Des millions de familles de fonctionnaires victimes d'une grosse cyberattaque | Le Net Expert Informatique

Des millions de familles de fonctionnaires victimes d'une grosse cyberattaque

La fonction publique aux USA a été la victime d'une importante cyberattaque. Les données de 21,5 millions de personnes sont concernées, parmi lesquelles les fonctionnaires et leurs familles.
Dans un communiqué de l'Office of Personnel Management, organisme qui chapeaute la fonction publique aux États-Unis, on apprend qu'une base de données a été pénétrée par des pirates informatiques. Ces derniers auraient ainsi récupéré les données personnelles (nom, prénom, adresse, numéro de sécurité sociale, etc.) d'environ 21,5 millions de personnes.
Parmi elles, 19,7 millions de fonctionnaires ayant fait l'objet d'une habilitation de sécurité, autrement dit une vérification des antécédents. Les autres sont des époux / épouses ou des enfants des fonctionnaires. Toute personne ayant fait l'objet d'un contrôle à partir de l'année 2000 est susceptible d'être concernée.

Ce piratage intervient après un autre révélé début juin qui concernait 4,2 millions de fonctionnaires toujours en poste. L'Office of Personnel Management estime que les deux attaques sont liées, ce qui place la Chine en tête des suspects. L'organisme indique toutefois qu'il ne dispose d'aucune information concernant la divulgation ou l'utilisation des données.

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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

Source : http://www.generation-nt.com/piratage-cyberattaque-donnees-personnelles-fonctionnaires-fonction-publique-actualite-1917077.html
Par Dimitri TAMION

Le Canada adhère à la

Convention de Budapest – Conseil de l’Europe | Le Net Expert Informatique

	Le Canada adhère à la Convention de Budapest – Conseil de l’Europe

L’Observateur permanent du Canada au Conseil de l’Europe, Alan Bowman, a déposé ce matin l’instrument de ratification de la Convention de Budapest sur la cybercriminalité.
Ainsi, le nombre de Parties atteint 47. Sept autres États ont signé la Convention et douze autres pays ont été invités à y adhérer. Actuellement, 66 États sont des Parties ou se sont officiellement engagés à devenir Parties à ce traité.

Liste des signatures, ratifications et adhésions à la Convention de Budapest

---

Source : http://www.coe.int/fr/web/cybercrime/-/canada-joins-budapest-convention

Cybercriminalité : 80 interpellations enregistrées au premier trimestre 2015 en Côte d'Ivoire – Abidjan.net | Le Net Expert Informatique

	Cybercriminalité : 80 interpellations enregistrées au premier trimestre 2015 en Côte d'Ivoire

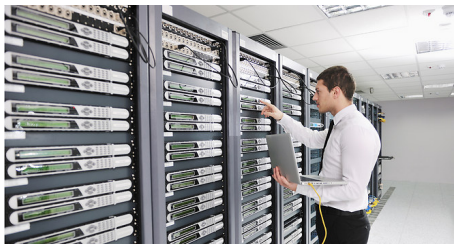
Quatre-vingts personnes soupçonnées de cybercriminalité ont été interpellés au premier trimestre 2015 en Côte d'Ivoire, avec 480 affaires traitées contre 450 affaires traitées et 70 interpellations 2014 dans le pays, a appris l'AIP auprès du directeur de la direction de l'informatique et des traces technologiques (DITT), le commandant Ouattara Guelpetchin.

Le directeur de la DITT, qui a fait cette annonce vendredi à Yamoussoukro, lors d'un colloque international sur la cybercriminalité, a indiqué par ailleurs que 90 % des infractions recensées au monde sont des infractions classiques avec usage des technologies de l'information et de la communication (TIC).

