Le datacenter d’Interxion de La Courneuve interdit d’exploitation | Le Net Expert Informatique

	Le datacenter d’Interxion de La Courneuve interdit d’exploitation

Le tribunal administratif de Montreuil vient d'annuler l'arrêté préfectoral qui autorisait l'exploitation du datacenter d'Interxion installé à La Courneuve, selon le site Mediapart. Contactée par la rédaction, la société n'a pas souhaité commenter la décision.

La mésaventure qui arrive au fournisseur de datacenters Interxion pourrait-elle arriver à d'autres opérateurs de sites ?

Le tribunal administratif de Montreuil a annulé un arrêté préfectoral qui l'autorisait à exploiter son datacenter situé à La Courneuve, selon nos confrères de Mediapart. Il vient de rendre sa décision après l'audience qui s'est tenue le 1er octobre dernier, à la suite de la plainte d'un collectif de riverains du datacenter, rassemblé dans l'association Urbaxion'93. Contacté par la rédaction, la société Interxion n'a pas souhaité commenter cette décision. Elle a ouvert son datacenter Par7 en juin 2012 sur une surface de 4 500 m2 d'espace équipé avec une puissance électrique affichée de 64 MW.

Les plaignants ont demandé l'annulation de l'autorisation permettant à Interxion d'exploiter son datacenter situé rue Rateau, en faisant état d'une irrégularité de l'enquête publique et d'insuffisances dans l'étude d'impact, selon le site reporterre.net. Ces riverains se plaignent du bruit généré par l'installation qui refroidit les centaines de serveurs informatiques abrités par l'immense hangar d'Interxion. A cela s'ajoutent les risques liés au stockage de plusieurs centaines de milliers de litres de fuel conservés pour alimenter les groupes électrogènes diesel du site.

Des habitations situées à quelques mètres du datacenter

Avec le développement accéléré de l'usage d'Internet, des communications mobiles, de la vidéo à la demande de type Netflix et des applications cloud dans les entreprises, le déploiement de datacenters pour traiter ces milliards d'interactions informatiques est passé à la vitesse supérieure. Un certain nombre d'entre eux se sont installés depuis plusieurs années en Ile-de-France, notamment en Seine-Saint-Denis (à Pantin, Aubervilliers, La Courneuve…) ou dans les Hauts-de-Seine (à Clichy notamment) et ils continuent à se développer.

Or, si ces implantations, qui consomment énormément d'énergie et génèrent des nuisances sonores pour refroidir les armoires informatiques, sont souvent situées dans des zones industrielles relativement éloignées des quartiers d'habitation, ce n'est pas toujours le cas. A La Courneuve, rue Rateau, le fonctionnement du datacenter d'Interxion est loin d'être passé inaperçu. Les logements des premiers riverains sont situés à quelques mètres du datacenter qui se trouve tout simplement de l'autre côté de la rue. Cette décision du tribunal administratif de Montreuil va-t-elle inspirer d'autres Franciliens ayant à subir dans d'autres villes de semblables désagréments ?

Les datacenters, nouveaux pollueurs

De façon générale et en dehors des nuisances directes de voisinage, les impacts environnementaux des datacenters sont en passe de devenir un problème majeur. Au regard de leurs besoins considérables en dépense énergétique, ces centres de calcul deviennent des pollueurs notoires. Aux Etats-Unis, ils ont consommé en 2013 près de 91 milliards de kilowatts-heure et ils devraient en consommer 139 milliards en 2020, soit une augmentation de 53% selon une étude publiée l'an dernier par la National Resources Defense Council.

En juin dernier, en France, sur le forum Teratec 2015 consacré au calcul haute performance, Thierry Breton, président d'Atos, avait également insisté sur l'importance des problématiques énergétiques des datacenters, bien connues et de longue date. « Ce sont des sujets à ne pas prendre à la légère », avait-il rappelé.

Source :
http://www.lemondeinformatique.fr/actualites/lire-le-datacenter-d-interxion-de-la-courneuve-interdit-d-exploitation-62707.html
Par Maryse Gros

L’ultimatum des CNIL européennes concernant le Safe Harbor | Le Net Expert Informatique

L’ultimatum des CNIL européennes concernant le Safe Harbor

Après la suspension du mécanisme dit Safe Harbor, les régulateurs du G29 montent au créneau. Ils donnent trois mois aux institutions européennes pour négocier avec les États-Unis un accord intergouvernemental sur les données transférées offrant des garanties aux citoyens européens.

Après la décision de la Cour de Justice de l'Union européenne (CJUE) invalidant l'accord dit Safe Harbor, le groupe des CNIL européennes (G29) demande aux autorités européennes et américaines d'agir sous trois mois pour trouver des « solutions techniques et juridiques » qui permettent le transfert de données de l'Union européenne vers les États-Unis, « dans le respect des droits fondamentaux ».
« De telles solutions pourraient intervenir dans le cadre de négociations d'un accord intergouvernemental offrant des garanties fortes aux citoyens européens.
Les négociations actuelles portant sur un nouvel accord Safe Harbor pourraient constituer une partie de la solution. Dans tous les cas, ces solutions devront s'appuyer sur des mécanismes clairs et contraignants et comporter au minimum des obligations de nature à garantir le contrôle des programmes de surveillance par les autorités publiques », explique le G29.

