Sony Pictures va piéger les films piratés pour mettre un terme aux fuites

Sony Pictures va piéger les films piratés pour mettre un terme aux fuites

Victime d’un piratage à l’envergure peu commune, Sony Pictures semble être plus que déterminé à mettre un terme à la diffusion de ses fichiers sur le Net. En effet, la filiale du groupe japonais orchestrerait elle-même plusieurs opérations de piratage afin d’empêcher le partage de documents sensibles…

L’information est révélée par le site Re/Code, qui évoque des sources « en connaissance directe du dossier ». Selon celles-ci, Sony Pictures s’appuierait sur les datacenters asiatiques d’Amazon utilisés pour fournir les services cloud du marchand afin de mener une attaque par déni de service sur les sites proposant de télécharger des données issues du récent piratage dont la compagnie a été victime. Et ce ne serait pas tout : le Japonais s’attèlerait également à décourager les curieux en diffusant des copies piégées des fichiers volés.
Rappelons que Sony Pictures a toutes les raisons de chercher à mettre un terme à ces fuites. Outre des films encore inédits, la centaine de To de données volées contenait aussi de nombreux documents personnels d’employés et d’acteurs, des rapports financiers, ou encore des accords confidentiels. Si la diffusion de ces informations a d’ores et déjà occasionné quelques grincements de dents, le Japonais se doit de limiter les dégâts, d’autant que tout ce butin numérique n’est pas encore disponible sur le Web. La méthode, toutefois, peut laisser perplexe.
Cependant, ce n’est pas la première fois qu’un poids lourd des médias combat le feu par le feu. En 2007, plusieurs firmes, dont Sony Pictures mais aussi Universal, EMI, Paramount ou encore Ubisoft avaient été pointées du doigt pour avoir eu recours aux services de MediaDefender, dont les tactiques anti-piratage étaient fort décriées. En effet, ce spécialiste de la défense des intérêts des producteurs de médias pratiquait déjà la diffusion de faux fichiers afin de rendre le piratage franchement laborieux – sans compter qu’il s’était particulièrement illustré par un litige avec The Pirate Bay, qui l’accusait, non sans preuve, d’avoir orchestré une attaque en bonne et due forme contre ses serveurs.

Mais revenons-en à l’affaire qui nous occupe. Pour l’heure, les spécialistes qui se penchent sur le cas de Sony Pictures sont unanimes : il s’agit d’une attaque sophistiquée, qui aurait sans l’ombre d’un doute fonctionné contre une vaste majorité de systèmes. Son origine, toutefois, demeure à confirmer. Bien que les regards se soient d’emblée tournés vers la Corée du Nord, et bien que les pirates aient explicitement demandé l’annulation du film The Interview, qui met en scène l’assassinat de Kim Jong-un par deux journalistes plutôt limités, le régime nie avoir avoir entrepris une quelconque action à l’encontre de Sony Pictures au-delà de ses sommations de renoncer au long-métrage. Une autre piste, de plus, a fait son apparition : une des salves de leaks (fuites) a été orchestrée depuis le très chic hôtel St. Regis, à Bangkok. De quoi s’interroger sur la véritable identité des curieusement vindicatifs Guardians of Peace.

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

Source : http://www.lesnumeriques.com/sony-pictures-mene-attaque-ddos-pour-mettre-terme-fuites-n37601.html
Par Johann Breton

Cyber-sécurité : 10 tendances pour 2015

	Cyber-sécurité : 10 tendances pour 2015

L'année 2014 a été particulièrement chargée pour les professionnels de la sécurité informatique. A quoi s'attendre pour 2015 ? Le point avec Thierry Karsenti, directeur technique Europe de Check Point.

Pour l'année 2014, « nous nous attendions à une augmentation des tentatives d'ingénierie sociale, et l'avons bien constatée. Elles ont conduit à d'importantes fuites de données dans plusieurs enseignes bien connues. Les campagnes de logiciels malveillants ciblées se sont également intensifiées. Les attaques de « RAM scraping » et les attaques de rançonneurs ont fait les gros titres. Le nombre de problèmes de sécurité mobile a également continué d'augmenter, indique Thierry Karsenti. Le hic, ce sont les vulnérabilités massives qui ont été découvertes dans des composants informatiques établis, tels que Heartbleed et BadUSB, qui ont touché des dizaines de millions de sites web et d'appareils dans le monde entier. Personne n'y avait été préparé. 2015 verra-t-il les mêmes cyber-risques ?

1. **Les logiciels malveillants « zéro seconde »**

Plus d'un tiers des entreprises auraient téléchargé au moins un fichier infecté par des logiciels malveillants inconnus au cours de l'année dernière. Les auteurs de logiciels malveillants utilisent de plus en plus des outils spécialisés de masquage, afin que leurs attaques puissent contourner les mécanismes de détection des produits antimalwares et infiltrer les réseaux. Efficaces, les bots continueront d'être une technique d'attaque privilégiée, indique Thierry Karsenti.