» En 2013, 85% de ces infractions sont commis depuis l'Afrique « , a précisé le commandant Ouattara Guelpetchin.
Initié par l'institut de lutte contre la criminalité économique (ILCE) de la haute école de gestion Arc (HEG Arc) et l'Ecole supérieure de commerce et d'administration des entreprises (ESCAE) de l'institut national polytechnique Houphouët-Boigny de Yamoussoukro, le colloque international a pour thème » l'impact de la cybercriminalité sur la société Ouest-africaine : exemple de la Côte d'Ivoire « .
Les infractions qualifiées « délinquance astucieuse » sur internet ont un impact au plan culturel, social et sur les investissements étrangers. « On évalue le préjudice subi à 1,5 milliards F CFA », a confié lors de sa communication l'étudiant Koné Aboubacar Sidiki de l'INP-HB dans le cadre de ses travaux de recherche .
Le colloque international sur la cybercriminalité, deuxième du genre, rassemble des experts du domaine en provenance de Suisse et de la Côte d'Ivoire, ainsi que les représentants des institutions publiques, des entreprises privées et des établissements d'enseignement supérieur, la presse et société civile.

Source : http://news.abidjan.net/h/559340.html

Des datacenters Helvétiques très discrets | Le Net Expert Informatique



Des datacenters Helvétiques très discrets

Pas d'opération clean data à l'horizon grâce à l'ipséité du droit suisse, mais plutôt un data shopping auquel se livrent les entreprises du monde entier. Avec une réglementation aussi exigeante que celle l'Union européenne, mais sans la surveillance tous azimuts des citoyens, la Suisse attire les sociétés désireuses de protéger leurs données dans un havre de sécurité et de secret.

Une protection des données à caractère personnel équivalente à celle de l'Union européenne

Le droit suisse de la protection des données personnelles repose sur la loi fédérale 235.1 de 1992 par l'Assemblée fédérale de la Confédération suisse (ou LPD). Les similitudes avec le droit européen sont nombreuses tant dans son champ d'application (définition des données à caractère personnel et statut particulier des données sensibles telles que les données de santé), que dans ses principes : licéité de la collecte des données et de leur traitement, bonne foi, proportionnalité, finalité, exactitude, sécurité et droits d'accès (art.4 à 25 LPD).

Ceci résulte des accords de Schengen et de Dublin, en vertu desquels la Suisse doit reprendre le droit pertinent de l'UE, y compris en matière de protection des données personnelles. Le droit suisse de la protection des données personnelles est d'ailleurs reconnu adéquat au sens de la directive 95/46/CE par la Commission européenne depuis 15 ans (décision n°2000/5/8/CE). Les garanties sont donc bien plus solides que celles offertes par le droit américain qui ne bénéficie que d'un accord de Safe Harbor (les entreprises américaines qui veulent recevoir des données de l'UE doivent y adhérer).

La Suisse préserve le secret digital

La valeur ajoutée de la Confédération réside dans le fait qu'elle se refuse à exercer tout contrôle administratif sur les données stockées tel qu'il existe aux US avec le Patriot Act et en France avec la Loi de Programmation Militaire qui permet de requérir l'accès à des informations de connexion ou à la localisation des équipements terminaux utilisés ou encore avec le Projet de loi français relatif au renseignement déposé à l'Assemblée nationale le 19 mars 2015. De tels mécanismes poussent les entreprises à faire héberger leurs données hors des territoires américain et français.

La Confédération helvétique, bien au contraire, n'autorise la levée du secret que sur ordre judiciaire et garantit ainsi le respect du principe démocratique. Le juge suisse utilise d'ailleurs la jurisprudence européenne en matière de protection des données personnelles pour justifier ses propres considérants (affaire Logistep, 2010). La Suisse maintient ainsi un niveau de protection des données à caractère personnel équivalent au droit de l'UE tout en respectant les libertés individuelles.

