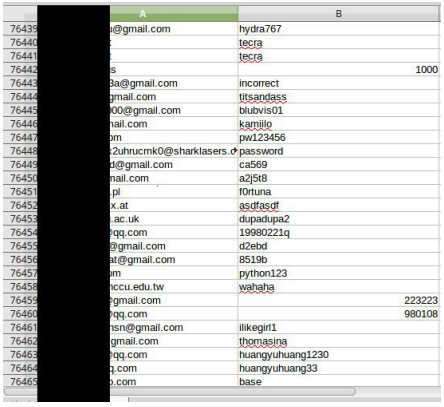
Un site Internet pour adultes piraté. Les comptes d’accès bradés sur le BlackMarket

Un site Internet pour adultes piraté. Les comptes d’accès bradés sur le BlackMarket

Un internaute a tenté de revendre les données de 270 000 amateurs de sites pornographiques dans le blackmarket. Le business du Porn Account pour les nuls !

Vous avez peut-être entendu à la radio et lu dans la presse généraliste ce piratage de données ayant visé 270 000 amateurs de sites pornographiques. Un piratage qui a débuté via l'attaque par injection SQL de plusieurs sites pour adultes appartenant au groupe Paper Street Media.
Le pirate a expliqué avoir contacté l'entreprise pour « discuter ». Soyons clair, il a tenté de leur soutirer de l'argent en proposant la faille qui lui a permis d'extraire les informations des clients (IP, mail, mots de passe…).
Paper Street Media n'a pas répondu dans le sens de l'internaute. Bilan, l'adolescent a mis en vente, dans le blackmarket, la base de données volée pour 360 euros. Pourquoi revendre les données dans le BM ? Toutsimplement pour que les professionnels du porn account puissent sauter sur l'occasion.
Dans cette même boutique qui aurait servi au pirate à revendre cette base de données [je n'ai pas retrouvé le vendeur], d'autres « commerçants » proposent des accès « piratés » aux sites interdit au – de 18 ans de Paper StreetMedia pour 9 $. Je vous laisse faire l'addition. Nous sommes très très loin des 360 euros réclamés ! « **Je peux me faire entre 300 et 500 dollars par semaine** » m'indique un de ces vendeurs de Porn Account croisé dans une boutique spécialisée.



	A	B
76439	[redacted]@gmail.com	hydra767
76440	[redacted]	tecra
76441	[redacted]	tecra
76442	[redacted]s	1000
76443	[redacted]3a@gmail.com	incorrect
76444	[redacted]gmail.com	titsandass
76445	[redacted]00@gmail.com	blubvis01
76446	[redacted]ail.com	kamiilo
76447	[redacted]m	pw123456
76448	[redacted]2uhrucmk0@sharklasers.c	password
76449	[redacted]d@gmail.com	ca569
76450	[redacted]ail.com	a2j5t8
76451	[redacted].pl	f0rtuna
76452	[redacted]x.at	asdfasdf
76453	[redacted].ac.uk	dupadupa2
76454	[redacted]qq.com	19980221q
76455	[redacted]@gmail.com	d2ebd
76456	[redacted]at@gmail.com	8519b
76457	[redacted]m	python123
76458	[redacted]ccu.edu.tw	wahaha
76459	[redacted]gmail.com	223223
76460	[redacted]qq.com	980108
76461	[redacted]nsn@gmail.com	ilikegirl1
76462	[redacted]gmail.com	thomasina
76463	[redacted]qq.com	huangyuhuang1230
76464	[redacted]q.com	huangyuhuang33
76465	[redacted]o.com	base

Un pirate russe revend des milliers de comptes du site Naughty America.
A noter que j'ai pu consulter [ci-dessus] un document diffusé par un autre pirate informatique. Ce dernier, il est russe, a mis la main sur 150 000 comptes clients du site pornographique Naughty America. Un injection SQL, une backdoor (shell) dans le serveur et les comptes clients ont fini dans les mains du pirate.

Pendant ce temps…
… le groupe hôtelier Trump est de nouveau piraté. Des logiciels d'espionnage ont été retrouvés dans les ordinateurs des hôtels Trump situés à New York, Toronto et Honolulu. Même type d'attaque vécue en juillet 2015. Cela donne une idée de la gestion de la sécurité informatique de ce groupe. Les pirates visaient les identités et les données bancaires.
En ce qui concerne les numéros de CB, pas besoin d'être intelligent pour comprendre l'intérêt. Achats de produits dématérialisés qui seront revendus moitié prix [blanchir l'argent détourné]… En ce qui concerne les informations dédiées aux identités : fraude bancaire [ouverture de compte], usurpation d'identité, … [Lire la suite]