2. **La mobilité**

Comme vecteurs d'attaque, les appareils mobiles offrent un accès direct à des actifs plus variés et plus précieux que tout autre moyen d'attaque individuel. « C'est également le maillon faible de la chaîne de sécurité, qui donne aux agresseurs un accès à des informations personnellement identifiables, des mots de passe, la messagerie professionnelle et personnelle, des documents professionnels, et l'accès aux réseaux et aux applications d'entreprise », précise le directeur technique.

3. **Les systèmes de paiement mobile**

Le lancement d'Apple Pay avec l'iPhone 6 est susceptible de relancer l'adoption des systèmes de paiement mobiles par les consommateurs, ainsi que d'autres systèmes de paiement concurrents : "Tous ces systèmes n'ont pas été testés pour résister à de réelles menaces, ce qui pourrait signifier d'importantes chances de succès pour les agresseurs qui trouveront des vulnérabilités à exploiter ».

4. **Les failles dans l'open source**

Qu'il s'agisse de Heartbleed (voir l'interview de Patrick Duboys, fondateur d'Alice and Bob http://www.solutions-logiciels.com/actualites.php?actu=14573) ou de Shellshock (voir l'interview vidéo de Vincent Hinderer, expert en cyber-sécurité au Cert du groupe Lexsi http://www.solutions-logiciels.com/actualites.php?actu=15039), les vulnérabilités critiques des plates-formes open source communément utilisées (Windows, Linux, iOS) sont très prisées par les agresseurs car elles offrent d'énormes possibilités. Logiquement, ces derniers vont donc continuer de rechercher des failles pour essayer de les exploiter.

5. **Les attaques sur les infrastructures critiques**

Les systèmes Scada qui commandent les processus industriels devenant de plus en plus connectés, cela va étendre les vecteurs d'attaque qui ont déjà été exploités par des agents logiciels malveillants connus tels que Stuxnet. Près de 70% des entreprises d'infrastructures critiques interrogées par le Ponemon Institute ont subi des attaques au cours de l'année passée.

6. **Les objets connectés**

L'Internet des objets fournit aux criminels un réseau mieux connecté et plus efficace pour lancer des attaques. Les entreprises doivent se préparer à leur impact.

7. **Les réseaux définis par logiciel (SDN)**

La sécurité n'est pas intégrée au concept SDN, « et doit l'être », affirme Thierry Karsenti qui enchérit : « *Avec son adoption croissante dans les centres de données, nous nous attendons à voir des attaques ciblées qui tentent d'exploiter les contrôleurs centraux SDN pour prendre le contrôle des réseaux et contourner les protections réseau* ».

8. **L'unification des couches de sécurité**

Pour lui, les architectures de sécurité monocouche et les solutions isolées provenant de différents fournisseurs n'offrent plus une protection efficace pour les entreprises. Il affirme que de plus en plus de fournisseurs proposeront des protections unifiées issues de développements, de partenariats et d'acquisitions.

9. **Les protections en mode SaaS**

Thierry Karsenti prévoit « une utilisation croissante des solutions de sécurité sous forme de services pour fournir visibilité, contrôle, prévention des menaces et protection des données ». Cette augmentation se fera parallèlement à l'utilisation croissante des services de sécurité externalisés dans le Cloud public.

10. **L'évolution des analyses grâce au Big Data**

Le Big Data va apporter d'énormes possibilités à l'analyse des menaces pour identifier de nouveaux schémas d'attaque, selon l'éditeur. Les fournisseurs intégreront de plus en plus ces capacités analytiques à leurs solutions, et les entreprises devront également investir dans leurs propres systèmes d'analyse pour prendre les bonnes décisions en fonction du contexte et des menaces pesant sur leur activité. Le partage collaboratif de renseignements sur les menaces continuera de se développer, pour proposer des protections à jour qui répondent aux besoins spécifiques des utilisateurs finaux. Le directeur technique de Check Point ajoute que ces possibilités alimenteront à leur tour des solutions de sécurité unifiées capables de fournir automatiquement une protection contre les nouvelles menaces émergentes pour renforcer la sécurité des entreprises.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…
Source : http://www.solutions-logiciels.com/actualites.php?actu=15189&titre=Cyber-securite-10-tendances-pour-2015 Par Juliette Paoli

Sony victime de hackers organisés et obstinés

Sony victime de hackers organisés et obstinés

Outre une société de sécurité mandatée par Sony, le FBI enquête lui aussi sur l'attaque informatique qui a visé récemment une filiale du groupe japonais, Sony Pictures. Et de premiers éléments ont été présentés par les enquêteurs au Sénat américain.

