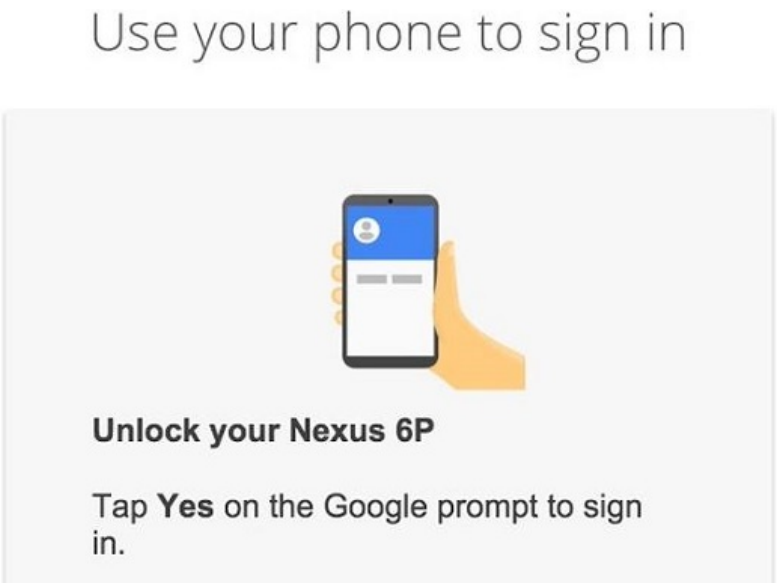
Google propose d’utiliser son téléphone en guise de mot de passe

Google propose d’utiliser son téléphone en guise de mot de passe

Saisir sur votre ordinateur un long mot de passe pour accéder à votre compte Google pourrait devenir une chose du passé pour peu que vous ayez en poche votre téléphone mobile.

Google s'efforce depuis longtemps de retirer les différentes barrières s'opposant à un accès rapide aux données. Et il pourrait bien avoir un nouveau tour dans son sac : au lieu de saisir comme d'habitude un mot de passe depuis son PC, sa tablette ou un autre terminal, vous pourriez simplement utiliser votre téléphone pour vous authentifier.
L'utilisateur de Reddit, Rohit Paul, a été invité à tester la fonctionnalité, qui nécessite encore un peu de saisie de la part de l'internaute.

Adresse Gmail saisie sur un mobile pour se connecter sur PC



Comme relevé par Android Police, une fois le téléphone de Rohit Paul enrôlé comme terminal d'authentification, ce dernier n'a plus eu qu'à entrer son adresse Gmail sur son smartphone pour se connecter à Google depuis son ordinateur.
Si le processus ne s'avère pas aussi rapide pour tous, ceux dont le mot de passe Google compte de nombreux caractères pourraient en profiter en réduisant le temps de saisie nécessaire à l'authentification.
Naturellement, si vous perdez votre téléphone ou si vous ne souhaitez plus utiliser ce mode d'authentification, vous pouvez toujours vous connecter à votre compte Google de manière classique.
Google n'ayant pas annoncé officiellement cette nouvelle fonctionnalité, les détails techniques de la procédure d'accès restent inconnus. La firme de Mountain View n'est cependant pas la seule à vouloir s'affranchir des mots de passe et à développer des méthodes alternatives d'authentification. C'est par exemple le cas de Microsoft dans Windows 10 au travers d'une fonction comme Next Generation Credentials.

Réagissez à cet article

Source : *Google souhaite remplacer le mot de passe par votre téléphone*

Quelques explications sur le projet de règlement européen sur la Protection des Données Personnelles dans les tuyaux

	Quelques explications sur le projet de règlement européen sur la Protection des Données Personnelles dans les tuyaux

---

Le texte de la réforme du cadre juridique de l'UE sur la protection des données personnelles stipule, notamment, que les entreprises devront communiquer pro-activement sur les failles dont elles seraient victimes.

Le Parlement européen et le Conseil de l'Union européenne se sont mis d'accord au sujet de la future modification du cadre juridique de l'UE sur la protection des données personnelles. La Commission européenne a publié le contenu de la reforme qu'elle propose, aboutissement d'âpres débats entamés en 2012. La reforme concerne aussi bien le droit des citoyens que les futures règles en la matière pour les entreprises. En cas de feu vert du Parlement européen et du Conseil début 2016, les nouvelles règles entreront en vigueur deux ans plus tard.