Enfin, une nouvelle génération de datacenter écologiques a récemment été récompensée par le Prix du développement durable afin de promouvoir auprès des clients, partenaires, fournisseurs et des collaborateurs une gouvernance intégrant l'éthique et des valeurs de responsabilité sociale (engagements autour de thématiques telles que l'énergie, la mobilité, la politique d'achat et la gestion des déchets). Or, les entreprises doivent réaliser un audit énergétique de leurs activités avant le 5 décembre 2015. Une raison de plus d'exiler ses données vers la Confédération.

Source : http://www.lesechos.fr/idees-debats/cercle/cercle-134577-lexil-des-datacenters-vers-la-confederation-helvetique-1135913.php
Par Nathalie Devillier / Docteur en Droit – Grenoble Ecole de Management

---

Les voitures promises aussi à

des bugs logiciels et des mises à jour ? | Le Net Expert Informatique

	**Les voitures promises aussi à des bugs logiciels et des mises à jour ?**

Ford doit rappeler 433.000 voitures en Amérique du Nord en raison d'un bug logiciel, à savoir l'impossibilité de couper le moteur. Les propriétaires doivent retourner chez leur garagiste pour effectuer une mise à jour. On n'arrête plus le progrès ?

Fin mai, Frédéric Charles du blog Green SI de ZDNet.fr expliquait pourquoi il avait été obligé rebooter sa voiture en raison d'un problème logiciel. Car en effet, le logiciel est de plus en plus présent dans nos véhicules. Pour les automobilistes, les pannes mécaniques ne sont plus le seul tracas qui les guette.
Et notre bloggeur n'est pas un cas isolé. Le constructeur Ford a ainsi été contraint d'émettre un rappel portant sur 433.000 voitures en Amérique du Nord (modèles Focus, C-MAX et Escape). C'est précisément le logiciel du système de commande qui est en cause.

Le logiciel apporte des fonctions, et des bugs potentiels
Sur son site Internet, Ford mentionne un dysfonctionnement du module de contrôle ayant pour conséquence l'impossibilité de couper le moteur de la voiture, y compris lorsque le conducteur tourne et retire la clé.
Les propriétaires concernés sont invités à se rendre chez leurs concessionnaires… afin d'appliquer une mise à jour logicielle sur leur véhicule, un peu comme cela se fait déjà, et depuis de nombreuses années, sur un ordinateur.
Confronté à l'impossibilité de reprendre la route, Frédéric Charles avait procédé à ce qui s'apparente à une forme de « reboot » ou redémarrage de sa voiture. Comment ?
« Clef dans la poche en dehors du véhicule, je débranche [la batterie], j'attends 30s, je rebranche, la voiture se réinitialise, je redémarre, et voilà que tout rentre dans l'ordre. Mon garagiste étant le premier surpris. J'ai depuis avalé des centaines de kilomètres sans aucun problème » racontait-il.
« L'enjeu des véhicules connectés est aussi le support numérique, de véhicules de plus en plus sophistiqués. Sinon, il ne nous restera plus qu'à apprendre à rebooter notre voiture régulièrement et croiser les doigts à chaque fois, comme avec les bon vieux PCs. Nostalgie, nostalgie… » commentait-il encore.

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

Source : http://www.zdnet.fr/actualites/les-voitures-promises-comme-les-pc-a-des-bugs-logiciels-et-des-mises-a-jour-39822008.htm

Une nouvelle loi en matière de protection des données obligera les entreprises à de l'autocontrôle | Le Net Expert Informatique

© Thinkstock

Une nouvelle loi en matière de protection des données obligera les entreprises à de l'autocontrôle

L'Europe va moderniser la loi portant sur la conservation des données personnelles. Cela devrait simplifier la vie des entreprises européennes, mais celles-ci devront aussi veiller à ne pas enfreindre cette loi par mégarde.