Ainsi comme les experts en sécurité de Mandiant, le FBI estime que l'attaque était inhabituelle et complexe à prévenir. Seules quelques entreprises auraient eu la capacité de bloquer la réalisation d'une telle attaque, estime l'agence fédérale.

Une attaque efficace sur 90% des entreprises

« Le malware qui a été utilisé aurait passé 90% des protections Internet qui sont déployées à l'heure actuelle dans le secteur privé et aurait probablement constitué un défi y compris pour un gouvernement fédéral » a déclaré le directeur adjoint de la division cybersécurité du FBI, Joe Demarest.

A l'occasion de cette audition devant un comité du Sénat, ce dernier a également précisé, selon The Hill, que l'attaqué était organisée et que son niveau de sophistication était extrêmement élevé. Quant à l'identité des auteurs, le FBI estime ne pas pouvoir la déterminer à ce stade, faute de preuves suffisantes.

Des liens avec la Corée du Nord ont été évoqués depuis le début de l'affaire, mais non confirmés. Les autorités du pays ont depuis démenti être à l'origine de cette cyberattaque, après avoir entretenu le flou au départ.

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

Source : http://www.zdnet.fr/actualites/sony-victime-de-hackers-organises-et-obstines-39811145.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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

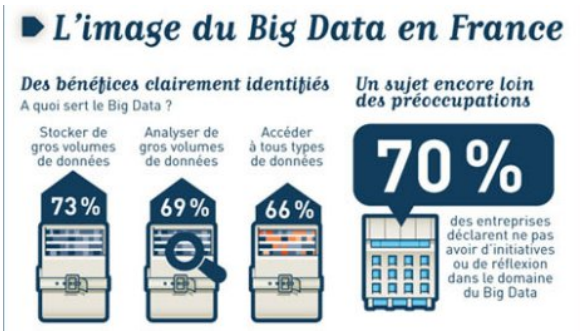
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

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

Comment stocker ses données en toute sécurité

Comment stocker ses données en toute sécurité

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



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

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

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

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

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

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

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

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

ESET s’engage auprès de Facebook pour protéger les utilisateurs des cyber-menaces

	ESET s’engage auprès de Facebook pour protéger les utilisateurs des cyber-menaces

ESET protège tous les utilisateurs Facebook contre le piratage.
ESET rejoint l'initiative Anti-malware lancé par Facebook et offre « ESET Online Scanner » à tous les utilisateurs de Facebook. Cette solution permet d'identifier les posts provenant non pas des utilisateurs mais de logiciels malveillants. Ces posts sont alors retirés en toute sécurité. ESET Online Scanner pour Facebook est disponible depuis le 03 décembre 2014 et pour tous les utilisateurs de Facebook.

« Notre but est d'offrir à nos utilisateurs la meilleure technologie afin d'améliorer l'utilisation de nos services et de protéger au mieux leurs appareils connectés. ESET Online Scanner va de manière significative diminuer le nombre de clics sur des liens malicieux, effectués des milliards de fois chaque jour sur Facebook » explique Chetan Gowda, Web developer chez Facebook.

La version dédiée d'ESET Online Scanner pour Facebook, a été conçue pour détecter et nettoyer les ordinateurs infectés des utilisateurs de Facebook. « ESET est heureux d'offrir ses services aux utilisateurs de Facebook du monde entier. ESET est reconnu pour sa légèreté et sa qualité de détection, ces deux atouts se retrouvent dans cette version pour Facebook, gratuitement.», annonce Ignacio Sbampato, Directeur Commercial et Marketing chez ESET HQ.

Votre ordinateur a besoin d'être nettoyéSuppression des logiciels malveillants Un fonctionnement simple et ciblé
Lorsqu'un utilisateur se connecte à son compte, Facebook cherche des comportements malicieux – comme l'envoi de spams ou de liens infectés provenant d'amis Facebook. Si ce type d'activité est détecté, Facebook invite l'utilisateur à utiliser ESET Online Scanner. L'analyse s'effectue directement sur Facebook, gratuitement et en tâche de fond.

L'utilisation du scanner est sans impact sur le système de l'utilisateur, de sorte qu'il peut continuer à utiliser son appareil sans gêne. Une fois l'analyse terminée, l'utilisateur reçoit une notification de la part de Facebook; un compte rendu du scan est aussi disponible. Le nettoyage commence une fois l'analyse terminée si des malwares ont été détectés.

Ce service pour Facebook est basé sur une solution gratuite ESET Online Scanner protégeant des millions d'internautes. Sur plus de 44 millions de scans, ESET Online Scanner a détecté avec succès des malwares dans presque la moitié des analyses.