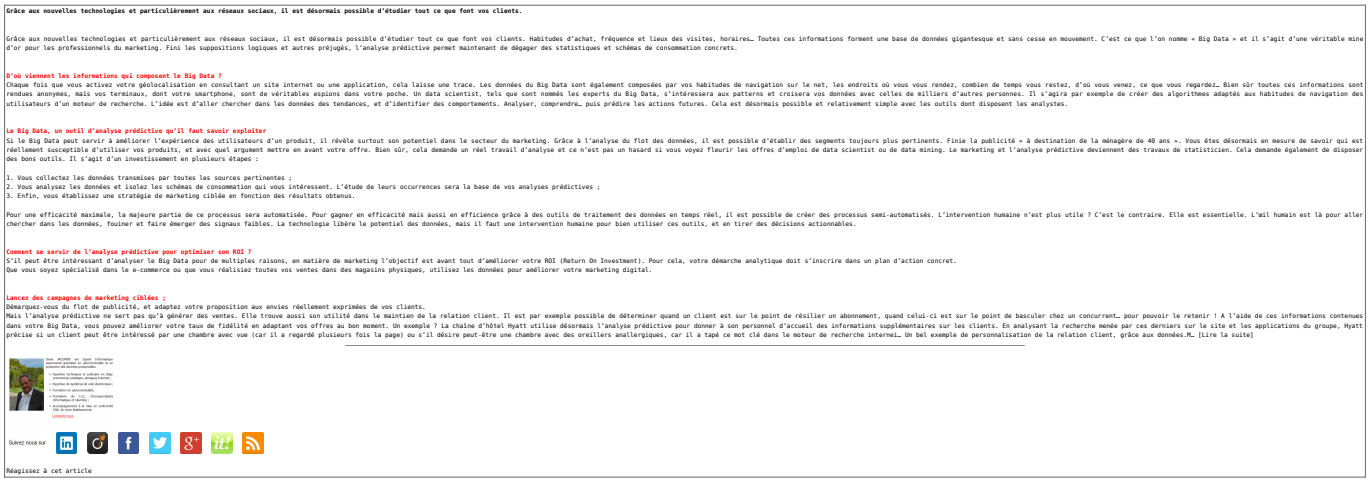
Réagissez à cet article

Source : *Porn Account : 270000 amateurs de pornos piratés – Data Security BreachData Security Breach*

Mieux connaître le

consommateur avec ses données

	**Mieux connaître le consommateur avec l'analyse prédictive et le Big Data**



Grâce aux nouvelles technologies et particulièrement aux réseaux sociaux, il est désormais possible d'étudier tout ce que font vos clients.

Grâce aux nouvelles technologies et particulièrement aux réseaux sociaux, il est désormais possible d'étudier tout ce que font vos clients. Habitudes d'achat, fréquence et lieux des visites, horaires… Toutes ces informations forment une base de données gigantesque et sans cesse en mouvement. C'est ce que l'on nomme « Big Data » et il s'agit d'une véritable mine d'or pour les professionnels du marketing. Fini les suppositions logiques et autres préjugés, l'analyse prédictive permet maintenant de dégager des statistiques et schémas de consommation concrets.

D'où viennent les informations qui composent le Big Data ?

Chaque fois que vous activez votre géolocalisation en consultant un site internet ou une application, cela laisse une trace. Les données du Big Data sont également composées par vos habitudes de navigation sur le net, les endroits où vous vous rendez, combien de temps vous restez, d'où vous venez, ce que vous regardez… Bien sûr toutes ces informations sont rendues anonymes, mais vos terminaux, dont votre smartphone, sont de véritables espions dans votre poche. Un data scientist, tels que sont nommés les experts du Big Data, s'intéressera aux patterns et croisera vos données avec celles de milliers d'autres personnes. Il s'agira par exemple de créer des algorithmes adaptés aux habitudes de navigation des utilisateurs d'un moteur de recherche. L'idée est d'aller chercher dans les données des tendances, et d'identifier des comportements. Analyser, comprendre… puis prédire les actions futures. Cela est désormais possible et relativement simple avec les outils dont disposent les analystes.

Le Big Data, un outil d'analyse prédictive qu'il faut savoir exploiter

Si le Big Data peut servir à améliorer l'expérience des utilisateurs d'un produit, il révèle surtout son potentiel dans le secteur du marketing. Grâce à l'analyse du flot des données, il est possible d'établir des segments toujours plus pertinents. Finie la publicité « à destination de la ménagère de 40 ans ». Vous êtes désormais en mesure de savoir qui est réellement susceptible d'utiliser vos produits, et avec quel argument mettre en avant votre offre. Bien sûr, cela demande un réel travail d'analyse et ce n'est pas un hasard si vous voyez fleurir les offres d'emploi de data scientist ou de data mining. Le marketing et l'analyse prédictive deviennent des travaux de statisticien. Cela demande également de disposer des bons outils. Il s'agit d'un investissement en plusieurs étapes :

1. Vous collectez les données transmises par toutes les sources pertinentes ;
2. Vous analysez les données et isolez les schémas de consommation qui vous intéressent. L'étude de leurs occurrences sera la base de vos analyses prédictives ;
3. Enfin, vous établissez une stratégie de marketing ciblée en fonction des résultats obtenus.

Pour une efficacité maximale, la majeure partie de ce processus sera automatisée. Pour gagner en efficacité mais aussi en efficience grâce à des outils de traitement des données en temps réel, il est possible de créer des processus semi-automatisés. L'intervention humaine n'est plus utile ? C'est le contraire. Elle est essentielle. L'œil humain est là pour aller chercher dans les données, fouiner et faire émerger des signaux faibles. La technologie libère le potentiel des données, mais il faut une intervention humaine pour bien utiliser ces outils, et en tirer des décisions actionnables.

Comment se servir de l'analyse prédictive pour optimiser son ROI ?

S'il peut être intéressant d'analyser le Big Data pour de multiples raisons, en matière de marketing l'objectif est avant tout d'améliorer votre ROI (Return On Investment). Pour cela, votre démarche analytique doit s'inscrire dans un plan d'action concret.
Que vous soyez spécialisé dans le e-commerce ou que vous réalisiez toutes vos ventes dans des magasins physiques, utilisez les données pour améliorer votre marketing digital.