Obligation d'informer sans délais sur les violations données

Du côté des individus, le texte vise à leur donner davantage le contrôle de leurs données personnelles. Le texte fait notamment état d'un droit d'être informé en cas d'accès non autorisé aux données personnelles. Ce droit signifie que les entreprises et organisations doivent notifier à l'autorité nationale de contrôle, dans les plus brefs délais et de façon proactive, les violations de données graves, afin que les utilisateurs puissent prendre les mesures appropriées. Les nouvelles règles permettront en théorie aux citoyens de disposer de plus d'informations sur la façon dont leurs données sont traitées.
La reforme prévoit en outre un droit à la portabilité des données personnelles d'un prestataire de services à un autre et contient également un droit à l'oubli «plus clair», permettant aux personnes qui le désirent de voir leurs données supprimées dès lors qu'aucun motif légitime ne justifie leur conservation. Un autre article de la reforme fait déjà couler beaucoup d'encre dans les médias généraliste. Il concerne l'interdiction aux moins de 16 ans de s'inscrire à des médias sociaux tels que Facebook ou Instagram.

Les entreprises devront nommer un délégué aux données

Pour les entreprises, la Commission européenne propose des règles qui, selon elle, n'entravent pas le commerce, mais au contraire «créent des opportunités commerciales et encouragent l'innovation.» Un droit unique à l'échelle européenne devrait rendre moins coûteux l'exercice d'activités entrepreneuriales en Europe, précise le communiqué de l'UE. Lequel indique aussi que le règlement imposera que des garanties en matière de protection des données soient «intégrées aux produits et services dès la phase initiale de leur conception.»
La reforme exige également que les firmes européennes se dotent d'un délégué à la protection des données (une exigence à laquelle les PME seront exemptées dans le cas où le traitement des données n'est pas leur cœur de métier). Par ailleurs, le règlement établi que les entreprises établies hors d'Europe devront se conformer à la réglementation européenne pour pouvoir offrir leurs services dans l'Union. En cas de violations de ces règles, les sanctions pourront atteindre jusqu'à 4% de chiffre d'affaires de l'entreprise. Digital Europe, un groupe de lobbying représentant les intérêts de firmes US comme Google, Apple, IBM ou Microsoft, n'a pas attendu la fin des négociations pour monter au front. Faisant craindre à certains observateurs une édulcoration des règles de la réforme proposée. Mais cela n'a finalement pas été le cas.

Réagissez à cet article

Un décret autorise les captations de données et de conversations Skype en temps réel

Un décret autorise les captations de données et de conversations Skype en temps réel

Dans le calme d'un dimanche précédent le début des vacances de Noël, le gouvernement a publié au Journal officiel un décret autorisant les forces de l'ordre à surveiller toutes les informations apparaissant sur l'ordinateur d'un suspect (de ses conversations Skype à ses sites consultés), dans le cadre de procédures judiciaires.
Permettre à des enquêteurs de capter en temps réel (et à distance) les données informatiques de suspects, c'est possible. Depuis le vote de la LOPPSI de 2011, l'article 706-102-1 du Code de procédure pénale autorise en effet les officiers et agents de police judiciaire à accéder et enregistrer des données « telles qu'elles s'affichent sur un écran » ou telles que l'utilisateur d'un ordinateur « les y introduit par saisie de caractères » – et ce à partir du moment où un juge d'instruction a émis une ordonnance motivée en ce sens, prise après avis du Procureur de la République.
Cette procédure, activable uniquement pour des crimes et délits relativement graves (terrorisme, association de malfaiteurs, meurtre, crime de fausse monnaie, escroquerie ou prêt illicite de main d'œuvre en bande organisée, etc.), a même été élargie suite à l'adoption de la loi anti-terroriste de novembre 2014 aux données « reçues et émises par des périphériques audiovisuels ». L'objectif ? Pouvoir capter aussi les sons, comme ceux d'une conversation Skype par exemple.