En finir avec le flou juridique

Considérant que le niveau adéquat de protection des données personnelles n'est pas assuré, la Cour de Justice de l'Union européenne a invalidé, le 6 octobre 2015, l'accord dit Safe Harbor du 26 juillet 2000. Cette décision de justice concerne plus de 4000 entreprises américaines qui adhèrent volontairement au Safe Harbor, ainsi que les entreprises européennes qui leur transmettent des données.
Pour la Commission nationale de l'informatique et des libertés (CNIL), il ne s'agit pas d'un « vide », mais d'une « question juridique » sur la base légale des transferts de données vers les États-Unis. Aujourd'hui, il revient aux régulateurs nationaux en charge de la protection des données d'informer les parties prenantes et de fournir plus de « lisibilité » aux entreprises sur ce dossier.

Une solution attendue pour janvier 2016

Les institutions européennes et les États membres devront donc trouver, avec les autorités américaines, une solution « satisfaisante » avant le 31 janvier 2016. Faute de quoi, les régulateurs du G29 « s'engagent à mettre en œuvre toutes les actions nécessaires, y compris des actions répressives coordonnées ». En attendant, les autres outils encadrant les tranferts – les clauses contractuelles types et les règles internes d'entreprise (BCR ou Binding Corporate Rules) – peuvent être utilisées par les entreprises. Mais « les autorités de protection des données se réservent la possibilité de contrôler certains transferts, notamment à la suite des plaintes qu'elles pourraient recevoir », précise le G29.
Dans une récente tribune, l'avocat François Coupez, associé au cabinet ATIPIC, indiquait que l'adoption très probable d'ici la fin de l'année du règlement européen sur la protection des données « pourrait limiter la nécessité à moyen terme d'un Safe Harbor 2 ».

Source : http://www.silicon.fr/safe-harbor-ultimatum-g29-cnil-europeennes-129297.html
Par Ariane Beky

Des Macs en entreprise: la fin d’un tabou ? | Le Net Expert Informatique

	Des Macs en entreprise: la fin d’un tabou ?

S'il n'y a qu'un sujet qui est tabou à la DSI, c'est bien le Mac! Mais quand Cisco ou IBM fricottent avec Apple, le DSI peut commencer à se demander s'il n'est pas temps de retourner sa veste…

S'il n'y a qu'un sujet qui est tabou à la DSI, c'est bien le Mac!

Quand Cisco ou IBM fricottent avec Apple, le DSI peut commencer à se demander s'il n'est pas temps de retourner sa veste et de faire rentrer les Mac dans l'entreprise ! Mais comme ce sujet de discussion peut dégénérer rapidement, GreenSI fait appel à votre curiosité pour lire ce billet jusqu'à la fin, avant de décider de le brûler pour blasphème en récitant des incantations

Bien sûr, le couple Mac/MacOS est présent dans l'entreprise, qui n'est pas équipée uniquement de postes de travail Windows. La valeur par défaut est Windows mais on peut justifier l'usage des Macs, par exemple dans les services marketing pour travailler avec les agences de communication, ou dans certains secteurs d'activités. Sans oublier les machines pour les développeurs qui demandent de la puissance, de l'autonomie, et ne sont pas toutes connectées au réseau de l'entreprise (mais qu'a internet).

Mais la réalité du marché est que plus de 90% des systèmes livrés dans le monde le sont encore sous PC/Windows en 2015.

La raison est connue: Apple ne fait pas dans le low-cost. Donc à configurations égales, on a beau le tourner dans tous les sens, un Mac coûte plus cher à l'achat qu'un PC.

Mais dans l'entreprise qui raisonne « TCO » (total cost of ownership) incluant le coût du support et de la formation (de l'ordre de 1200-1500€/an/poste), le choix ne doit pas s'arrêter au seul prix d'achat.

Cette semaine, c'est sur Twitter avec l'effet d'une petite bombe qui a retenue l'attention de GreenSI, que Fletcher Previn, « Monsieur Poste de travail as a service » chez IBM, a annoncé les premiers résultats du déploiement massif de Mac chez IBM (au rythme de 1900 par semaine !) suite à l'accord signé entre Apple et IBM en 2014 autour du mobile:

- 5% des utilisateurs de Mac utilisent le service de dépannage interne (contre 40% pour les utilisateurs de PC)
- 98,7% des requêtes sont résolues au premier appel

Ce qui a valu à l'influent Marc Andreessen, et à Philip Schiller, le VP marketing d'Apple, un trait d'humour pour rappeler qui avait inventé le PC …

Dans le contexte d'IBM (population avertie et déploiement massif), les coûts de support sur Mac sont inférieurs à ceux sur PC. C'est donc bien la fin d'une légende. Et malgré un coût d'achat plus élevé, avec une certaine durée de vie et des coûts de support plus faibles, on peut imaginer que le choix et l'achat de Mac soit plus rentable pour l'entreprise en terme de TCO.

Sans compter qu'avec la montée en puissance de la mobilité et de l'internet mobile, l'OS le plus utilisé en entreprise risque rapidement d'être… Android. Et éventuellement iOS avec l'iPhone ou les nouveaux iPadPro (Un iPadPro pour l'entreprise, et alors?).

Le dernier argument des « pro-windows » – n'avoir qu'un seul OS dans l'entreprise pour tout simplifier – est en train de tomber. L'entreprise aura de facto plusieurs OS sur ses postes de travail, assurant l'accès au SI et les fonctions de collaboration entre salariés, qui sont fixes mais aussi mobiles.