Lancez des campagnes de marketing ciblées ;

Démarquez-vous du flot de publicité, et adaptez votre proposition aux envies réellement exprimées de vos clients.
Mais l'analyse prédictive ne sert pas qu'à générer des ventes. Elle trouve aussi son utilité dans le maintien de la relation client. Il est par exemple possible de déterminer quand un client est sur le point de résilier un abonnement, quand celui-ci est sur le point de basculer chez un concurrent… pour pouvoir le retenir ! A l'aide de ces informations contenues dans votre Big Data, vous pouvez améliorer votre taux de fidélité en adaptant vos offres au bon moment. Un exemple ? La chaîne d'hôtel Hyatt utilise désormais l'analyse prédictive pour donner à son personnel d'accueil des informations supplémentaires sur les clients. En analysant la recherche menée par ces derniers sur le site et les applications du groupe, Hyatt précise si un client peut être intéressé par une chambre avec vue (car il a regardé plusieurs fois la page) ou s'il désire peut-être une chambre avec des oreillers anallergiques, car il a tapé ce mot clé dans le moteur de recherche interne… Un bel exemple de personnalisation de la relation client, grâce aux données.M… [Lire la suite]

Suivez nous sur

Réagissez à cet article

Source : *Analyse prédictive et Big Data : mieux connaître le consommateur avec ses données*

Quelques conseils pour se protéger des pirates informatique

Un élu se fait voler 3000€ via le piratage de sa carte bancaire. Ne soyez plus une victime, cela n'arrive pas qu'aux autres.

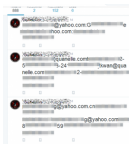
Un élu de Vanne, en Bretagne, vient d'expliquer sa mésaventure bancaire à la presse locale. Ses données bancaires ont été subtilisées. Le pirate a revendu les informations dans le blackmarket. Bilan, des achats de places de cinéma, une location de voiture en région parisienne, un voyage en Thaïlande, des billets d'avion ont été acquis avec la carte bancaire piratée et clonée. Comment l'élu a-t-il pu être ainsi piégé ? Plusieurs cas ont possibles pour le piratage de CB.

D'abord, la fuite de données via un site de vente en ligne.
Même si de plus en plus de sécurité sont mises en place entre le client et la boutique, le fameux HTTPS, que deviennent les données ? Je rencontre encore de très nombreux cas de vols de bases de données avec des informations privées et sensibles (dont les données de la CB) dans des fichiers dérobés sur des sites piratés. Un HTTPS sur le site ? La belle affaire. Le S indique que votre connexion est sécurisée (chiffrée) entre votre ordinateur et la boutique. Parfait pour ne pas se faire intercepter les données via une connexion un peu trop légère (wifi public…). Mais ce HTTPS ne vous sauvera pas si la base de données, ou un malveillant interne à la boutique, met la main sur la base de données. Un exemple que j'ai rencontré dernièrement en est le parfait aperçu. Depuis une dizaine de jours, sur Twitter, un bot pirate recrache les informations des comptes Paypal de centaines de personnes que le pirate trouve sur des sites web.

Vient ensuite le skimming, le piratage de CB par clonage via un système physique collé sur un distributeur de billets automatique, une pompe à essence, un parcmètre…
Le matériel copie la bande magnétique. Une caméra miniature, ou un faux clavier posé sur le vrai, permet de récupérer le mot de passe. Je vous expliquais, il y a peu, comment la police italienne, avec l'aide d'Europol, avait mis fin aux agissements d'un gang de pirates de cartes bancaires qui sévissait dans toute l'Europe.

Chez les commerçants, le remplacement du boitier de paiement par un pirate.
Copie directe, sans que la boutique ne puisse s'en rendre compte en temps réel. Regardez toujours sous ce lecteur de CB si un autocollant protège le matériel.
Le phishing, la copie du site Internet de votre banque, par exemple. Toujours, malheureusement, aussi efficace pour ceux qui ne prennent pas le temps de regarder correctement l'url caché dans le courriel reçu.

Pour finir avec le piratage de CB, la simple copie mentale, par une personne ayant eu accès, même quelques secondes à votre bout de plastique.
Ne perdez JAMAIS de vue votre carte bancaire. C'est le lecteur de CB qui vient à votre moyen de paiement, pas le contraire.
Comme vous avez pu le voir, le piratage de CB peut prendre de multiples formes. Je ne vous relate que les plus courantes. Un dernier point important ! Arrêtez de vous contenter du « Cela n'arrive qu'aux autres » ou, plus grave encore à mon sens « Fort heureusement, j'ai une assurance ! » N'hésitez jamais à déposer plainte. Votre identité numérique est définitivement perdue. Le pirate ne se contentera pas que de votre carte bancaire !



