d'un MacBook à partir des accessoires périphériques comme une clé USB ou un adaptateur Ethernet branché dans le port Thunderbolt. L'agence pouvait alors **introduire un micro indétectable dans le logiciel profond** (firmware) de l'ordinateur et **bénéficier d'un accès permanent à son contenu** car même une réinstallation du système d'exploitation ou un reformatage de l'appareil ne pouvait suffire à l'effacer. La CIA devait avoir accès physiquement aux appareils visés pour les infecter.
Un autre document montre que la CIA avait conçu cet outil dès 2008 pour l'installer physiquement sur des iPhone neufs. Selon Wikileaks, il est par conséquent « probable que beaucoup d'attaques physiques par la CIA aient infecté la chaîne d'approvisionnement » d'Apple « en bloquant des commandes ou des livraisons ». L'agence américaine « peut faire cadeau à une cible d'un MacBook Air sur lequel a été installé ce micro », indique un document daté de 2009. « L'outil prendra la forme d'un implant/relais opérant dans le (logiciel) profond du MacBook Air et nous permettant d'avoir les moyens de (le) commander et de (le) contrôler », peut-on lire dans ces documents.

Les produits actuels vraisemblablement pas concernés

Apple n'a pas encore réagi à ces révélations. La plupart des documents datant de plus de sept ans et concernent les premières générations d'iPhone. Il apparaît peu probable que les produits actuels du groupe soient vulnérables à ces techniques. La méthode « Sonic Screwdriver » utilisée pour infecter des MacBook rappelle la faille « Thunderstrike » découverte fin 2014, qui permettait de contaminer un Mac lors de l'allumage à l'aide d'un appareil Thunderbolt vérolé, et corrigée par Apple depuis.
Le 9 mars, Wikileaks avait déjà diffusé près de 9.000 fichiers mettant à nu les capacités d'espionnage de la CIA et le recours à des pratiques particulièrement intrusives pour transformer des télévisions et des voitures connectées en mouchards, espionner des iPhone et des smartphones Android ou contourner des antivirus commerciaux. La CIA n'a jamais authentifié les documents mais de nombreux experts les jugent crédibles. Apple avait fait savoir qu'elle avait corrigé les failles évoquées dans ces documents. Wikileaks affirme détenir des informations sur plus de 500 programmes au total et promet de les publier dans les prochaines semaines.
Benjamin Hue, Journaliste RTL

Source : *Wikileaks montre comment la CIA a piraté des MacBook et iPhone neufs*

WhatsApp et Telegram corrigent des vulnérabilités importantes

WhatsApp et Telegram corrigent des vulnérabilités importantes

WhatsApp et Telegram ont corrigé des failles dans leurs applications après que des chercheurs en sécurité ont révélé qu'il était possible de prendre le contrôle des comptes d'utilisateurs.

WhatsApp et Telegram sont deux applications de messagerie instantanée qui ont plus d'un milliard d'utilisateurs cumulés. Elles offrent des communications chiffrées, un envoi de messages rapide et un tas d'autres fonctionnalités. Mais de nouvelles recherches révèlent qu'une image injectée par un logiciel malveillant aurait suffi à voler les comptes Web WhatsApp ou Telegram d'une personne. Il faudrait seulement quelques secondes pour que l'attaquant obtienne un contrôle total sur les comptes, y compris l'accès aux images, aux vidéos, aux fichiers audio et aux contacts. Et le cryptage serait effectivement une aide avec ce genre de hack.
La vulnérabilité était présente sur les versions desktop des applications, ainsi si vous n'utilisez pas WhatsApp ou Telegram sur votre ordinateur, alors vous étiez déjà à l'abri.
Les chercheurs en sécurité ont découvert que le code malveillant pouvait être caché à l'intérieur d'une image. Lorsqu'il est cliqué, le fichier image exécute le code et l'attaquant obtient un accès complet aux données de stockage WhatsApp et/ou Telegram. Le pirate pourrait ensuite envoyer le fichier à tous les contacts de la victime, en diffusant le malware à d'autres cibles.
Découverte par Check Point, la vulnérabilité a été communiquée à WhatsApp et Telegram le 8 mars, et les deux entreprises ont déjà déployé des correctifs pour leurs clients desktop…[lire la suite]

Notre métier : Vous aider à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus…) et vous assister dans vos démarches de mise en conformité avec la réglementation relative à la protection des données à caractère personnel.
Par des actions d'expertises, d'audits, de formations et de sensibilisation dans toute la France et à l'étranger, nous répondons aux préoccupations des décideurs et des utilisateurs en matière de cybersécurité et de mise en conformité avec le règlement Européen relatif à la Protection des Données à caractère personnel (RGPD) en vous assistant dans la mise en place d'un Correspondant Informatique et Libertés (CIL) ou d'un Data Protection Officer (DPO) dans votre établissement.. (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle n°93 84 03041 84)
Plus d'informations sur : https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles

---

Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...) ;
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert INFORMATIQUE Cybersécurité & Conformité

Contactez-nous

Réagissez à cet article

Source : *WhatsApp et Telegram corrigent des vulnérabilités importantes – Gridam*

Google, ou la révolution transhumaniste via le Big Data

Google, ou la révolution transhumaniste via le Big Data

A l'occasion de la sortie du livre de Christine Kerdellant Dans la Google du loup, Éric Delbecque décrypte le projet de « fusion » entre le vivant et le digital porté par le géant de l'informatique américain.