Captation de tout ce qui apparaît à l'écran, les conversations Skype, etc.
Avec ce décret entré en vigueur ce lundi 21 décembre 2015, le gouvernement vient de permettre l'application de ces dispositions en autorisant la création de traitements de données à caractère personnel, destinés à recevoir les fameuses informations extirpées par les forces de l'ordre dans ce type de procédures. « Les traitements autorisés par le présent décret permettent de collecter, enregistrer et conserver les données informatiques ainsi captées et de les mettre à la disposition des enquêteurs de la police et de la gendarmerie nationales comme de la douane judiciaire », précise le texte.
Les opérations, bien que placées sous le contrôle du juge, permettront aux services de se pencher sur « l'ensemble des données captées », y compris s'il s'agit de données personnelles sensibles. Toutes les informations enregistrées devront être « conservées dans le traitement jusqu'à la date de clôture des investigations ». À ce moment, poursuit le décret, elles seront « placées sous scellés fermés et effacées ». Une transcription des enregistrements effectuée par les forces de l'ordre devra néanmoins être transmise à l'autorité judiciaire, pour être versée au dossier de la procédure – en vue d'un éventuel procès.
En donnant son avis sur ce qui n'était alors qu'un projet de décret, la Commission nationale de l'informatique et des libertés (CNIL) prévenait l'exécutif que l'utilisation de tels dispositifs de surveillance risquait de conduire à la collecte de « données relatives à d'autres personnes que l'utilisateur [suspecté], telles que, par exemple, l'identité des personnes en relation avec l'utilisateur du système d'information surveillé ».

La gardienne des données personnelles affirmait par ailleurs que le gouvernement ne faisait pas explicitement référence à la mise en œuvre de dispositifs de reconnaissance vocale ni d'analyse comportementale des dynamiques de frappe au clavier (keylogging). « Si de tels mécanismes devaient à l'avenir être mis en œuvre, la commission devra être saisie pour avis sur un projet de décret modificatif prévoyant expressément le recours à de tels dispositifs » mettait-elle en garde.

Un dispositif qui n'était pas encore totalement opérationnel en avril dernier
Tout en regrettant « de ne pas avoir été destinataire de l'ensemble du dossier technique (…), certains éléments n'ayant été communiqués qu'à l'Agence nationale de la sécurité des systèmes d'information (ANSSI) », la CNIL soutenait qu'au moment de rédiger son avis, le dispositif prévu par le ministère de l'Intérieur « ne permet[tait] pas encore la captation de données émises ou reçues par des périphériques audiovisuels ». La délibération de l'autorité administrative indépendante date toutefois du 2 avril 2015, ce qui signifie que les choses ont pu grandement évoluer depuis…
La CNIL ajoutait néanmoins qu'elle prenait acte « que lorsqu'un nouveau dispositif aura été développé dans cette perspective, des informations complémentaires ser[aient] portées à sa connaissance ». Nous n'avons cependant pas réussi à joindre l'institution afin de savoir si elle avait depuis obtenu de nouveaux éléments.

Sur un plan technique, la CNIL expliquait qu'au regard des éléments à sa disposition, « la solution retenue pourra s'adapter à l'environnement applicatif des utilisateurs visés par une enquête (système d'exploitation, applications tierces, etc.). Des tests de fonctionnement seront exécutés afin de s'assurer de la correcte adaptation de l'outil à l'environnement de chaque utilisateur. Une procédure de suppression automatique de l'outil sur les terminaux informatiques visés est prévue. L'architecture de collecte sera en outre pourvue de mesures visant à assurer la sécurité et le cloisonnement des données collectées. »
Rappelons enfin que la récente loi sur le renseignement permet à de nombreux services d'utiliser des dispositifs intrusifs à l'insu des personnes surveillées (à l'image des ISMI catcher), sans toutefois qu'un juge soit cette fois mis dans la boucle…

Réagissez à cet article

Source : *Un décret autorise les captations de données et de conversations Skype en temps réel*

UFC Que Choisir a décidé de

porter plainte contre VTech pour son piratage

UFC Que Choisir a décidé de porter plainte contre VTech pour son piratage

C’est arrivé, la plainte a été lancée par le groupe UFC Que Choisir contre la société VTech pour une affaire de piratage de jouets. Cette plainte pour « faute intolérable » a été déposée auprès du Tribunal de Grande Instance de Versailles.

C’est arrivé, la plainte a été lancée par le groupe UFC Que Choisir contre la société VTech pour une affaire de piratage de jouets.
Cette plainte pour « faute intolérable » a été déposée auprès du Tribunal de Grande Instance de Versailles. En effet, cette association des consommateurs estime que la société VTech met en danger les données de ses clients.