Exemples de piratage de CB et de données

Voici deux exemples, sur 83 vécus cette semaine, visant des données volées à des clients Français.
Le site Internet Demain J'arrête, dédié aux cigarettes électroniques. Le pirate, après avoir fait ses « courses » dans la base de données, a diffusé son forfait sur la toile. Même sanction pour le cas de la boutique en ligne Mayline, un spécialiste de l'ameublement. Noms, adresses postales, mots de passe (hashé/chiffré en MD5), logins, mails… Plusieurs buts dans cette malveillance : effacer ses traces (surtout si des centaines de zozos 2.0 se jettent sur les informations, NDR) ; montrer sa puissance (le 1/4 d'heure Warholien, NDR).
Le problème dans ce genre de vol de données, les identités numériques pillées ne peuvent plus être maîtrisées par les légitimes propriétaires. Mails, adresses postales, téléphones, pseudos, mots de passe. Autant de contenus pouvant être exploités dans des dizaines d'arnaques. Un numéro de téléphone portable ? Diffusion de spams, fraudes aux appels surtaxés, de tentatives d'infiltrations via un MMS piégé… Une adresse physique ? Elles peuvent se vendre quelques dizaine d'euros dans le blackmarket pour être transformées en drop box, des boites aux lettres pirates pour recevoir du matériel volé pendant l'absence des propriétaires. Un mot de passe non chiffré ? Pas besoin de vous faire un dessin sur son utilisation (Espionnage, usurpation…) Bref, les pirates ne cherchent pas que les données bancaires. Les datas qu'amassent les entreprises sur le dos des Internautes sont aussi de véritables mines d'or. !

Mon mot de passe est chiffré ?
Je vais vous expliquer pourquoi avoir un mot de passe fort est une véritable obligation sur la toile, aujourd'hui. L'identifiant de connexion est hashé/chiffré au format MD5 ? Prenons un mot de passe des dizaines de fois rencontré : Football. Dans une base de données sans MD5, le pirate lira le password en clair. Une protection MD5 est installée ? Football se transforme en 37b4e2d82900d5e94b8da524fbeb33c0. Le pirate, au premier abord, ne peut rien en faire. Sauf que je vais vous démontrer qu'un mot de passe fort, avec majuscules, minuscules, chiffres, signes de ponctuations, est loin d'être négligeable. Notre pirate a donc en main 37b4e2d82900d5e94b8da524fbeb33c0. Rendez-vous sur le site http://md5cracker.org est rentré ce mystérieux code MD5. En moins d'une seconde, le « crack » va vous proposer 6 bonnes réponses sur 11 sites proposant de pirater un mot de passe au format MD5. Préférez donc un mot de passe de type J'a1m3_le_F0ot_B4L! qu'un simple football. A noter que si votre mot de passe est « cracké », il se retrouvera obligatoirement dans l'une des nombreuses bases de données regroupant les hash MD5 proposées sur la toile.
Pour finir, un mot de passe, un login et un mail d'identification ne s'utilise que pour un service utilisé. Il faut en changer, au risque d'ouvrir grandes les portes aux intrus… [Lire la suite]

- Denis JACOPINI est Expert Informatique assermenté spécialisé en cybercriminalité et en protection des données personnelles
- Expertises techniques et judiciaires
- Expertises de systèmes de vote électronique
- Formations en cybercriminalité
- Formation de C.I.L. (Correspondants Informatique et Libertés)
- Accompagnement à la mise en conformité CNIL de votre établissement

Contactez-nous

Réagissez à cet article

Source : *Piratage de CB : Fort heureusement, j'ai une assurance ! – ZATAZ*

Un piratage sur Tor par le FBI prive les victimes d'une justice

Un piratage sur Tor par le FBI prive les victimes d'une justice

La lutte contre la pédocriminalité est une absolue nécessité, qui exige une absolue rigueur. Un juge américain a dû invalider un mandat utilisé par le FBI pour pirater les ordinateurs de membres d'un site pédopornographique hébergé derrière le réseau Tor, privant les victimes et leurs proches de la possibilité d'un procès.

C'est un coup très dur pour le FBI, mais surtout pour les familles des victimes. Dans un jugement prononcé mercredi, un tribunal américain situé au Massachusetts a invalidé le mandat que la police fédérale avait utilisé pour maintenir un site pédopornographique en ligne et procéder au piratage des ordinateurs de plus d'un millier de ses membres. Le site en question, Playpen, n'était accessible qu'à travers le célèbre réseau d'anonymisation Tor, qui masquait l'adresse IP véritable des visiteurs, rendant très difficile leur identification et leur poursuite.
C'est sur un argument purement juridictionnel que s'est appuyé le magistrat pour dénoncer l'illégalité du mandat employé par le FBI. Selon le code de procédure pénal américain, les magistrats n'ont pas l'autorité suffisante pour émettre des mandats situés en dehors de leur compétence géographique. C'est pourtant ce qu'il s'est produit dans au moins l'un des cas de l'affaire Playpen.
Le site The Intercept, qui se fait l'écho des conclusions de la décision, explique en effet que le mandat a été émis au départ par un juge se trouvant en Virginie. Or, l'un des suspects qui a été attrapé par le FBI dans le cadre de l'enquête vit dans le Massachusetts. Les éléments contre lui – qui est à l'origine de la plainte visant à obtenir l'invalidation du mandat – ne peuvent donc pas être retenus comme preuves, car ils ont été obtenus sans mandat valable.
Le verdict rendu cette semaine risque fort de réduire à néant toute la stratégie du FBI pour faire fermer Playpen et mettre la main sur ses visiteurs américains. La décision est tout à fait susceptible de faire tache d'huile. D'autres accusés pourraient très bien se mettre à attaquer la légalité du mandat sur le même argument juridictionnel, ce qui ferait tomber des preuves à charge contre eux.
Christopher Soghoian, membre de l'American Civil Liberties Union, une association de protection des droits et libertés aux États-Unis, indique que le piratage du site pédopornographique a permis de constituer 1 300 dossiers en attente. À supposer que tous vivent aux USA, combien se trouvent dans des États qui sont en dehors de la compétence géographique de la Virginie ? Sans doute une grande majorité.