Il s'agit en l'occurrence de la 'general data protection regulation', un ensemble de règles qui s'appliquent actuellement dans chaque état membre et qui spécifient quelles données peuvent être tenues à jour, pendant combien de temps et ce que l'on peut en faire. L'objectif de l'Europe est de la moderniser au niveau européen, pour qu'une série de règles unique entre en vigueur dans toute l'Union européenne, en ce compris aussi une seule autorité susceptible de prendre des décisions à propos des litiges et infliger des amendes pour l'ensemble de l'UE.
L'un des éléments sur la table est d'y voir figurer ce qu'on appelle le droit à l'oubli, permettant aux citoyens de demander aux moteurs de recherche de ne plus afficher certains résultats, mais aussi à des entreprises de supprimer des données personnelles, si elles n'ont aucune raison légale de les conserver.
L'Union européenne estime que les entreprises économiseront annuellement 2,3 milliards d'euros avec une loi uniformisée. Il y a pourtant un revers à la médaille: quiconque est aujourd'hui en règle avec la législation belge, ne le sera peut-être pas avec la loi européenne, selon James Luby de BalaBit, spécialisé dans le 'log management': « La proposition de loi se caractérise par la 'privacy by design'. Mais nombre d'entreprises possèdent aujourd'hui automatiquement des données générées par les utilisateurs, tout en ne sachant pas qu'il s'agit de données personnelles. Elles devront également en faire plus pour conserver et gérer ces données. »
Luby évoque notamment des données de connexion, comme par exemple en e-commerce. « Beaucoup d'entreprises ne savent pas ce qu'elles collectent via leurs plates-formes. Or elles devront en être conscientes bientôt. »
Les entreprises devraient donc faire des économies à long terme, mais d'ici à l'entrée en vigueur de la loi modernisée, elles devront également veiller à se mettre en règle avec celle-ci. Mais ce n'est pas encore urgent, puisque les entretiens entre la Commission européenne, le Parlement européen et les ministres nationaux concernés débutent à peine. Il est probable que cela se traduira en texte de loi au début de l'année prochaine.

Source : http://datanews.levif.be/ict/actualite/une-nouvelle-loi-en-matiere-de-protection-des-donnees-obligera-les-entreprises-a-de-l-autocontrole/article-normal-402231.html
Par Pieterjan Van Leemputten

Les dessous de la société d’espionnage Hacking Team… | Le Net Expert Informatique

Les dessous de la société d’espionnage Hacking Team…

La firme, qui s'est fait voler plus de 400 gigaoctets de données confidentielles, avait présenté ses technologies aux services de renseignements français. La société Hacking Team, soupçonnée d'avoir livré des logiciels d'espionnage à des régimes autoritaires, assure n'avoir rien commis d'illégal.

On soupçonnait Hacking Team de rouler sa bosse pour des dictatures. Et voilà que le journal Le Monde nous apprend que la sulfureuse entreprise d'espionnage a également eu des contacts avec les services d'espionnage français… Lundi 6 juillet, la société italienne a été victime d'un piratage de grande ampleur de ses données confidentielles et des comptes Twitter de plusieurs de ses responsables. Des centaines de gigaoctets de données se sont déversées sur le Web et ont été immédiatement téléchargées et consultées par ceux qui l'accusaient de faire bénéficier de ses technologies des régimes autoritaires.
L'entreprise est en effet spécialisée dans le développement et la commercialisation de logiciels de surveillance ou de piratage très performants, principalement destinés à des États. Logiciels de blocage de pages internet, systèmes de mise sous surveillance de boîtes mails jugées suspectes… Hacking Team a développé une impressionnante gamme de services. Leur produit phare, dénommé RCS (pour Remote Control Systems), est un packaging incluant des logiciels tels que DaVinci et Galileo, qui permettent de visualiser les frappes effectuées sur le clavier de l'ordinateur visé, d'en collecter les informations sensibles telles que les adresses mails, les documents enregistrés ou les mots de passe, ou encore de récupérer les historiques de navigation.