Des serveurs VTech piratés

La plainte déposée par l’association UFC Que Choisir est en rapport avec des serveurs piratés de la société de jouets VTech. En effet pour cette association de consommateurs, les données des clients n’ont pas bénéficier de la meilleure sécurité puisqu’un seul hacker a pu pirater les serveurs. Pas moins de six millions de clients ont vu leurs données totalement violées et notamment sur l’identification de leurs enfants. Sans oublier que VTech ne se serait aperçu de rien jusqu’à que la presse vienne l’interviewer.

Un problème survenu plus précisément aux Etats-Unis

Il faut cependant savoir que ce problème de piratage a d’abord touché les serveurs de la société VTech Américaine. Ce sont les clients des Etats-Unis qui ont été les plus touchés par ce piratage de données, même si la France n’est pas à exclure car elle détient la seconde place. En tout, VTech a sans hésitation confirmé que 868 650 comptes clients ont été piratés en se servant d’applications en ligne mais également de différents services pour accéder aux informations de plus d’un million d’enfants.
Une plainte des plus justifiées car de nombreuses photos d’enfants mais également des adresses et des numéros de téléphone ont été ainsi facilement obtenus par des hackers directement en ligne. VTech va devoir répondre pour cette bavure très grave.

Réagissez à cet article

Source : *Pour cause de piratage UFC Que Choisir a décidé de porter plainte contre VTech*

Bitdefender : Les 5 tendances en cybercriminalité pour 2016

Bitdefender : Les 5 tendances en cybercriminalité pour 2016

Bitdefender publie ses prévisions en matière de sécurité. Dans son rapport, Bitdefender énonce les cinq évolutions notables qui impacteront notre façon de travailler, de jouer et de se sociabiliser sur Internet, au cours de l'année prochaine.

L'année 2016 verra un changement majeur dans la façon dont opèrent les cybercriminels. Le domaine probablement le plus impacté par cette refonte sera celui des PUA, dont l'activité s'est déjà accrue sur des plates-formes telles que Mac OS X et Android.
Suite aux nombreuses fermetures de réseaux de machines zombies et arrestations en 2015, les nouveaux cybercriminels transiteront probablement vers des systèmes de monétisation publicitaire spécifiques aux adwares agressifs, plutôt que de développer de nouvelles souches de malwares. Si pour le moment les botnets constituent toujours une partie importante de l'écosystème de la cybercriminalité, nous assisterons à une augmentation de la sophistication des PUA et des programmes incluant plus de greywares à l'installation.

La publicité sur le Web va également évoluer : étant donné le taux d'adoption ainsi que la popularité des bloqueurs de publicités, les régies publicitaires chercheront à utiliser des mécanismes plus agressifs afin de contourner ces blocages.

Les APT abandonneront le facteur de longévité
Les entreprises et les institutions gouvernementales feront toujours face à des attaques de ce type tout au long de 2016. Cependant, les APT (Advanced Persistent Threats, menaces persistantes avancées) mettront l'accent sur l'obfuscation et la récolte d'informations plutôt que sur la longévité. Les pirates ne s'infiltreront sur le réseau de l'entreprise que quelques jours, voire quelques heures.
Le monde de l'entreprise connaîtra une augmentation des attaques ciblées et des bots fortement obfusqués, avec une courte durée de vie et des mises à jour fréquentes, estime Dragoş Gavriluţ, Chef d'équipe au sein des Laboratoires antimalwares de Bitdefender. La plupart de ces attaques se spécialiseront dans le vol d'informations.
Également, l'évolution latérale de l'infrastructure des fournisseurs de services Cloud ira de pair avec l'avènement d'outils permettant aux pirates de compromettre l'hyperviseur à partir d'une instance virtuelle et de passer d'une machine virtuelle à l'autre. Ce scénario est particulièrement dangereux dans des environnements de « mauvais voisinage », où un tiers mal intentionné serait amené à partager des ressources sur un système physique avec un fournisseur de services ou une entreprise légitimes.

Des malwares mobiles de plus en plus sophistiqués
Du côté des particuliers, les types de malware sous Android sont désormais globalement les mêmes que sous Windows. Alors que les rootkits sont en perte de vitesse sur Windows, ils vont probablement devenir monnaie courante sur Android et iOS, car les deux plates-formes sont de plus en plus complexes et offrent une large surface d'attaque, affirme Sorin Dudea, Chef de l'équipe de recherche antimalwares. De nouveaux malwares mobiles, aux comportements similaires à ceux des vers, ou un réseau botnet mobile géant, sont deux autres possibilités envisagées pour l'année prochaine, selon Viorel Canja, Responsable des Laboratoires antimalwares et antispam chez Bitdefender. Ces attaques pourraient être la conséquence de techniques d'ingénierie sociale ou de l'exploitation de vulnérabilités majeures (telles que Stagefright) sur des plates-formes non patchées.