UNE FAILLE LÉGISLATIVE BIENTÔT CORRIGÉE ?
Cette règle de la procédure pénale pourrait toutefois disparaître. Le département de la justice américain souhaite lever cette barrière afin que les juges puissent délivrer des mandats pour des recherches à distance sur des ordinateurs qui sont situés en dehors de leur juridiction ou lorsque leur emplacement géographique est inconnu.
Selon The Intercept, le changement législatif a de bonnes chances de passer et le feu vert de la Cour Suprême est très probable – il devrait survenir très bientôt – malgré les protestations des organisations de défense des libertés individuelles et de quelques sociétés, comme Google. Le Congrès aura ensuite six mois pour l'approuver ou la rejeter, sinon la modification entrera en vigueur.

L'AFFAIRE PLAYPEN ET LE PIRATAGE DU FBI
L'affaire Playpen remonte début 2015, quand le FBI parvient à prendre le contrôle des serveurs du site. Au lieu de le fermer tout de suite, la police choisit une autre approche, celle du honeypot : le site reste actif pendant environ deux semaines, sur les serveurs du FBI, afin de savoir qui se connecte sur Playpen. Tactique qui provoquera au passage un déluge de critiques sur le FBI.
C'est au cours de cette période que le FBI a procédé à la contamination des ordinateurs des visiteurs, afin de collecter des informations sur eux, comme leur véritable adresse IP, qui est habituellement masquée avec le réseau d'anonymisation. En effet, la connexion transite par une succession de relais afin de camoufler la géolocalisation du PC. C'est avec ces données que le FBI s'est ensuite adressé aux opérateurs pour obtenir l'identité des internautes – en tout cas ceux aux USA… [Lire la suite]

Réagissez à cet article

Source : *Pédopornographie : quand un piratage par le FBI sur Tor prive les victimes d'une justice*

ZATAZ 93 millions d’électeurs Mexicains accessibles sur la toile – ZATAZ

	93 millions d’électeurs Mexicains accessibles sur la toile

Accessibles sur la toile ! Cela n'arrive pas qu'aux autres, la preuve, une fois de plus. Une base de données mal configurée a permis d'accéder à 93,4 millions de données d'électeurs mexicains. Une BDD sauvegardée… aux USA !

Dans la série, le #Fail du jour, voici venir le Mexique et des données accessibles sur la toile ! Il y a peu, une base de données énorme a été volée à la Turquie, 49 millions de dossiers, et d'une seconde, de 55 millions d'informations d'électeurs Philippins.
Aujourd'hui, traversons l'Atlantique et allons regarder du côté des électeurs Mexicains. Plus de 93,4 millions de citoyens mexicains ont eu leurs modalités d'inscription sur les listes électorales diffusées sur la toile via une base de données mal configurée. C'est Chris Vickery, chercheur en sécurité informatique qui a découvert la chose via l'outil Shodan et le bug de configuration visant le gestionnaire de base de données MongoDB.
Plus étonnant, la base de données qui appartient à l'Instituto Nacional Electoral (INE), une BDD de 132 Go, étaient sauvegardées aux USA, chez Amazon.
Parmi les informations accessibles détectées par Chris Vickery : identités, filiation familiale, enfants, métier, adresse postale, numéro d'identité, numéro d'électeur…

Accessibles sur la toile
Bref, à force de nous vendre le cloud comme notre nouvel ami (écologique, peu couteux, friendly), c'est surtout nous faire oublier que le cloud, c'est le diable en 2.0.
Cette année, La Grèce, Israël, les Etats-Unis, les Philippines et la Turquie se sont vues confrontées avec la fuite des données de leurs ressortissants. A ce rythme là, le big data de la NSA et autres collecteurs discrets n'est pas prêt de se tarir !… [Lire la suite]

Réagissez à cet article

Source : *ZATAZ 93 millions d’électeurs Mexicains accessibles sur la toile – ZATAZ*

Avant le règlement européen sur les données personnelles, la Loi pour la République Numérique

Avant le règlement européen sur les données personnelles, la Loi pour la République Numérique

---

Le nouveau règlement européen relatif à la protection des données personnelles (GDPR) fait grand bruit en Europe. Il donne, en effet, plus de droits aux consommateurs sur la façon dont leurs données sont traitées et requiert des contrôles complémentaires (et des informations) sur quiconque dispose de données personnelles dans l'Union européenne.

Comme toutes les lois, celle-ci a été largement discutée, avec des points de vue contradictoires, mais une chose a été acceptée par tous : les entreprises auront deux ans, à compter de la date de publication de la loi (en juin 2016), avant que celle-ci entre en vigueur. Deux années indispensables aux entreprises pour leur permettre de mettre en place les politiques, les processus et les technologies nécessaires pour être en conformité avec le règlement.
En avance sur ses voisins européens, la France a d'ores et déjà adopté un projet de loi en phase avec les principes fondamentaux du règlement européen relatif à la protection des données personnelles. Ainsi, le projet de loi pour une République numérique, validé par l'Assemblée nationale le 26 janvier dernier (actuellement examiné par le Sénat), devrait être approuvé pour entrer en vigueur cette année.

Quelles sont les grandes lignes de la loi pour la République numérique ?