Ennemie d'Internet
La facilité avec laquelle ces outils peuvent être utilisés à des fins d'espionnage de masse avait conduit certaines ONG à dénoncer les pratiques de cette société. Cette dernière avait même fini par être classée parmi les ennemis d'Internet par Reporters sans frontières en 2013, en raison des rapports commerciaux qu'elle entretenait alors avec le Maroc et les Émirats arabes unis. Des traces de ses logiciels avaient ainsi été retrouvées sur les ordinateurs du site d'information marocain Mamfakinch, quelques jours après que ce média a reçu le Breaking Borders Award 2012 remis par Global Voices et Google.
Autre soupçon : « Un expert en sécurité, Morgan Marquis-Boire, a examiné des pièces jointes attachées à un e-mail envoyé à Ahmed Mansoor, un blogueur émirati. Elles étaient contaminées. Il y a trouvé de fortes indications suggérant que la source du cheval de Troie provenait de Hacking Team », écrit également RSF.
L'entreprise jouit dans le milieu d'une réputation douteuse, et est soupçonnée de collaborer avec des pays peu recommandables. Jusqu'à présent, la société clamait son innocence et aucune preuve de son implication dans la mise en place des systèmes de surveillance électronique de ces pays n'avait été découverte. « Nous faisons extrêmement attention à qui nous vendons nos produits. Nos investisseurs ont mis en place un comité légal qui nous conseille continuellement sur le statut de chaque pays avec lequel nous entrons en contact », assurait le PDG de Hacking Team, David Vincenzetti, dans une interview accordée en 2011 au journaliste Ryan Gallagher.

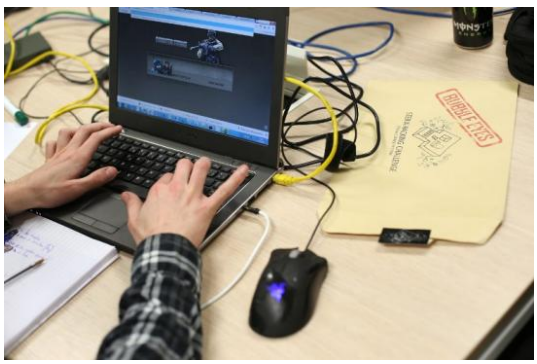
Des régimes autoritaires en clients
Kazakhstan, Arabie saoudite, Azerbaïdjan… De nombreux États – dont les dirigeants ne font pas toujours des libertés individuelles une priorité de leur règne… – font partie de la liste des clients. Parmi ces pays, certains sont connus pour une répression dure de leur population et leurs violations répétées des droits de l'homme. On peut ainsi noter l'exemple du Soudan, avec lequel Hacking Team a toujours nié avoir collaboré. Cependant, les documents publiés révèlent l'existence d'un contrat de 480 000 euros avec le gouvernement actuellement en place. La Russie fait également partie des heureux bénéficiaires des services de Hacking Team. La firme prend même la peine d'indiquer sur ses documents internes que ces deux pays ne sont « officiellement pas clients » (« oficially not supported ») de l'entreprise.
Interrogé au sujet de la série de contrats signés avec le Soudan, le porte-parole de l'entreprise, Éric Rabe, a quant à lui maintenu que le document cité remontait à avant les sanctions décidées par les Nations unies contre le pays.

