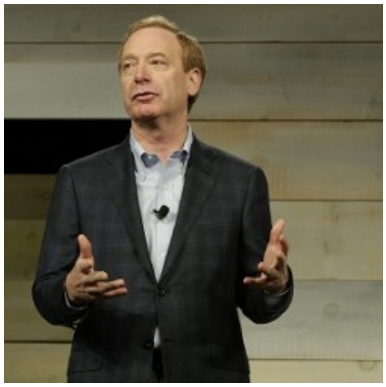
Charlie Hebdo : Microsoft a fourni en 45mn des données au FBI

	Charlie Hebdo : Microsoft a fourni en 45mn des données au FBI

S**ur demande du FBI, Microsoft a livré en un temps record des informations liées à des comptes de messagerie de suspects impliqués dans l'attentat de Charlie Hebdo. Une attitude qui remet sur le devant de la scène l'éternel débat entre protection des données personnelles et enjeux de sécurité.**

45 minutes. Tel a été le temps de réaction éclair de Microsoft pour transmettre au FBI des données liées à l'attentat qui a frappé Charlie Hebdo le 7 janvier dernier. Le journal économique Bloomberg explique ainsi que la firme de Redmond a répondu de façon hyper réactive à une requête du FBI réalisée dans le cadre de cette terrible affaire.

Brad Smith, avocat général de Microsoft, aimerait bien que sa société n'ait pas à jouer sur les deux tableaux en matière de vie privée et de sécurité. (crédit : D.R.)

« Il y a juste deux semaines, en pleine chasse aux suspects impliqués dans l'attaque de Charlie Hebdo, le gouvernement français a demandé à obtenir le contenu de mails de deux comptes clients détenus par Microsoft », a indiqué dans un discours à Bruxelles Brad Smith, l'avocat général de l'éditeur dont Bloomberg s'est fait écho. La firme de Redmond s'est ainsi montrée particulièrement coopérative en répondant à la demande du FBI de faire remonter le contenu des e-mails en question en tout juste 45 minutes.
Une réactivité dont n'a justement pas toujours fait preuve le même Microsoft pour fournir des informations, également liées à des mails et comptes de messagerie, à la justice américaine dans le cadre d'autres affaires comme celle, récente, relative à un trafic de drogue. La firme de Redmond ayant alors à l'époque tenu un discours qui tranche avec la réactivité dont elle a fait preuve pour répondre à la requête du FBI dans l'affaire Charlie Hebdo : « En vertu du 4e amendement de la constitution américaine, les utilisateurs ont le droit de garder leurs communications par courriel privées. Nous avons besoin que notre gouvernement respecte les protections constitutionnelles de vie privée et respecte les règles en matière de vie privée établies par la loi ».

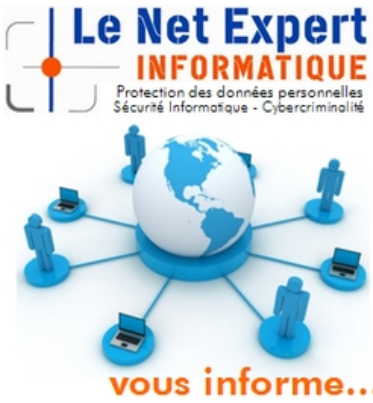
Microsoft en aucun cas prêt à se substituer au législateur
Mais depuis les attentats qui ont marqué la France et leurs répercussions partout dans le monde, des voix politiques se sont élevées pour fendre l'armure de la vie privée au nom des enjeux de sécurité. Notamment celle du Premier Ministre de la Grande-Bretagne, David Cameron, qui a prôné pour un renforcement des pouvoirs des services de sécurité pour s'assurer que les terroristes n'utilisent pas Internet pour communiquer secrètement entre eux.
« Si les membres du gouvernement veulent déplacer le curseur entre sécurité et vie privée, la façon appropriée de le faire est de modifier la loi plutôt que de demander aux acteurs privés comme nous de le déplacer nous-mêmes », a déclaré Brad Smith. Une saillie qui ne va à coup sûr pas manquer de raviver l'éternel débat – et les polémiques – entre ardents défenseurs de la vie privée et militants d'une sécurité sans faille. Car si tout le monde est d'accord pour détecter et empêcher les terroristes d'agir, l'étendue et la puissance des moyens à mettre en oeuvre pour y parvenir est loin de faire l'unanimité.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-charlie-hebdo-microsoft-a-fourni-en-45mn-des-donnees-au-fbi-59995.html
par Dominique Filippone

Protection des données personnelles : L'AFCDP

endosse la déclaration du groupe article 29



Protection des données personnelles : L'AFCDP endosse la déclaration du groupe article 29

Le 8 décembre 2014, à l'Unesco et en présence du Premier ministre, la Présidente de la CNIL a dévoilé la « Déclaration commune des autorités européennes de protection des données réunies au sein du groupe de l'article 29(1) ».