L'Internet des Objets (IOT) et la vie privée
La façon dont nous gérons notre vie privée va aussi changer durant l'année 2016. En effet, les récents vols de données ont contribué à mettre une quantité importante d'informations personnelles en libre accès sur Internet, rendant ainsi le « doxing » (processus de compilation et d'agrégation des informations numériques sur les individus et leurs identités physiques) beaucoup plus facile pour des tiers.
Les objets connectés vont devenir de plus en plus répandus, donc plus attrayants pour les cybercriminels. Compte tenu de leur cycle de développement très court et des limites matérielles et logicielles inhérentes à ce type d'objet, de nombreuses failles de sécurité seront présentes et exploitables par les cybercriminels ; c'est pourquoi la plupart des objets connectés seront compromis en 2016, ajoute Bogdan Dumitru, Directeur des Technologies chez Bitdefender. Également, les réglementations de surveillance de type « Big Brother », que de plus en plus de pays essaient de mettre en place pour contrecarrer le terrorisme, déclencheront des conflits quant à la souveraineté des données et le contrôle de leur mode de chiffrement.

Les ransomwares deviennent multiplateformes
Les ransomwares sont probablement la menace la plus importante pour les internautes depuis 2014 et resteront l'un des plus importants vecteurs de cybercriminalité en 2016. Alors que certains pirates préfèrent l'approche du chiffrement de fichiers, certaines versions plus novatrices se concentreront sur le développement de « l'extortionware » (malware qui bloque les comptes de services en ligne ou expose les données personnelles aux yeux de tous sur Internet).
Les ransomwares visant Linux vont se complexifier et pourraient tirer parti des vulnérabilités connues dans le noyau du système d'exploitation pour pénétrer plus profondément dans le système de fichiers. Les botnets qui forcent les identifiants de connexion pour les systèmes de gestion de contenu pourraient aussi se développer. Ces identifiants pourraient être ensuite utilisés par les opérateurs de ransomwares visant Linux pour automatiser le chiffrement d'une partie importante d'Internet.
Enfin, les ransomwares chiffrant les fichiers s'étendront probablement aux systèmes sous Mac OS X, corrélant ainsi avec les travaux de Rafael Salema Marques et sa mise en garde illustrée autour de son 'proof of concept' malware nommé Mabouia. En effet, si le principe de conception de Mabouia reste pour le moment privé, il pourrait être créé par des cybercriminels enrichissant alors leurs offres orientées MaaS (Malware-As-A-Service).

Réagissez à cet article

Source : *Bitdefender : Les 5 tendances en cybercriminalité pour 2016 – Global Security Mag Online*

Hello Kitty : les données de

millions de fans compromises

Hello Kitty : les données de millions de fans compromises

Les données personnelles de millions fans d'Hello Kitty étaient facilement accessibles. C'est un chercheur en sécurité Chris Vickery qui a donné l'alerte. Il a découvert une base contenant les informations de plus de trois millions d'utilisateurs, tels que nom, prénom, pays d'origine, emails, mots de passe. La société japonaise Sanrio qui gère la licence Hello Kitty assure avoir comblé la faille de vulnérabilité.

Et pour l'heure, l'entreprise assure aussi n'avoir détecté aucun vol de données. Une mauvaise configuration serait à l'origine du problème.
A quelques jours de Noël, la nouvelle passe mal. Le mois dernier déjà, c'est le fabricant de jouets hongkongais VTech qui était sur la sellette après le piratage de centaines de milliers de comptes et de profils d'enfants.

Réagissez à cet article

Source : *Hello Kitty : les données de millions de fans compromises | euronews, monde*

Les entreprises doivent prendre au sérieux la protection des données

Les entreprises doivent prendre au sérieux la protection des données

---

L'intelligence économique est devenue un mode de gestion (Le management est la mise en ?uvre des moyens humains et matériels d'une entreprise pour (…)) et de gouvernance de l'entreprise. Cet ouvrage réfléchit sur la démarche que le chef d'entreprise peut entreprendre pour éclairer ses décisions, garder sa marge de manoeuvre de compétitivité et toutes ses possibilités de développement afin de sécuriser sa pérennité.