ESET est un outil de protection et de désinfection que je conseille personnellement.
Vous avez envie de découvrir et de tester gratuitement ce logiciel de protection (ESET NOD32 ou ESET SMART SECURITY, je peux vous communiquer une licence sur simple demande.
Denis JACOPINI

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

Source : https://mail.google.com/mail/u/0/?hl=fr&shva=1#inbox/14a2e1044c5865c4

La protection des données personnelles, « atout pour la France », selon Manuel Valls

La protection des données personnelles, « atout pour la France », selon Manuel Valls

« Je mesure l'audace d'inviter un ancien ministre de l'intérieur parler de protection des données, cela peut paraître risqué » : surprise, c'est le premier ministre, Manuel Valls, qui a prononcé le discours d'ouverture de l'« European data governance forum », organisé lundi 8 décembre à Paris.

Cette journée de conférence au siège de l'Unesco a été mise en place par le G29, qui rassemble les autorités européennes de protection des données, afin de réfléchir à un « cadre éthique et juridique » sur la question des données personnelles.

Le chef du gouvernement a souligné à plusieurs reprises le rôle que doivent jouer, selon lui, les autorités européennes et les Etats : « Il serait erroné de penser que toute régulation tue l'innovation. La régulation, c'est le rôle des Etats. Les valeurs de la démocratie doivent peser sur le monde numérique, la loi doit s'y appliquer. »

Projet de loi sur le numérique

« En 2015 et 2016, la loi réaffirmera de manière solennelle le droit à la vie privée et à la protection des données personnelles, ainsi que le contrôle des actes des services de renseignement », a expliqué le premier ministre. Sans préciser si cette question sera abordée dans le cadre du projet de loi numérique, en 2015, ou s'il fera l'objet d'un texte distinct.

Manuel Valls et Mme Falque-Pierrotin, la présidente de la CNIL, ont également rappelé que 2015 serait l'année du règlement sur les données personnelles, adopté au printemps par le parlement européen et qui doit désormais faire l'objet d'un accord entre les Etats membres. Sur ce sujet, le premier ministre a souligné « le soutien de la France à la réflexion sur le règlement sur les données », tandis que Mme Falque-Pierrotin a estimé qu'il y avait « urgence à nous doter de cet instrument juridique unique pour toute l'Union ».

Sur la question très sensible de l'inclusion – ou non – de la lucrative question des données personnelles dans les négociations sur les traités de libre-échange actuellement en négociation notamment entre l'UE et les Etats-Unis, M. Valls s'est voulu rassurant : « La France veillera, dans les négociations sur les traités de libre-échange, à ce que le standard européen soit préservé. »

« DÉFICIT DE CONFIANCE »

Le gouvernement français en est convaincu, a martelé Manuel Valls : la protection des données est un atout économique. « L'Europe doit faire de la protection des données personnelles un argument d'attractivité et de compétitivité. L'utilisateur doit pouvoir faire ses choix sur ses propres données en toute connaissance. Cela a un potentiel économique énorme. »

Un avis partagé par Mme Falque-Pierrotin : « Il ne faut pas que le déficit de confiance se transforme en méfiance » générale au sein de l'écosystème numérique. « Le monde a changé. Certains voudraient faire croire que la vieille histoire de la protection des données est dépassée », a conclu Manuel Valls. « Chaque époque a son combat : le droit des femmes, l'abolition de la peine de mort… La France y a tenu sa place. C'est parce que la France est le pays des droits de l'homme qu'elle doit faire de la protection des données un grand combat pour les droits humains. »

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

Source : http://www.lemonde.fr/pixels/article/2014/12/08/la-protection-des-donnees-personnelles-atout-pour-la-france-selon-manuel-valls_4536408_4408996.html par Martin Untersinger

Le PSN inaccessible suite à une attaque de Lizard Squad

Le PSN inaccessible suite à une attaque de Lizard Squad

Depuis quelques heures, le PlayStation Network de Sony est inaccessible pour de nombreux utilisateurs. Il s'agirait visiblement d'une nouvelle attaque DDOS, revendiquée par le groupe Lizard Squad.

Les problèmes touchent principalement l'Amérique du Nord, mais d'autres joueurs dans le monde ont remarqué quelques soucis depuis le milieu de la nuit.
PlayStation a rapidement tenu informé ses joueurs via Twitter, sans toutefois donner trop d'informations.
On ne sait donc pas vraiment quand seront réglés ces soucis, mais on sait au moins que les équipes de Sony travaillent à régler le problème, et c'est déjà une bonne nouvelle.
Le groupe Lizard Squad a revendiqué cette attaque, et c'est donc visiblement le serveur d'authentification de Sony qui est visé (comme l'indique ce tweet https://twitter.com/LizardPatrol/status/541751366297743360), perturbant ainsi grandement le PSN.
Espérons que tout rentrera dans l'ordre rapidement, puisque ces problèmes répétés risquent fortement d'agacer les joueurs.

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

Source : http://www.gameblog.fr/news/47390-le-psn-inaccessible-suite-a-une-attaque-de-lizard-squad