Droit à la portabilité des données : le consommateur peut demander à ce que ses données soient conservées par le responsable du traitement des données et dispose en toutes circonstances d'un droit de récupération de ses données.
• Conservation des données : le responsable du traitement des données doit informer le consommateur de la durée pendant laquelle les données sont conservées.
• Droit de rectification : les consommateurs peuvent demander à ce que leurs données soient éditées pour les modifier.
• Droit à la suppression : les personnes concernées peuvent demander à ce que leurs données soient supprimées ou interdire l'usage de leurs données.
• Recours collectifs : les consommateurs peuvent déposer une plainte collective pour demander réparation lors de la perte ou de l'utilisation abusive de leurs données.
• Amende maximale : celle-ci peut aller de 150.000 à 20.000.000 euros ou 4 % du chiffre d'affaires global, pour l'amende la plus élevée.
D'autres pays vont-ils prendre exemple sur la France pour faire avancer leurs propres législations sur la protection des données avant la mise en œuvre du règlement européen ? Il y a fort à parier que oui. Et les entreprises ont également anticipé cette nouvelle réglementation puisque l'utilisation de services cloud basés dans la zone européenne a presque doublé en six mois (de 14,3 % au premier trimestre 2015 à 27 % pour 2016)… [Lire la suite]

Réagissez à cet article

Source : *Nouveau règlement européen sur les données personnelles : la France en avance sur ses voisins européens – Global Security Mag Online*

Vol massif d'empreintes digitales : la cybercriminalité entre dans une nouvelle ère

Vol massif d'empreintes digitales : la cybercriminalité entre dans une nouvelle ère

---

Cet été, 5.6 millions d'empreintes digitales ont été volées à un organisme étatique américain « l'Office of Personnel Management l'Office of Personnel Management », ce qui en fait la plus grande cyber attaque de l'histoire. Était-ce la première fois que des empreintes étaient dérobées ? Quel risque représente ce vol d'informations ?

Franck DeCloquement : Le bilan s'est en effet alourdit depuis les premières déclarations officielles. « L'Office of Personnal Management », une agence américaine en charge de la fonction publique aux États-Unis, a en effet indiqué mercredi 23 septembre 2015 que 5,6 millions de ses employés s'étaient fait « hacker » leurs empreintes palmaires. Dont des employés du Pentagone, de la NSA et du FBI… Ce piratage massif de fichiers qui aurait eu lieu en juin dernier avait aussi permis aux agresseurs d'accéder à des informations très personnelles, concernant plus de 21 millions d'Américains… Au nombre desquels leurs numéros de sécurité sociale ainsi que des éléments beaucoup personnels. Il y a trois mois à peine, l'OPM avait initialement déclaré que « seulement » 1,1 million d'empreintes avaient été dérobées…La réalité qui se fait jour est infiniment plus préoccupante…
Comme le rapportent les médias américains depuis ces révélations tapageuses – la chaine CNN en outre – ce piratage pourrait être le fait de hackers chinois… Il faut toutefois s'abstenir à cette heure, de toutes conclusions hasardeuses à ce sujet et savoir raison garder… [Lire la suite]

Réagissez à cet article

Source : *Vol massif d'empreintes digitales : la cybercriminalité entre dans une nouvelle ère | Atlantico.fr*

Le Paquet « Protection des données à caractère personnel » adopté

Le Paquet « Protection des données à caractère personnel » adopté

Le règlement général sur la protection des données ainsi que la directive relative à la protection des données à caractère personnel à des fins répressives ont été adopté le 14 avril…

Ce Paquet vise à réformer la législation communautaire d'une part et à remplacer la directive générale sur la protection des données qui datait de 1995 d'autre part.

1. Les nouveaux principes à mettre en oeuvre par le règlement

Le règlement européen sur la sur la protection des données (2) consacre de nouveaux concepts et impose aux entreprises de « disrupter » leurs pratiques et de revoir leur politique de conformité Informatique et libertés.
Si les formalités administratives sont simplifiées pour mettre en œuvre un traitement, les obligations sont en revanche renforcées pour assurer une meilleure protection des données personnelles :

• la démarche de « Privacy by design » (respect de la protection des données dès la conception) (Règlement, art. 25 §1) ;
• la démarche de « Security by default » (sécurité par défaut) (Règlement, art. 25 §2) ;
• les règles d'accountability (obligation de documentation) (Règlement, art. 24) ;
• l'étude d'impact avant la mise en œuvre de certains traitements (Règlement, art. 35) ;
• la désignation obligatoire d'un Data Protection Officer (DPO) (Règlement, art. 37) ;
• les nouveaux droits fondamentaux des personnes (droit à l'oubli, droit à la portabilité des données, etc.) sur lesquels nous reviendrons dans un prochain article.

1.1 Le respect de la protection des données dès la conception ou « Privacy by design »

Le règlement européen sur la protection des données consacre le principe de « Privacy by design » qui impose aux entreprises publiques comme privées de prendre en compte des exigences relatives à la protection des données dès la conception des produits, services et systèmes exploitant des données à caractère personnel.
Cette obligation requiert que la protection des données soit intégrée par la Direction des systèmes d'information dès la conception d'un projet informatique, selon une démarche « Privacy by design ». Elle rend également nécessaire la coopération entre les services juridiques et informatiques au sein des entreprises
.

1.2 La sécurité par défaut ou « Security by default »

Le règlement européen sur la protection des données pose une nouvelle règle, la « sécurité par défaut ». Cette règle impose à tout organisme de disposer d'un système d'information ayant les fonctionnalités minimales requises en matière de sécurité à toutes les étapes (enregistrement, exploitation, administration, intégrité et mise à jour).
La sécurité du système d'information doit être assurée dans tous ses éléments, physiques ou logiques (contrôle d'accès, prévention contre les failles de sécurité, etc.).
Par ailleurs, cette règle implique que l'état de la sécurité du système d'information puisse être connu à tout moment, par rapport aux spécifications du fabricant, aux aspects vulnérables du système et aux mises à jour.