Comme le poste de travail, la téléphonie d'entreprise est aussi devenue fixe et mobile. Début septembre, c'est Cisco qui a signé un accord avec Apple pour optimiser ses réseaux pour les terminaux et les applications iOS. Son objectif, pousser l'intégration de l'iPhone dans les environnements d'entreprise (notamment WebEx), et ses liens avec les téléphones fixes de bureau Cisco. La téléphonie et la collaboration autour des communications est aussi un enjeu de productivité pour l'entreprise, et Apple ne pouvait rester isolé avec son propre système – iPhone – sans mieux l'intégrer avec les infrastructures de l'entreprise.

Dans ce contexte, la stratégie multi-plateformes de Microsoft avec Windows 10 sur tous les terminaux sera d'abord vue par le DSI comme la possibilité de choisir Windows sur les terminaux qu'il souhaite, et non pas d'avoir Windows partout.

Microsoft en est bien conscient et met les bouchées doubles en remplaçant Linc par Skype Entreprise dans la communication instantanée. Car Webex, comme Skype, sont les plateformes applicatives Cloud qui amènent plus de valeur pour l'entreprise à ces terminaux. De même pour Office 365, Google Entreprise et toutes les applications comme Boxnet, maintenant déclinées en version entreprise.

Alors pour un DSI, faire rentrer des Macs/iOS en entreprise à la place de PC/Windows, à côté des iPhones, est un tabou qui est certainement en train de voler en éclat. La perspective stratégique sur le poste de travail du salarié a changé avec le mobile et doit intégrer les coûts de supports et le ratio entre le nombre d'agents au support versus la population supportée. Un ratio qui visiblement est plus faible pour Apple.

À Apple maintenant de mettre en place le réseau de distribution attendu par les entreprises. GreenSI veut parler de celles qui n'achètent pas 50.000 Macs d'un coup dans le cadre d'accords stratégiques mondiaux signés dans la langue de Shakespeare

Denis JACOPINI est Expert Informatique assermenté, consultant et formateur en sécurité informatique et en mise en conformité de vos déclarations à la CNIL.

Nos domaines de compétence :

- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.zdnet.fr/actualites/des-macs-en-entreprise-la-fin-d-un-tabou-39826656.htm
Par Frédéric Charles pour Green SI

Projet de loi numérique : que réclament les acteurs du secteur ? | Le Net Expert Informatique

Le projet de loi numérique plus en détail

La période de concertation sur le projet de loi numérique s'est achevée, dimanche. 20 000 contributeurs ont donné leur avis, parmi lesquels de nombreuses organisations. Voici ce qu'ils demandent.

Qu'est-ce que les associations, organisations et entreprises ont pensé du projet de loi numérique mis en ligne au début du mois ? Ils ont été nombreux à donner leur avis, approuvant des articles, en critiquant d'autres, proposant des modifications, suppressions ou ajouts. Voici ce qu'ils demandent :

Open data
Si la plupart des acteurs saluent les avancées des articles 1 à 7 concernant l'open data, à l'image de l'Afnic et du Syndicat des éditeurs de la presse magazine, ils sont aussi nombreux à réclamer des précisions ou des mesures allant plus loin que celles avancées par le gouvernement. Le Conseil National du Numérique propose d'élargir massivement les obligations de diffusion des documents des organismes publics, tout comme Regards Citoyens, qui réclame un droit à la publication en Open Data pour tous les citoyens et CCM Benchmark (éditeur du JDN), qui réclame par ailleurs de réduire les délais de mise à disposition des données publiques –revendication partagée par le syndicat de la presse indépendante d'information en ligne.
Le Medef, s'il se dit favorable à l'open data par défaut, et demande une précision quant à la nature des documents visés, « afin d'éviter un champ large de documents concernés pouvant porter atteinte aux droits de propriété intellectuelle (…) ou encore au secret en matière commerciale et industrielle. » L'organisation patronale vote par ailleurs contre la réutilisation des données des services publics industriels et commerciaux, l'ouverture des données des délégations de service public et des subventions publiques.

L'INA pose la question des redevances
L'INA, de son côté, pose la question des redevances dans le cadre du droit d'accès des organismes publics aux données publiques : « Des redevances pourront-elles être établies, compte tenu notamment des coûts générés pour répondre à ces demandes de transmission ? » L'avenir de la Cada est aussi débattu : Le CCNum veut renforcer ses droits, CCM Benchmark s'oppose à une fusion avec la Cnil.
Se sont aussi exprimés sur le sujet la FIEEC, fédération de l'industrie, qui réclame le déploiement du protocole ouvert IPv6, l'AFNUM, syndicat professionnel qui représente les industriels des réseaux, des terminaux de l'électronique grand public, de la photographie et des objets connectés, ou encore l'Association des archivistes français (AAF).

Avis de consommateurs
L'article 15 du projet de loi, qui vise à « mieux informer les consommateurs sur les avis en ligne » en imposant aux sites Internet d'indiquer, de manière explicite, si les avis ont été vérifiés ou non, fait débat. S'il a reçu 421 votes positifs, contre seulement 49 mitigés et 18 négatifs, plusieurs acteurs proposent d'apporter des précisions au texte de loi. L'agence de voyage Nomade Aventure réclame de rendre obligatoire l'affichage de tous les avis et leur classement par défaut par ordre chronologique pour plus de neutralité. Afnor Certification, qui délivre divers labels de qualité aux entreprises, demande à aller plus loin en mettant en place des outils pour informer les internautes dont les avis auraient été rejetés ou en instaurant un droit de réponse du responsable du produit ayant fait l'objet d'une critique.