Traitement de l'information et renseignements

Un renseignement utile peut être obtenu de façon proactive, active, ou réactive.

Le cycle de renseignement pour l'entreprise doit s'intégrer au processus de veille stratégique sur les différents volets de l'intelligence économique : veille technologique, veille d'image, veille concurrentielle, etc.

L'intelligence économique distingue trois niveaux d'information utile au renseignement :

image: http://www.atlantico.fr/sites/atlantico.fr/files/u65387/2015/12/capture_2_0.jpg

L'intelligence économique ne cherche pas à obtenir l'information noire. Elle se limite à l'information que l'on peut obtenir par des moyens légaux (ex : pour se protéger des problèmes de réputation, d'escroquerie, de fraude, de cybercriminalité, de propriété intellectuelle, de savoir-faire, de brevets, etc.).

Il s'agit surtout de formaliser de façon pragmatique, ou de rendre systématique, une démarche proactive de veille dans ce domaine, notamment pour l'obtention de l'information « grise ».

Les PME sont souvent très en retrait sur la construction du savoir (ex : suivi des avancées des concurrents, organisation de la veille juridique, réglementaire, lobbying, etc.).

Sécurité et protection de l'information

Trop peu d'entreprises prennent au sérieux la protection des données. Il devient impératif de disposer d'un solide processus de sauvegarde, de prévention, d'action, et de réaction aux pannes et aux attaques informatiques. Notons ici que certaines entreprises sensibles aux problématiques de reprise après incident commencent à considérer les prestations d'externalisation applicatives (Cloud computing ou autres solutions) pour optimiser le niveau de sécurité des données.

Quantité et gouvernance des données

Les données sont la base de l'information, et comme le disent souvent les anglo-saxons: « data is the oil of the 21st century ». Savoir chercher et collecter l'information, la traiter et la diffuser (tout en protégeant la part de données sensibles qui doivent être protégées), constitue une tâche prioritaire de tous les acteurs économiques, et la définition même de l'intelligence économique.

image: http://www.atlantico.fr/sites/atlantico.fr/files/u65387/2015/12/capture_3_0.jpg

Le pouvoir c'est l'information, mais à condition qu'elle soit de qualité …

La direction et les organes sociaux doivent s'appuyer sur des informations de qualité (fiables, précises, actualisées)

Read more at http://www.atlantico.fr/decryptage/entreprises-doivent-prendre-au-serieux-protection-donnees-gouvernance-et-intelligence-economique-en-pme-georges-nurdin-daniel-2494228.html##Vrl3qqLdiB14upbK.99

Réagissez à cet article

Source : *Marketing/ Les entreprises doivent prendre au sérieux la protection des données*

Vaincre les attaques DoS/DDoS en temps réel

Vaincre les attaques DoS/DDoS en temps réel

La vulnérabilité des serveurs DNS des fournisseurs de services vis-à-vis des attaques DoS/DDoS est bien réelle et s'intensifie à un rythme effréné, mettant ainsi en péril l'expérience utilisateur des clients ainsi que la réputation des fournisseurs de services.

Les techniques actuelles visent à arrêter les attaques en dotant le site du fournisseur de matériel supplémentaire ou en identifiant le coupable caché dans le logiciel malveillant sur le site du client. Cependant, ces deux méthodes sont onéreuses et ne permettent de résoudre le problème que partiellement. La nouvelle approche consiste à intégrer la protection contre les attaques DoS/DDoS directement dans un serveur cache DNS à haute fiabilité et à contrecarrer l'attaque en temps réel au moment où elle pénètre dans l'infrastructure, la désamorçant avant même qu'elle n'affecte les performances ou le service.
Lire la suite…

Réagissez à cet article

Source : *InfoBlox*

La SACEM tente d’étendre ses taxes au Cloud

La SACEM tente d’étendre ses taxes au Cloud

L'ennui avec le progrès, c'est qu'il se fiche comme d'une guigne des prés carrés, des rentes de situations et des petits arrangements entre amis. Parfois, ce progrès provoque l'effondrement plus ou moins rapide de juteuses pensions qu'on croyait établies pour toujours. C'est exactement ce à quoi est confronté la SACEM.

La SACEM, c'est cette vénérable institution de ponctions culturelles qui utilisait jusqu'à présent le bras armé de l'État pour faire valoir des droits construits de toute pièce il y a un siècle et demi et qui arrivait encore assez facilement à prélever sa dime… Jusqu'à l'avènement du numérique : rapidement, la facilité de copie est devenue telle qu'il a rapidement été impossible de les tracer.