Christine Kerdellant a relevé un beau défi *Dans la Google du loup* (Plon)! Elle met le doigt là où Google pose véritablement problème, à savoir sur la révolution anthropologique du transhumanisme… Pour ce qui concerne sa participation à la société de surveillance globale que fabriquent un certain nombre d'acteurs publics et privés, l'affaire est entendue depuis des années… Sous l'administration Obama, les dirigeants de Google se rendirent à la Maison-Blanche 230 fois! Ils confirmèrent en 2013 que les agences gouvernementales de l'Oncle Sam les sollicitaient annuellement – dans le cadre du Patriot Act – pour surveiller 1000 à 2000 comptes. En janvier 2015, la firme vedette du Web a reconnu avoir fourni au Ministère de la Justice américain l'intégralité des comptes Google de trois membres de WikiLeaks.

Nous assistons à l'émergence d'une société de surveillance de masse dont l'État n'est pas le centre mais l'un des maillons.

Il paraît dès lors compliqué de penser qu'une idéologie sécuritaire explique à elle seule l'extension de l'ombre de Big Brother sur le monde. Les géants du numérique du secteur privé (les GAFA: Google, Amazon, Facebook, Apple) participent largement à la manœuvre, plus ou moins volontairement (pas pour des raisons politiques, mais économiques). Nous assistons à l'émergence d'une société de surveillance de masse dont l'État n'est pas le centre mais l'un des maillons. Sa stratégie en matière de renseignement doit se lire comme un fragment d'un système cybernétique (au sens de science du contrôle) beaucoup plus vaste, où le capitalisme financier californien et numérique occupe une place décisive. Séparer ce dernier du complexe militaro-sécuritaro-industriel de l'Oncle Sam devient de plus en plus difficile, voire hasardeux.

L'intérêt plus décisif du livre de Christine Kerdellant est ailleurs. Il explore de manière très accessible et percutante le cœur du projet Google, ou plutôt sa signification philosophique profonde. Derrière les joyeux Geeks de la Silicon Valley s'exprime la volonté de réifier l'humanité, de l'enchaîner à une raison calculante. Cette dernière va nous émanciper nous répète-t-on, nous libérer – via le Big Data – des limites de notre condition, nous délivrer de la mort et transformer notre existence en un jardin de fleurs. Mais lorsqu'on choisit d'examiner de plus près les conséquences des propositions de Google, on découvre une perspective d'avenir moins réjouissante…[lire la suite]

Réagissez à cet article

Source : *Google, ou la révolution transhumaniste via le Big*

Data

Les messages de WhatsApp peuvent être facilement lus par la CIA

Les messages de WhatsApp peuvent être facilement lus par la CIA

L'organisation WikiLeaks a reçu une importante base de données révélant les techniques de cyber-surveillance et de piratage de la CIA. Selon ces informations l'agence de renseignement américaine peut facilement accéder aux messageries, y compris WhatsApp et Telegram.

La Central Intelligence Agency (agence centrale de renseignement, CIA) est capable de contourner le cryptage de certaines applications populaires de messagerie, y compris WhatsApp et Telegram, selon les documents publiés par WikiLeaks aujourd'hui.
« Ces techniques permettent à la CIA de contourner le cryptage de WhatsApp, de Signal, de Telegram, de Wiebo, de Confide et de Cloackman en piratant les téléphones « intelligents » sur lesquels ces applications sont installées et de collecter les enregistrements audio et les messages avant que le cryptage ne soit activé », informe le document publié par WikiLeaks.

© FLICKR/ VIN CROSBIE
Espionnage en plein ciel: Air France dans le viseur des services secrets US et UK

Cette fuite a semé le trouble parmi les utilisateurs de WhatsApp, dont beaucoup ont réagi avec virulence aux nouvelles selon lesquelles l'application aurait commencé à partager des données avec Facebook l'année dernière.
La révélation de WikiLeaks suggère que les espions du gouvernement américain ont eu accès aux messages des utilisateurs malgré la mise en place d'un cryptage de bout en bout, qui est pourtant conçu pour protéger la confidentialité des utilisateurs.
Cependant, il se pourrait que la CIA n'ait pas piraté les applications elles-mêmes, mais craqué les outils de cryptage en attaquant les smartphones des utilisateurs.

© AFP 2017 SAUL LOEB
WikiLeaks publie plus de 8.700 documents concernant les capacités de cyber-espionnage de la CIA

Le site de Julian Assange, WikiLeaks, a annoncé le 7 mars la publication d'une nouvelle série de fuites sur la CIA sous le code « Vault 7 » qui sera, d'après le communiqué de l'organisation, la plus importante publication de documents confidentiels sur l'agence.
La première partie des fuites, intitulée « Year Zero », comprend 8 761 documents et fichiers qui ont été collectés sur un réseau isolé de haute sécurité du Centre Cyber Intelligence (département de la CIA) à Langley, dans l'État de Virginie.
Les fuites de « Year Zero » révèlent les capacités de piratage de la CIA contre un large éventail de produits américains et européens, notamment Windows, iPhone, Android et même les téléviseurs Samsung, qui ont été transformés en microphones cachés par le programme Weeping Angel…[lire la suite]

Réagissez à cet article

Source : *Les messages de WhatsApp peuvent être facilement lus par la CIA*