1.3 L'étude d'impact

Le règlement européen sur la protection des données consacre l'obligation par les organismes de réaliser des analyses d'impact relatives à la protection des données.
Cette obligation impose à tous les responsables de traitements et aux sous-traitants d'effectuer une analyse d'impact relative à la protection des données personnelles préalablement à la mise en œuvre des traitements présentant des risques particuliers d'atteintes aux droits et libertés individuelles.
Dans un tel cas, le responsable du traitement ou le sous-traitant, doit examiner notamment les dispositions, garanties et mécanismes envisagés pour assurer la protection des données à caractère personnel et apporter la preuve que le règlement sur la protection des données est bien respecté.

1.4 L'obligation de documentation ou « accountability »

Le règlement européen sur la protection des données met à la charge du responsable de traitement des règles d'accountability qui constituent la pierre angulaire de la conformité « ab initio » avec la règlementation en matière de données personnelles.
Il s'agit pour le responsable du traitement de garantir la conformité au règlement en adoptant des règles internes et en mettant en œuvre les mesures appropriées pour garantir, et être à même de démontrer, que le traitement des données à caractère personnel est effectué dans le respect du règlement.
Les mesures prévues en matière de données personnelles et d'accountability vont de la tenue de la documentation, à la mise en œuvre des obligations en matière de sécurité en passant par la réalisation d'une analyse d'impact.
Cette démarche anglo-saxonne connue sous le terme d'accountability est une obligation pour le responsable du traitement de rendre compte et d'expliquer, avec une idée de transparence et de traçabilité permettant d'identifier et de documenter les mesures mises en œuvre pour se conformer aux exigences issues du règlement.
Il devra démontrer qu'il a rempli ses obligations en matière de protection des données. C'est une charge de la preuve qui l'oblige à documenter l'ensemble des actions de sa politique de protection des données de manière à pouvoir démontrer aux autorités de contrôle ou aux personnes concernées comment il s'y tient.

2. La protection des données à caractère personnel traitées à des fins répressives

Les pratiques en matière pénale sont très différentes d'un Etat à l'autre. Jusqu'à présent il n'y avait pas de cadre commun aux services répressifs des Etats membres.
La directive relative à la protection des données à caractère personnel à des fins répressives (3) prévoit que chaque Etat membre doit suivre un cadre commun tout en développant sa propre législation qui devra reprendre toutes les règles de base en matière de protection des données notamment en matière de sécurité.
Ce n'est pas une chose aisée dans la situation actuelle avec les menaces terroristes qui pèsent en Europe.
Parmi les nouveaux éléments importants de cette directive, figure la nécessiter de se préoccuper en permanence de la protection des données et de la vie privée. A ce titre, toutes les institutions liées aux services répressifs devront se doter d'un « Data protection officer ».
Il ne devrait plus y avoir de collecte de données personnelles sans objectif clair, sans durée limitée et les justiciables auront des droits clairs, comme celui de savoir quelles sont les données collectées, à quelle fin, et combien de temps elles seront conservées.
La directive permet de prendre en compte les spécificités liées aux services répressifs tout en préservant les droits universels des citoyens justiciables. Ces deux textes font partis d'un même paquet « protection des données ».
La tâche n'a pas été simple de réformer la directive de 1995 et d'en faire un règlement unifié directement applicable par les Etats membres. C'est probablement une grande première que d'avoir réalisé un tel texte qui s'applique directement à toute l'Union européenne dans un domaine qui règlemente un droit aussi fondamental que la protection des données.
Le règlement entrera en vigueur 20 jours après sa publication au Journal officiel de l'Union européenne. Ses dispositions seront directement applicables dans tous les Etats membres deux ans après cette date, soit en avril 2018.
En ce qui concerne la directive relative à la protection des données à caractère personnel à des fins répressives, les Etats membres auront deux ans pour transposer les dispositions qu'elle contient dans leur droit national.
Il s'agit là d'une grande avancée pour l'Union européenne tant pour les citoyens consommateurs que pour les entreprises.
Notes :
(1) Résolution législative du Parlement européen du 14 avril 2016 sur la position du Conseil en première lecture en vue de l'adoption du règlement général sur la protection des données.
(2) Règlement général sur la protection des données révisé le 8 avril tel qu'adopté par le Parlement européen le 14 avril 2016.
(3) Résolution législative du Parlement européen du 14 avril 2016 sur la position du Conseil en première lecture en vue de l'adoption de la directive relative à la protection des données à caractère personnel à des fins répressives… [Lire la suite]

Réagissez à cet article

Source : *Adoption du Paquet « Protection des données à caractère personnel »*

Le règlement sur la protection des données adopté par le parlement européen

Le règlement sur la protection des données adopté par le parlement européen

Le Parlement européen a adopté mercredi 6 avril 2016 le règlement sur la protection des données personnelles, qui entrera en application en 2018 pour remplacer l'actuelle directive de 1995, et harmoniser le droit de tous les états membres.