Neutralité du Net
Le volet sur la neutralité du Net a recueilli 1 370 votes positifs, 45 mitigés et seulement 11 contre. Le Syndicat des éditeurs de la presse magazine a par exemple salué la disposition, tout comme l'Afnum et l'Afnic.

Alcatel-Lucent : des réserves sur la Neutralité du Net
Alcatel-Lucent se prononce cependant contre le texte en expliquant que la notion de « classe de service » est nécessaire et pas incompatible avec un Internet « ouvert et transparent : « la classification des paquets et la réservation de la bande passante pour la transmission de certains flux s'avère nécessaire à un bon fonctionnement des réseaux et à une bonne expérience utilisateur. » Le Syntec Numérique explique de son côté juger inutile la disposition discutée en ce moment au niveau européen et a critiqué l'extension des pouvoirs de l'Arcep aux « personnes fournissant des services de communication en ligne ».

Loyauté des plateformes
Le projet de loi numérique veut imposer aux plateformes l'obligation de fournir une information loyale et claire sur leurs liens capitalistiques ou de rémunération avec les fournisseurs des offres qu'elles référencent (lire : « Loyauté des plateformes : ce que va changer la Loi sur le numérique », du 14/10/15). Globalement bien reçu, le texte a tout de même enregistré certaines réserves. L'Afnum, d'abord, estime « qu'il est trop tôt pour légiférer au niveau national » et qu'il serait « préférable de traiter ce sujet au niveau européen ». Le CNNum réclame de son côté l'introduction du principe de contradiction dans le retrait ou déréférencement de contenus par les plateformes : « chacune des parties à un litige est en mesure de discuter et contester l'énoncé des faits et des arguments que lui oppose son adversaire ».
L'Open Internet Project estime pour sa part que la portée actuelle du texte est trop étroite. L'organisation réclame de faire état des « gatekeepers », les plateformes dominantes par lesquelles les internautes passent pour accéder à d'autres, et de leur imposer une obligation de loyauté : « l'article, s'il oblige les plateformes à informer le consommateur au sujet des relations entretenues avec ses partenaires, ne leur interdit pas pour autant de pénaliser d'autres acteurs en ayant recours à des pratiques déloyales ».

Données personnelles
Le projet de loi numérique met notamment l'accent sur la protection des données personnelles des utilisateurs à travers plusieurs articles, salués par les contributeurs.

L'Afnic réclame un tiers de confiance pour la portabilité des données
Certains acteurs de l'écosystème, cependant, s'inquiètent de la mise en œuvre des dispositions : le Syndicat des éditeurs de la presse magazine se dit ainsi contre la portabilité des données : « Un droit à la portabilité des données trop étendu, par les contraintes fortes qu'il entraînerait, risque de détourner les acteurs du numérique de leurs efforts d'investissement et d'innovation. Le sujet, complexe donc, est actuellement à l'étude dans le cadre des travaux menés au niveau européen, autour du projet de règlement de protection des données. » L'Afnic, au contraire, veut aller plus loin et réclame la possibilité de passer par un tiers de confiance pour s'assurer la portabilité de ses données.
La disposition sur la mort numérique (article 20), qui permet de décider par avance du sort de ses données en cas de décès, a été très bien reçue par les contributeurs (583 d'accord, 17 pas d'accord). Pourtant, selon Benjamin Rosoor, cofondateur de la start-up Transmitio qui permet de protéger et transmettre les informations de son entreprise, « il semble difficile d'imposer par une loi française ou même européenne des procédures à des services qui sont souvent américains ». De manière générale, les contributeurs s'interrogent sur les sanctions en cas de non-respect des services.
L'ACN, Alliance pour la confiance numérique s'est aussi exprimée sur plusieurs articles concernant les données privées. Elle propose notamment que le certificat de conformité créé par la loi, qui permettra aux entreprises d'obtenir des avis de la CNIL sur leurs méthodes de gestion des données personnelles, soit délivré par des organismes indépendants.

Domaine public informationnel
Les éditeurs vent debout contre le domaine public informationnel
L'article 8, portant sur la définition positive du domaine commun informationnel –le but étant d'interdire de revendiquer des droits sur ce qui appartient au domaine public- ne fait pas l'unanimité. Si les contributeurs se sont prononcés en majorité pour (655 d'accord contre 83 pas d'accord et 84 avis mitigés), plusieurs acteurs réclament la suppression du texte, qui pourrait constituer un précédent facheux pour leur économie, comme la Société civile des auteurs multimédias (Scam), la Société des auteurs et compositeurs dramatiques, le Syndicat national de l'édition, les éditions Actes Sud et les éditions Dalloz ou encore Hachette.

Propositions annexes
Outre commenter les articles et proposer des modifications, plusieurs acteurs ont émis des propositions subsidiaires. Regards Citoyens, par exemple, propose de publier en Open data, en plus des subventions, toutes les informations liées aux fonctions des élus, à leurs indemnités et liens d'intérêts. Le Conseil National du Numérique demande la création d'un médiateur du numérique ou encore de pouvoir ouvrir une action collective sur la protection des données personnelles. Medias-Cite réclame la création d'un label « entreprise numérique citoyenne » et propose de limiter l'obsolescence programmée en promouvant les fablabs et Repairs Cafés.

Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.journaldunet.com/ebusiness/le-net/1164530-projet-de-loi-numerique-que-reclament-les-acteurs-du-secteur/

Ce que va changer la Loi sur le numérique à propos de la protection des données personnelles | Le Net Expert

Informatique

	Ce que va changer la Loi sur le numérique à propos de la protection des données personnelles

Secret des correspondances, droit à l'oubli ou encore pouvoirs de la Cnil… Le projet de loi veut imposer le concept de libre disposition des données personnelles d'un utilisateur.

Le tant attendu projet de loi pour la République numérique d'Axelle Lemaire a enfin pris forme. Fruit d'une grande concertation nationale de près d'un an, le projet de loi est désormais soumis à une ultime consultation en ligne jusqu'au 18 octobre. L'occasion pour le JDN de faire le point sur les différents volets de ce projet de loi participatif.
Cette loi est « une loi de progrès du droit », explique le gouvernement. Une loi qui affirme les grands principes nécessaires à la protection des citoyens, en matière de données personnelles notamment, nous promet-on. Ainsi le projet de loi prend-t-il le soin de réaffirmer le fameux secret des correspondances dans un article 22 qui stipule que « tout traitement automatisé d'analyse du contenu de la correspondance en ligne ou des documents joints a`celle-ci constitue une atteinte au secret des correspondances, sauf lorsque ce traitement a pour fonction l'affichage, le tri ou l'acheminement de ces correspondances, ou la détection de contenus non sollicités ou malveillants ». Oui, Gmail, Outlook ou Yahoo mail peuvent étudier vos échanges d'emails s'il s'agit de mettre en exergue ceux-qui sont les plus à même de vous intéresser ou, au contraire, de filtrer les spams.

Google ne pourra plus lire vos mails pour des pubs ciblées
« Ces services ne pourront en revanche plus examiner automatiquement le contenu des correspondances privées échangées en leur sein pour des fins commerciales, comme ils pouvaient le faire jusque-là », explique Alan Walter, avocat associé au sein du cabinet Walter Billet. La fin de la publicité ciblée via le scan des mails dans Gmail et consorts ? Les Français pourront en tout cas désormais invoquer l'article 226.1 et suivant du code Pénal pour poursuivre en justice les contrevenants. Mais l'histoire récente montre qu'un tel combat judiciaire ne peut se mener avec succès que s'il est mené à l'échelle européenne. Ne reste plus qu'à espérer qu'il fera effet domino chez nos voisins.
Alors que la quantité des données nous concernant, online, croît de manière exponentielle, la loi veut redonner le contrôle aux individus sur leurs données personnelles. C'est le principe de la « libre disposition de ses données » de l'article 16 qui se veut une alternative à l'absence d'un droit de propriété sur les données. Et dans cette perspective, le projet de loi fait de la Cnil un véritable garde-fou entre l'internaute et les services de traitement de données. Sur le droit à l'oubli des mineurs, celle-ci pourra être saisie en cas d'absence ou d'absence de réponse de la part du responsable de traitement. Elle se prononcera sur la demande dans « un délai de 15 jours », affirme le projet de loi. Un vœu pieux selon Alan Walter qui affirme que « l'institution va vite être dépassée ». Une prédiction que les problèmes rencontrés par Google au moment d'appliquer lui-même le droit à l'oubli (56 jours pour traiter les demandes au début) semble conforter.

Plus de prérogatives pour la Cnil… Mais quid des moyens ?
L'avocat estime qu'il en va de même pour l'article 17 qui propose au président d'assemblée parlementaire de « soumettre a`l'avis de la commission une proposition de loi comportant des dispositions relatives a`la protection des données a`caractère personnel » et l'article 18 qui donne à la Cnil le pouvoir de « certifier la conformité du processus d'anonymisation totale ou partielles de jeux de données à caractère personnel ». « C'est très positif de donner plus de prérogatives à l'institution mais, s'il y a une nette amélioration récemment, on se rend compte que les gens de la Cnil n'ont eux-mêmes pas toujours le temps de répondre à nos sollicitations », explique-t-il. « Et je doute qu'ils soient vraiment outillés pour le faire à un tel rythme et une telle échelle avant quelques années ». D'autant que se profile dans les années à venir une fusion compliquées avec la Cada.
L'article 21 du projet de loi renforce en tout cas la procédure de sanction de la Cnil, qui pourra prononcer « une sanction immédiate lorsque le manquement ne peut pas être réparé. Dans un exercice de pédagogie, le gouvernement donne l'exemple suivant : « la CNIL pourra sanctionner financièrement une entreprise ayant perdu des milliers d'adresses email, ce qui n'est pas possible aujourd'hui (simple mise en demeure) ». Le projet de loi propose également de raccourcir les délais de mise en demeure en cas d'urgence, le ramenant à 24 heures. « On notera quand même que le montant de la sanction pécuniaire ne bouge lui pas », note Alan Walter, un brin taquin. D'un montant maximal de 150 000 euros, et, en cas de récidive, jusqu'à 300 000 euros. Un montant par vraiment dissuassif pour les géants américains.