La France, elle aussi intéressée par les services de l'entreprise
D'après certains documents, la France et Hacking Team seraient entrés en contact plusieurs fois ces dernières années. La prise de contact entre le ministère de la Défense et l'entreprise a eu lieu en 2013, alors qu'une réunion de présentation s'est tenue fin 2014 dans un hôtel près de l'aéroport Charles-de-Gaulle à Paris. Étaient représentés à cette réunion la DGSI et le Groupement interministériel de contrôle (GIC) chargé quant à lui des écoutes administratives (c'est-à-dire menées sans mandat judiciaire), et dirigé par le Premier ministre.
Si la DGSI affirme n'avoir donné aucune suite à cette réunion, ce n'est pas le cas du GIC qui a poursuivi ses échanges avec Hacking Team. Comme le révèle un échange de courriels entre le GIC et Hacking Team, Philippe Vinci, l'un des responsables de l'entreprise, s'est rendu au siège du GIC le vendredi 3 avril 2015. Cette information est confirmée par un échange de courriels entre la société et le groupement interministériel datant du mardi 7 avril. On y apprend également que le GIC serait intéressé par une démonstration de la part d'Hacking Team. L'entreprise aurait alors proposé aux représentants du GIC de venir assister à une telle démonstration en Italie courant mai. Aucune information concernant la suite à donner à ces rendez-vous n'a pour le moment fuité.

« Nous n'avons rien à cacher »
Après deux jours sans réaction, l'entreprise a finalement commenté ce vol de données dans une interview accordée au site IBTimes : « Nous n'avons rien à cacher sur nos activités et nous pensons qu'il n'y a aucune preuve dans ces 400 gigabits de données que nous avons violé une quelconque loi », a ainsi affirmé le porte-parole de l'entreprise, Éric Rabe.
Pour le moment, et en attendant de connaître exactement le contenu des données qui ont été piratées, la société italienne a demandé à ses clients de cesser d'utiliser ses logiciels. Les auteurs du piratage ne se sont pas encore manifestés.

Source : http://www.lepoint.fr/high-tech-internet/les-curieux-clients-de-la-societe-d-espionnage-hacking-team-08-07-2015-1943190_47.php
Par Ian BEAURAIN

Alerte à diffuser ! Une faille de vulnérabilité Flash Player révélée par le piratage de Hacking Team | Le Net Expert Informatique



Alerte à diffuser ! Une faille de vulnérabilité Flash Player révélée par le piratage de Hacking Team

Les cybercriminels s'en frottent déjà les mains entre deux piratages. Deux jours après la mise en ligne de données piratées de l'éditeur de logiciels espions Hacking Team, les experts, qui ont épluché les 400 Go de documents, ont fait la découverte d'une faille de sécurité importante de Flash Player, un lecteur multimédia autonome utilisé par des sites commes Youtube, Dailymotion ou encore Facebook.

C'est l'éditeur d'antivirus Micro Trend qui a révélé sur son blog cette faille «zero-day», c'est à dire inconnue jusqu'à présent et sans correctif pour l'instant. Elle permet à un attaquant de prendre le contrôle à distance d'un ordinateur en exécutant un code arbitraire à distance ou dans le cas plus précis d'une entreprise de surveillance comme Hacking Team d'installer ses logiciels espions sans se faire remarquer.
Symantec a confirmé cette porte d'entrée dans votre ordinateur et conseille sur son blog (en anglais) de désactiver temporairement Flash Player sur les sites Internet douteux surtout sur Internet Explorer, le navigateur le plus exposé.
Le Centre gouvernemental de veille, d'alerte et de réponse aux attaques informatiques (CERT-FR) a lui aussi confirmé la faille et ses potentielles conséquences. Le CERT-FR précise que des «plusieurs kits d'exploitation (de pirates informatiques, NDLR) ont intégré cette vulnérabilité qui est activement exploitée».
Prise à défaut, l'entreprise américaine Adobe, à l'origine de Flash Player, a promis d'apporter un patch correcteur dans la journée de mercredi. D'autres failles de sécurité pourraient être révélées sur la masse de documents qui ont fuité. Mais les plus dangereuses restent celles dont seul un groupe d'initiés est au courant.

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

Source : http://www.leparisien.fr/high-tech/flash-player-une-faille-de-vulnerabilite-revelee-par-le-piratage-de-hacking-team-08-07-2015-4928849.php
Par Damien Licata Caruso

Comment prémunir les visiteurs de votre site internet de cyberattaques ? | Le Net Expert Informatique

Comment prémunir les visiteurs de votre site internet de cyberattaques?