Parallèlement, l'effondrement des ventes de galettes de vinyle ou de polyacrylates a rendu la collecte des fameux droits beaucoup plus complexe. Moyennant une bonne couche de lobbying, on se souvient que les sociétés culturelles concernées (comprenant la SACEM mais aussi les majors musicales ou du cinéma) avaient réussi à pousser dans les tuyaux législatifs français des lois compensant assez largement ces changements drastiques de modes de revenus par une taxe française sur les supports numériques vierges, depuis les iPods jusqu'aux cartes mémoires en passant par les disques durs.

Cette taxe permit, on s'en doute, de largement renflouer les comptes de ces associations lucratives, et de placer presque instantanément les supports numériques français parmi les plus chers du monde. Commander un disque dur, un iPod ou une carte mémoire de l'autre côté de la frontière est rapidement devenu un sport national tant le différentiel devenait grotesque. Eh oui : la société civile s'adapte bien plus vite que les lois.

Quant aux progrès technologiques, ils continuent à un rythme tel qu'à peine les ponctions sur les supports numériques actés, ces derniers devinrent quasiment caduques. Rapidement, le consommateur déporte ses données dans le Cloud, et n'utilise plus, directement, de support numérique.
Autrement dit, le support numérique du consommateur est minimal, et ne comporte que la petite quantité de données qu'il écoute au moment où il veut. L'ensemble de ses bibliothèques numériques (films, musiques, vidéos, photos) est de plus en plus déporté dans un nuage numérique fourni par des entreprises spécialisées, allant de Google (GoogleDrive) à Microsoft (SkyDrive) en passant bien sûr par Apple (iCloud), Dropbox et autres solutions plus ou moins intégrées avec les outils numériques du moment.

Pour la SACEM, c'est une nouvelle catastrophe.
Comme le relate un récent article de NextInpact, David El Sayegh, le secrétaire général de la SACEM, a ainsi expliqué avec quelques trémolos dans la voix lors d'une table ronde organisée par la Commission de la Culture au Sénat toute la difficulté de la situation que rencontre sa société :
« on a décalage entre la législation française qui explique que la copie privée ne peut être invoquée que pour les particuliers qui ont la garde matérielle des produits et l'évolution technologique qui permet de réaliser des copies privées quand bien même vous n'avez pas la garde technique de ces matériels. »

Eh oui. *« si vous perdez votre iPad ou votre portable, c'est dommage de perdre toute votre discothèque »*, mais comme tout est dans ce fameux Cloud, pouf, vous pouvez tout récupérer.
Magie de la technologie moderne ? Peut-être, mais en tout cas, il y aurait comme des copies privées dans ce cloud que ce ne serait pas étonnant, insiste clairement notre bon secrétaire général. Ce qui voudrait dire (miam, miam et slurp) que ces copies seraient sujettes à redevance, pardi ! Et donc, « le Sénat, dans sa sagesse, doit absolument légiférer », sinon, c'est évidemment le début de la fin, la fermeture du robinet, et l'apocalypse de la création musicale, garantie sur facture.

Et c'est bien d'assujettir le Cloud à cette taxe de copie privée qu'il est question ici, puisque le brave secrétaire en appelle à l'amendement Rogemont qui proposait exactement ça : soit on ponctionnera le service en ligne, soit les espaces de stockages classiques, soit les offres de streaming en temps différé (typiquement, les « magnétoscopes » en ligne, proposés par les FAI). Décidément, rien n'échappe à la rage taxatoire des uns et des autres.
Il ne reste plus qu'à pondre une bonne petite loi, et l'affaire sera dans le sac : la SACEM, sauvée d'une pénurie inopinée de fonds, retrouvera vigueur et couleurs d'antan et pourra repartir à l'assaut des portefeuilles bien garnis des consommateurs.
Mais voilà : c'est bien joli, toutes ces décisions finement élaborées et frappées au coin du bon sens bien compris de la nomenklatura française, cependant, si on s'éloigne des intentions, toujours extrêmement claires et dont les effets sont tous parfaitement connus et même planifiés, et si on s'attarde un peu sur les résultats, toujours plus incertains, on découvre comme un petit écart.
Prenez par exemple notre magnifique HADOPI, que le monde, ébahi, ne comprend pas, ne nous envie pas et qui déclenche même souvent l'hilarité, en France comme ailleurs. Il en aura fallu, des aventures amusantes, pour en arriver à sa création. Il en aura fallu, du « pare-feu OpenOffice » et de fines manœuvres du Capitaine Anéfé pour aboutir à un appendice boursouflé incapable de faire, même vaguement, ce pourquoi il fut créé en premier lieu…