Comme tout professionnel de l'informatique et de l'Internet, il est de mon devoir de vous informer que vous devez mettre en conformité et déclarer à la CNIL tous vos traitement de données à caractère personnel (factures, contacts, emails…).
Même si remplir un formulaire de déclaration à la CNIL est simple et gratuit, il vous engage cependant, par la signature que vous apposez, à respecter point par point la loi Informatique et Libertés. Cette démarche doit commencer par une analyse précise et confidentielle de l'ensemble de vos systèmes de traitements de données. Nous pouvons vous accompagner pour vous mettre en conformité avec la CNIL, former ou accompagner un C.I.L. (correspondant CNIL) ou sensibiliser les agents et salariés à l'hygiène informatique.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.journaldunet.com/ebusiness/le-net/1164005-protection-des-donnees-personnelles-loi-sur-le-numerique/
Par Nicolas Jaimes — JDN

Le FBI enquête sur une cyberattaque visant le groupe de médias Dow Jones | Le Net Expert Informatique

FBI enquête sur une cyberattaque visant le groupe de médias Dow Jones

La police fédérale américaine, le FBI, enquête sur une attaque informatique visant le groupe de médias Dow Jones (Wall Street Journal), une filiale de NewsCorp, l'empire de la presse du milliardaire Rupert Murdoch.

«Nous sommes au courant d'une attaque informatique (contre Dow Jones) et sommes en train d'enquêter», a déclaré à l'AFP une porte-parole de l'antenne new-yorkaise du FBI, confirmant des informations de presse.

Interrogée sur la possible origine russe des pirates informatiques comme l'affirme l'agence Bloomberg News, elle n'a pas souhaité commenter.

Des hackers auraient réussi à pénétrer illégalement le système informatique de Dow Jones & Co et auraient volé des informations sur des entreprises qui étaient sous embargo, selon Bloomberg.

Les titres de Dow Jones & Co (le Wall Street Journal, Barron ou encore l'agence d'informations éponyme) reçoivent, comme les autres médias, des informations sous embargo sur des entreprises ou des indicateurs économiques des agences gouvernementales susceptibles d'influencer les marchés, les opérations de fusions-acquisitions.

Cette attaque informatique serait plus sérieuse que celle qu'avait révélé il y a une semaine le groupe, assure Bloomberg News, citant des sources proches du dossier.

Il y a quelques jours, Dow Jones avait révélé que des pirates avaient essayé de s'introduire illégalement dans son système informatique pour y voler les données personnelles de près de 3.500 de ses clients.

Les pirates cherchaient à obtenir des informations dont des articles avant qu'ils ne soient publiées, croit savoir Bloomberg.

Source : http://lematin.ma/express/2015/le-fbi-enquete-sur-une-cyberattaque/233636.html

---

La Marine Américaine reprend

la navigation céleste | Le Net Expert Informatique

	La Marine Américaine reprend la navigation céleste

Face à la menace croissante des cyberattaques, l'US Navy repasse au sextant qui fait ainsi son retour dans l'armée la plus moderne au monde.

Après près de 20 ans d'interruption, l'Académie navale américaine d'Annapolis (Maryland) recommence à former ses aspirants à la navigation astronomique, vu le danger de plus en plus imminent des cyberattaques, rapporte le Washington Post.

« Nous nous sommes entièrement informatisés, en renonçant au sextant en faveur des ordinateurs qui sont vraiment excellents. Le problème, c'est qu'il n'y a plus de solution de secours », a déclaré au journal le lieutenant-colonel Ryan Rogers, titulaire de la chaire de navigation à l'Académie.

Le bon vieux sextant fait son retour dans l'armée la plus moderne au monde, car cet instrument restera fiable en cas de cyberattaque. La réintroduction du sextant marque en quelque sorte la fin de la croyance en l'infaillibilité technologique.

L'été dernier, les aspirants de l'Académie d'Annapolis ont commencé à recevoir trois heures de cours hebdomadaires. La promotion 2017 sera la première à avoir des rudiments dans l'utilisation du sextant.

Dans le contexte des scandales d'espionnage informatique qui défraient la chronique depuis un certain temps avec les révélations sur l'activité de l'agence américaine NSA, bien des pays, dont la Russie, envisagent un retour aux vieilles méthodes.

Les spécialistes soulignent que du point de vue de la sécurité, toute sorte de communication électronique est vulnérable. On peut capter n'importe quelle information depuis un ordinateur, il existe des moyens de protection, mais sans garantie à 100 % de leur sûreté. Pour garder des secrets, la « méthode primitive » est préférable: la main humaine avec un stylo ou la machine à écrire.

Source :

http://fr.sputniknews.com/international/20151017/1018907696/usa-marine-sextant-cyberattaques.html

Le hack étonnant qui peut tromper Siri, Cortana et Google Now grâce aux ondes radio | Le Net Expert Informatique

	Le hack étonnant qui peut tromper Siri, Cortana et Google Now grâce aux ondes radio

Deux hackers français ont montré qu'il était possible d'injecter des commandes vocales par l'émission d'ondes radioélectriques. Mais cette attaque nécessite quand même un peu de matériel.

Les assistants vocaux sont bien pratiques et déployés sur pratiquement tous les smartphones aujourd'hui, qu'il s'agisse de Siri pour iOS, de Google Voice pour Android ou de Cortana pour Windows 10 Mobile. Mais ces interfaces présentent des vulnérabilités que deux chercheurs en sécurité de l'ANSSI – José Lopes Esteves et Chaouki Kasmi – ont mis en lumière dans un article publié par le magazine scientifique IEEE Electromagnetic Compatibility. Ils ont également présenté leurs recherches en juin dernier, à l'occasion de la conférence académique SSTIC, qui s'était déroulée à Rennes.