Après plus de quatre ans de débats, le Parlement européen a adopté jeudi le paquet sur la protection des données, qui comporte d'une part une directive sur les transferts de données à des fins policières et judiciaires, et d'autre part le très riche règlement de protection des données, qui entrera en vigueur d'ici deux ans.
Le règlement remplace l'actuelle directive de 1995, et présente par nature l'avantage de ne pas nécessiter de mesures d'adaptation par les différents états membres de l'Union européenne. Même s'il reste des options, l'essentiel du texte est d'effet direct et uniforme dans tous les pays, ce qui permettra aux citoyens et aux entreprises de bénéficier enfin des mêmes règles dans les 28 pays membres.
Opposable y compris aux entreprises basées hors de l'UE qui ciblent des consommateurs européens, le texte détermine le socle minimum de droits et de devoirs applicables aux traitements de données personnelles, notamment sur Internet.
Parmi les mesures notables, pour la plupart déjà prévues par le droit français ou anticipées dans le cadre du projet de loi numérique, figurent :
• L'obligation de recueillir un consentement « clair et explicite » (article 7) avant tout traitement de données personnelles. Il sera interdit de se contenter par exemple d'une politique de vie privée accessible par un lien, ou même de cocher par défaut par des cases de recueil du consentement. Celui-ci devra être en opt-in uniquement.
• L'interdiction aux enfants des réseaux sociaux ou autres services collecteurs de données, sauf autorisation des parents (article 8). Les états membres pourront fixer la limite d'âge entre 13 et 16 ans, selon leur sensibilité.
• La reconnaissance d'un « droit à l'oubli » (article 17) qui permet à un individu de demander l'effacement des données qui le concerne, y compris chez les sous-traitants ou partenaires, à condition que leur conservation ne soit pas nécessaire pour un motif légitime (recherches historiques, scientifique, statistiques, santé publique, exécution d'un contrat…), y compris le droit à la liberté d'expression.
• Le droit à la portabilité des données (article 20) qui offre aux utilisateurs d'un service en ligne la possibilité de prendre leurs données avec eux pour les importer vers un service concurrent, par exemple pour changer de fournisseur de messagerie électronique sans avoir à perdre ses contacts ou ses messages.
• La limitation du profilage par algorithmes (article 21). En principe, aucune décision ne doit pouvoir être prise sur la base d'une détermination purement algorithmique du profil de la personne. Par ailleurs, celui-ci n'est autorisée que si la personne donne son consentement. La portée exacte de l'article reste toutefois à analyser, tant il semble souple.
• Le droit d'être informé en cas de piratage des données (articles 33 et 34) : si une entreprise ou une organisation quelconque est victime d'un piratage de données de ses clients ou de tiers, elle devra immédiatement en informer l'autorité de protection des données (en France la Cnil), et dans le cas où cette divulgation ne pose pas de problème de sécurité, en informer les principaux concernés.
• La possibilité d'infliger des amendes jusqu'à 4 % du chiffre d'affaires mondial d'une entreprise, lorsqu'elle viole le droit à la protection des données. La sanction sera d'autant plus forte que la violation sera grave et consciente. Actuellement, le droit français n'autorise la CNIL qu'à infliger des amendes de 150 000 euros maximum, ce qui est ridiculement faible lorsqu'il s'agit de condamner des Google ou Facebook.

Nous aurons l'occasion de revenir plus en détails sur ces différentes mesures et le paquet de protection des données, qui seront applicables à partir de 2018…. [Lire la suite]

Réagissez à cet article

Source : *Le règlement sur la protection des données adopté par le parlement européen*

Microsoft poursuit le gouvernement américain

Microsoft	Microsoft poursuit le gouvernement américain

Aux États-Unis, Microsoft a initié une procédure à l'encontre du Department of Justice afin de faire invalider certaines dispositions de l'Electronic Communications Privacy Act. En substance, le géant veut pouvoir prévenir ses clients quand les autorités réclament des données les concernant.

Au fil des 18 derniers mois, Microsoft a reçu 5 624 demandes d'information émanant des autorités. Sur ce total, la firme a compté la bagatelle de 2 576 requêtes associées à une obligation de garder le silence. Elle a en outre relevé 1 752 cas dans lesquels cette contrainte était valable jusqu'à nouvel ordre – autant dire ad vitam æternam. Pour Microsoft, cette situation n'est pas acceptable. Sous couvert de l'Electronic Communications Privacy Act, établi en 1986, les autorités ignorent complètement la Constitution. Une procédure légale vient donc d'être engagée.
Concrètement, Microsoft s'attaque au Department of Justice (équivalent de notre ministère de la Justice), à qui il reproche d'ignorer sciemment deux amendements de la Constitution. En empêchant la firme de prévenir un client lorsque ses données sont consultées par une agence du gouvernement, celui-ci ferait à la fois fi de la liberté d'expression de Microsoft (1er amendement de la Constitution) et du droit du client à savoir ce que les autorités font avec sa propriété (4e amendement). En conséquence, plusieurs dispositions de l'Electronic Communications Privacy Act devraient tout simplement être invalidées. Reste à voir si le tribunal de Washington partagera ce point de vue.

Rappelons que ce n'est pas la première initiative de Microsoft pour mettre un terme aux indiscrétions silencieuses de la NSA (entre autres). Cela fait deux ans, maintenant, que la firme réclame ouvertement une très sérieuse remise en question des pratiques du gouvernement et des différents corps policiers qui en dépendent. L'appel, cependant, n'a toujours pas porté le moindre fruit. Il est donc temps, à l'évidence, d'actionner d'autres leviers pour espérer aboutir à un résultat… [Lire la suite]

Réagissez à cet article

Source : *Données personnelles : Microsoft poursuit le gouvernement américain*