Switch propose un site web visant à aider les propriétaires de noms de domaines internet en Suisse à protéger leur site web contre des cyber-attaques.

Afin d'aider les propriétaires de sites internet à lutter contre les malwares qui pourraient y être installés, Switch met en ligne Safer Internet, un site internet d'information sur les menaces que représentent les criminels sur internet et les mesures préventives à adopter. Michael Hausding, expert en sécurité de Switch, explique les raisons de la mise en place d'un tel site: «Par la plateforme de sécurité Safer Internet, nous nous adressons à tous les détenteurs d'un site web .ch. Nous y donnons des conseils sur la prévention de l'abus de noms de domaine et informons sur les dangers relatifs à des contenus online.»
Les propriétaires de noms de domaines y trouveront notamment cinq conseils pour prévenir des attaques par Drive-by (qui infectent les usagers d'un site contenant un malware) et par Phishing (qui consistent à obtenir des informations personnelles via notamment des sites contrefaits). Parmi ses conseils se trouvent par exemple le fait d'utiliser une système de gestion du contenu (CMS) toujours à jour.
Ce site est disponible en quatre langues: allemand, français, italien et anglais. Il s'adresse en premier lieu aux gestionnaires de sites web qui sont tenus de nettoyer leur site s'il est infecté au risque de les voir bloqué.
La fondation Switch a pour objectif de rendre internet sûr en Suisse.

Le lien vers le site Internet « Safer Internet » de la société « Switch » : http://www.switch.ch/saferinternet

---

Source : http://www.ictjournal.ch/fr-CH/News/2015/07/07/Comment-premunir-les-visiteurs-de-votre-site-internet-de-cyberattaques.aspx

---

Pourquoi le Big data va révolutionner les DRH | Le Net Expert Informatique

Pourquoi le Big data va révolutionner les DRH

Le Big data se met au service des ressources humaines. Aujourd'hui, les plates-formes collectent des données sur les candidats partout sur Internet. Une technologie qui va totalement bousculer la gestion de carrières et dynamiter le recrutement. Pour le meilleur, mais aussi pour le pire.

Depuis quelques années, les éditeurs de logiciels de gestion des ressources humaines, notamment ceux qui offrent leur service dans le cloud, s'intéressent au Big data. Certains utilisent des bases de données in-memory, d'autres ont mis en place des technologies type Hadoop afin d'offrir à leurs utilisateurs des capacités avancées d'analyse et de reporting sur les données RH.
Non seulement, ceux-ci peuvent davantage croiser des données entre les formations, les compétences, les salaires, les absences, mais ils peuvent aussi injecter, dans leurs analyses, des données captées sur Internet et sur les réseaux sociaux.
Dans le recrutement, le Big data permet déjà aux entreprises d'aller chercher les meilleurs candidats non plus dans le vivier de CV qui leur sont adressés, mais directement sur les forums et les réseaux sociaux.
Alors, pourquoi s'embêter à lire des CV quand un algorithme peut jouer les chasseurs de tête ou détecter les salariés « à risque » ? Ces méthodes prédictives tout droit venues du marketing débarquent dans les RH. C'est une véritable révolution qui s'apprête à voir le jour dans la profession.

Lire la suite….

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement.
Besoin d'informations complémentaires ?
Contactez-nous
Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

Expert Informatique assermenté et formateur spécialisé en sécurité Informatique, en **cybercriminalité** et en **déclarations à la CNIL**, Denis JACOPINI et Le Net Expert sont en mesure de prendre en charge, en tant qu'intervenant de confiance, la sensibilisation ou la **formation de vos salariés** afin de leur enseigner les bonnes pratiques pour assurer une meilleure sécurité des systèmes informatiques et améliorer la protection juridique du chef d'entreprise.
Contactez-nous

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