Les deux chercheurs ont montré qu'il était possible d'injecter des commandes vocales dans ces systèmes par l'intermédiaire d'ondes radio. Comment? Au travers des écouteurs du kit mains-libres. « Le câble des écouteurs est une bonne antenne pour des fréquences comprises entre 80 et 108 MHz », explique José Lopez Esteves, dans la vidéo de leur présentation SSTIC. L'idée du hack est donc d'enregistrer une commande vocale, de la moduler en amplitude sur une onde porteuse de la bande 80-108 MHz et de l'envoyer vers les écouteurs. Ce rayonnement va induire dans le câble un signal électrique qui va automatiquement être traité par le système de commandes vocales, après avoir été filtré et amplifié. Au final, « on obtient un signal relativement proche du signal vocal original », précise M. Lopes Esteves.

Cette attaque fonctionne avec tous les principaux systèmes vocaux disponibles, à savoir Cortana, Siri et Google Voice. Il y a néanmoins une condition nécessaire, c'est que la commande vocale soit activée, c'est-à-dire que l'on puisse interroger l'assistant virtuel par un simple mot-clé (« OK Google », « Dis Siri » ou « Hey Cortana »), ce qui n'est pas une option par défaut sur les smartphones.

L'impact de l'attaque dépendra de l'état du téléphone. Il sera maximal s'il est déverrouillé. L'assistant vocal pourra alors accéder au carnet d'adresse, envoyer un message, ouvrir une page web, lancer une application, etc. « On pourra par exemple envoyer une commande pour que l'appareil ouvre un site web malveillant », souligne M. Lopes Esteves. Le mieux dans cette affaire, c'est que l'utilisateur pourrait ne rien remarquer du tout car la commande vocale injectée est totalement silencieuse pour lui. Seul l'assistant vocal l'entendra.

Limité à quelques mètres

En revanche, si le téléphone est verrouillé, l'assistant vocal n'aura qu'un accès limité, comme par exemple interroger l'appli météo ou appeler un numéro. Ce qui n'est pas rien quand même, car il est possible alors de passer des coups de fil en douce pour générer des revenus frauduleux (via des numéros surtaxés) ou pour simplement espionner les conversations environnantes.

Si ce piratage est relativement simple sur le principe, il nécessite quand même du matériel. Avec un équipement radio de la taille d'un sac à dos, le rayon d'action est de seulement deux mètres. Pour atteindre cinq mètres, il faut déjà une camionnette. Et dans ce cas, mieux vaut ne pas se trouver à proximité de l'émetteur, car le niveau de rayonnement sera alors plutôt intense.

Source :
http://www.01net.com/actualites/siri-cortana-et-google-voice-sont-vulnerables-aux-attaques-radio-922670.html
Par Gilbert KALLENBORN

Alerte Ransomware : Attaque massive dans le doc | Le Net Expert Informatique

	**Alerte Ransomware : Attaque massive dans le doc**

Depuis ce mardi matin, des milliers de courriers malveillants visent entreprises et collectivités locales françaises. Prudence !

Ils se font passer pour des fax en attente ou pour un communiqué de presse. Ils sont cachés dans des courriels publiés ce mardi matin, dans une diffusion massive et malveillante. ZATAZ.COM a pu en référencer 300 différents, en quelques minutes. Des courriers électroniques contenant des pièces jointes qu'il ne faut surtout pas ouvrir. Des fichiers Word, PowerPoint piégés. Ils vont chercher sur la toile un code malveillant qui, dans la majorité des cas, était un ransomware ou encore le code pirate Dridex.

Dridex, est un outil qui exploite la technologie du peer-to-peer (P2P) afin d'attaquer le contenu des ordinateurs infiltrés. Mission, mettre la main sur des données bancaires. Le département américain de la Sécurité intérieure (DHS), en collaboration avec le Federal Bureau of Investigation (FBI) et le ministère de la Justice (DOJ) ont publié une alerte quelques heures après l'annonce de ZATAZ, preuve que cette diffusion massive est à échelle internationale.

Dridex est un ensemble de logiciels malveillants multifonctionnel qui exploite le langage Macro proposés dans les outils de Microsoft. L'objectif principal de Dridex est d'infecter les ordinateurs, voler des informations d'identification, et obtenir l'argent des comptes bancaires des victimes infiltrées. Exploitée principalement comme un cheval de Troie bancaire, Dridex est généralement distribué par courrier électronique, comme le cas de ce lundi matin.

Un système infecté par Dridex peut être utilisé pour envoyer du spam, participer à DDoS… la question est de savoir pourquoi une telle attaque, en pleine semaine. Le bot des pirates a-t-il été mis en action car le besoin en données bancaires se fait sentir chez les malveillants après les dernières importantes arrestations dans le monde du carding international ?

Microsoft propose un outil pour scanner votre ordinateur à la recherche du malveillant code : http://www.microsoft.com/security/scanner/en-us/default.aspx

---

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.

Nos domaines de compétence :

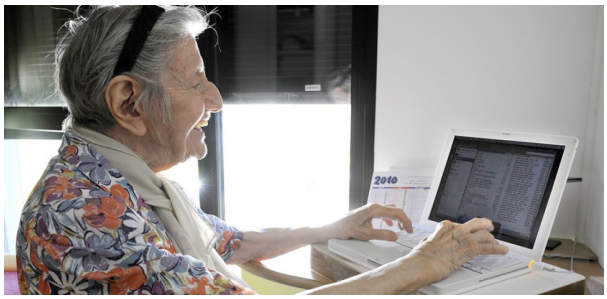
- **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
- **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
- **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.