Or, au constat déjà catastrophique de la nullité de l'institution en terme de lutte contre le piratage, on doit maintenant ajouter un effet clairement négatif sur le cinéma français : on apprend en effet au détour d'une enquête de l'INSEE que la lutte contre le piratage menée par la Hototorité a « clairement favorisé » le cinéma américain au détriment des films français.

Apparemment, d'après l'étude, « l'introduction de la loi Hadopi est associée à une augmentation de la part de marché des films américains de 9%, mais sans augmentation de la demande totale pour les films en salle ». Pour HADOPI, c'est carton plein : les entrées en salle n'ont pas augmenté, mais les films américains ont été plus vus que les français, ce qui laisse furieusement à penser que les films français sont plus piratés. De là à conclure hardiment que leur valeur intrinsèque ne justifie pas le déplacement et l'achat d'une place en salle, et que le risque est moins grand de les pirater que pour les productions américaines, il n'y a qu'un tout petit pas facile à franchir.
Bref, vous avez bien lu : non seulement, la HADOPI ne parvient pas à endiguer, même un peu, le piratage qu'elle prétend combattre, non seulement cette création ubuesque nous coûte 8,5 millions d'euros par an (plus encore que les années précédentes suite à l'élargissement de son budget, sans doute pour la récompenser de ses performances), mais de surcroît, elle parvient même à saboter le marché sur lequel elle opère. C'est, on doit l'admettre, un échec de proportion épique.

À présent, il devient difficile de s'empêcher de mettre en regard ce résultat catastrophique de la HADOPI, instance d'ailleurs issue des belles législations de nos assemblées et de la fameuse « sagesse » à laquelle se réfère le secrétaire général de la SACEM, et ce que ce dernier propose de faire à nouveau concernant la copie privée et son avatar sur les clouds.
L'expérience permet d'éviter de répéter sans arrêt les mêmes bêtises. Inversement, Einstein notait judicieusement que la folie consistait à refaire toujours la même chose en espérant obtenir des résultats différents.
De l'expérience ou de la folie, que croyez-vous donc que notre législateur va choisir ?

Réagissez à cet article

Source : *La SACEM tente d’étendre ses taxes au Cloud | Contrepoints*

Juniper : une faille de sécurité permettait de surveiller le trafic VPN

	**Une faille de sécurité permettait de surveiller le trafic VPN**

La firme indique avoir découvert des portes dérobées dans ScreenOS, présent dans ses pare feux et services VPN. Par mesure de sécurité, Juniper a mis à jour son système d'exploitation.

Juniper indique qu'un morceau de code informatique non-autorisé était présent dans son système d'exploitation maison. Ce dernier est utilisé pour une partie de ses solutions de sécurité tels que les firewall et les services de VPN. La société a donc émis un bulletin de sécurité au sujet de ce code-espion.
Ce dernier aurait été initialement publié en 2008, de quoi laisser le temps aux éventuels attaquants d'utiliser cette porte dérobée pour utiliser des informations transitant par le biais de ces équipements. Un correctif est donc actuellement déployé par Juniper, en particulier pour les équipements de la gamme NetScreen.
Malgré ces mises à jour de sécurité, Juniper n'a pas identifié la provenance de ce code aux effets malfaisants. Si la thèse des services de renseignement n'est pas à exclure, il pourrait également s'agir de hackers ou même de développeurs présents en interne (voire des sous-traitants).

La porte dérobée doit en principe permettre à un attaquant d'accéder à distance en mode administration à un équipement sous ScreenOS. Quant à la seconde vulnérabilité mise au jour par Juniper, elle autorise un pirate à surveiller un trafic au sein d'un VPN.
Malgré l'ampleur du problème, la direction se veut rassurante. Elle précise : « pour le moment, aucun rapport n'indique que ces vulnérabilités ont été exploitées. Nous recommandons vivement aux clients de mettre à jour leurs systèmes et d'appliquer les versions corrigées sans délai ».

Réagissez à cet article

Source : *Juniper : une faille de sécurité permettait de surveiller le trafic VPN*