Contactez-nous

Cet article vous plait ? Partagez !
Un avis ? Laissez-nous un commentaire !

Source : http://www.zataz.com/attaque-massive-ransomware-dans-le-doc/
Par Damien Bancal

Pas assez connectée pour être menacée ? Madame Walsh s’est pourtant fait pirater | Le Net Expert Informatique



Pas assez connectée pour être menacée ? Madame Walsh s’est pourtant fait pirater

Le piratage, ça n'arrive pas qu'aux autres. Et il n'y a pas besoin d'être ultra-connecté pour en être victime. C'est ce que raconte le « New York Times », avec l'exemple de Madame Walsh, vivant en Californie.

Cette grand-mère de six petits-enfants a accepté de servir de cobaye à deux hackeurs, se pensant à l'abri, puisque n'étant pas quelqu'un de « connecté ». Mme Walsh explique ne disposer d'aucun objet connecté (montre, etc.), sa maison n'est équipée d'aucun appareil technologique récent (thermostat connecté ou autre), et elle n'est pas une grande adepte des gadgets électroniques. Bien sûr, elle dispose d'un compte Facebook, mais n'y publie jamais rien, et s'en sert uniquement pour rester en contact avec des amis. Et pourtant.

E-mail, PaylPal, télévision et garage piratés

Les hackeurs ont bien réussi à pirater Madame Walsh. Le quotidien raconte que les pirates ont successivement testé plusieurs pistes pour tenter de s'attaquer à la grand-mère. Si son compte Facebook se révèle bien protégé, la découverte d'un « J'aime » pour une page de la plateforme de pétitions Change a été le déclic. Dix minutes plus tard, les hackeurs adressent à Mme Walsh un faux e-mail émanant de Change.org proposant de signer une fausse pétition. Bingo, la grand-mère clique, et entre son identifiant et son mot de passe. La voilà victime de « phishing ».

Madame Walsh confesse au « New York Times » utiliser le même mot de passe sur l'ensemble des services internet. Les pirates sautent sur la brèche et s'introduisent dans sa messagerie e-mail pour récupérer ses données de sécurité sociale et d'assurance maladie, et de ses comptes PayPal et Miles.

Pis, les hackeurs s'introduisent également dans le compte e-mail de sa fille, dont le code était « caché » dans un message. Enfin, ils laissent sur l'ordinateur de Mme Walsh un virus qui enregistre tout ce qui est tapé et remplace les publicités des sites visités afin de leur générer des revenus.

Pas repus, les deux hackeurs se sont attaqués à sa maison. En une heure et demie, ils ont pris le contrôle de sa télé (l'installateur du câble n'avait pas protégé la connexion) et trouvé un moyen d'ouvrir à distance la porte de son garage (via un procédé de « brute force » qui a essayé des centaines de combinaisons possibles avant de tomber sur la bonne pour la porte électrique).

Le phishing, risque numéro un

L'exemple du « New York Times » est extrême mais illustre bien que personne n'est à l'abri d'un piratage, même ceux qui se pensent « trop peu connecté pour être en danger ». Et le risque premier demeure le phishing, aussi appelé hameçonnage.

Aujourd'hui, plus de 90% des attaques dans le monde démarrent par un e-mail de phishing », affirme Ismet Geri, directeur général pour la France et l'Europe du Sud de Proofpoint, société spécialisée dans la sécurité des e-mails.

Un e-mail sur 392 serait une tentative de phishing, estime l'entreprise de sécurité informatique Symantec dans son dernier rapport. Au total, 37,3 millions d'internautes sont tombés dans le panneau dans le monde, affirme une enquête de la société de sécurité Kaspersky. La France se classe septième pays au monde dans les victimes avec un internaute sur 30 floué.

LIRE »J'ai cliqué » : chronique d'un phishing ordinaire

L'objectif des pirates est simple : récupérer des coordonnées bancaires, mais aussi des informations personnelles. Selon Symantec, au marché noir, les détails d'une carte de crédit se revendent entre 0,50 et 20 dollars, un passeport scanné 1 à 2 dollars, l'accès à un compte cloud 7 à 8 dollars, l'accès à un compte de jeux vidéo en ligne 10 à 15 dollars, etc.

L'utilisation de ces données est évidente. Les données bancaires permettent d'effectuer des achats en ligne, tandis que les informations personnelles vont permettre de s'identifier sur l'ensemble des services. Surtout que le sésame identifiant/mot de passe devient un Graal, quand on sait que 75% des Français utilisent toujours le même mot de passe.

Je m'estimais plutôt malin, je m'étais trompé ! », a confié le blogueur Thomas Messias au « Parisien » après un piratage de ses comptes. « Evidemment, j'utilisais le même mot de passe pour eBay et pour tous les autres sites… »

Voilà Madame Walsh prévenue. Et pour ce qui est de la maison, de nombreux experts en informatique démontraint régulièrement comment prendre le contrôle d'objets usuels. Cet été, le hackeur Samy Kamkar a démontré comment ouvrir des portes de garage à partir d'un jouet Mattel en moins de 10 secondes :

Denis JACOPINI est Expert Informatique, conseiller et formateur en entreprises et collectivités et chargé de cours à l'Université.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source :
http://tempsreel.nouvelobs.com/tech/20151015.OBS7721/pas-assez-connectee-pour-etre-menacee-madame-walsh-s-est-pourtant-fait-pirater.html#xtor=EPR-1-ObsActu8h-20151016