L'AFCDP (Association Française des Correspondants à la protection des Données à caractère Personnel) se reconnait pleinement dans les quinze points de cette déclaration, qu'elle vient d'endosser.
Les projets européens de règlement et de directive relatifs à la protection des données doivent assurer un haut niveau de protection des données aux personnes, conforme aux valeurs et droits fondamentaux de l'Europe.
« Dans la continuité de ce que fait le CIL aujourd'hui, le futur Délégué à la protection des données doit être un acteur clé de la protection des données personnelles dans la proposition de règlement » déclare Paul-Olivier Gibert, Président de l'AFCDP, « Cet expert contribuera à rendre plus effective la protection des données personnelles, à réduire les contraintes administratives inutiles, et à créer la confiance ».
Les projets européens de règlement et de directive relatifs à la protection des données doivent être adoptés en 2015. Outre contribuer à l'unification du marché numérique européen, ces textes doivent assurer un haut niveau de protection des données aux personnes, conforme aux valeurs et droits fondamentaux de l'Europe.
« Les propositions que nous avons formulées auprès de Bruxelles2, via la Confédération européenne des organisations de protection des données (CEDPO), vont dans ce sens » ajoute Paul-Olivier Gibert.
Pour la Présidente de la CNIL, Madame Isabelle Falque Pierrotin, cette déclaration permet de réaffirmer les valeurs communes de l'Europe : « Notre vie quotidienne est numérique et les données personnelles constituent la particule élémentaire de ce monde numérique. Des quantités gigantesques de données sont stockées, traitées et partagées sans que les individus disposent d'une réelle maîtrise de leurs données. Du fait de son histoire et de sa culture, l'Europe doit faire entendre sa voix à un moment charnière. C'est l'objet de la déclaration politique adoptée par les 28 autorités de protection européennes qui réaffirment les valeurs communes de l'Europe et proposent des actions concrètes pour assurer un équilibre entre protection des données personnelles, innovation et impératifs de sécurité. En activant l'ensemble de ces leviers, l'Europe pourra proposer un cadre éthique durable et offrir un environnement de confiance aux citoyens et de compétitivité aux acteurs économiques. »

L'AFCDP a été créée dès 2004, dans le contexte de la modification de la Loi Informatique & Libertés qui a officialisé un nouveau métier, celui de « Correspondant à la protection des données à caractère personnel » (ou CIL, pour Correspondant Informatique & Libertés).
L'AFCDP est l'association représentative des CIL, mais elle rassemble largement. Au-delà des professionnels de la protection des données et des Correspondants désignés auprès de la CNIL, elle regroupe toutes les personnes intéressées par la protection des données à caractère personnel. La richesse de l'association réside – entre autres – dans la diversité des profils des adhérents : Correspondants Informatique & Libertés, délégués à la protection des données, juristes et avocats, spécialistes des ressources humaines, informaticiens, professionnels du marketing et du e-commerce, RSSI et experts en sécurité, qualiticiens, archivistes et Record Manager, déontologues, consultants, universitaires et étudiants.

Quelques membres de l'AFCDP :
3 Suisses, Accor, Adecco, AG2R La Mondiale, American Hospital of Paris, AXA, BP France, Carrefour, Cecurity.com, Caisse nationale des allocations familiales, Communauté Urbaine de Marseille Provence, Conseil Général de Seine-Maritime, CCIP, CPAM des Bouches du Rhône, Crédit Immobilier de France, Ecole Polytechnique, Fédération Nationale des Tiers de Confiance, Orange, IBM France, INRA, Groupe Casino, Legrand, Malakoff Mederic, Michelin, La Poste, Port autonome de Dunkerque, RATP, Région Haute Normandie, Région Lorraine, Sénat, SNCF, Ville de Paris, Ville de Saint-Etienne, Total…
1 Texte en français disponible sur http://europeandatagovernance-forum.com/pro/fiche/quest.jsp
2 Appel à mesures d'incitation afin de promouvoir la désignation de délégués à la protection des données, disponible en français sur http://www.novosite.nl/editor/assets/cedpo/CEDPO_Warsaw_Declaration_final%20in%20French.pdf

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

Source : http://www.dsih.fr/article/1327/protection-des-donnees-personnelles-l-afcdp-endosse-la-declaration-du-groupe-article-29.html

---

Les services DDoS à la

demande des pirates de Sony, Lizard Squad, piratés

	Les services DDoS à la demande des pirates de Sony, Lizard Squad, piratés

L’adage veut que les cordonniers soient toujours les plus mal chaussés. Le piratage de LizardStresser, le service de DDoS à la demande de Lizard Squad, tend à confirmer cette règle : le fichier contenant les identifiants et mots de passe des membres n’était même pas chiffré.

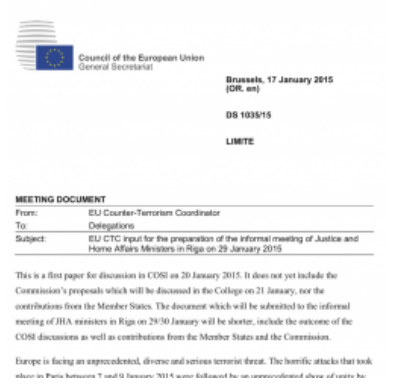
Petit retour en arrière. Nous sommes fin décembre, à quelques heures de Noël, et le groupe de pirates connu sous le nom de Lizard Squad se rappelle au bon souvenir de tout le monde en mettant le PlayStation Network et le Xbox Live hors ligne. Les conséquences s’étendent sur plusieurs jours et le collectif peut se réjouir : il a livré une démonstration très visible de la force de frappe de son réseau basé sur des routeurs piratés. Son service LizardStresser, qui propose de lancer des attaques DDoS à la demande, enregistre alors de nombreuses inscriptions.
Mais cette période faste n’a été que de courte durée. En effet, outre plusieurs arrestations, notamment outre-Manche, un autre pirate ou groupe de pirates s’en est pris au site hébergeant le service LizardStresser. Le service en lui-même est a priori intact, mais sa base de données incluant notamment les pseudonymes et mots de passe des membres est maintenant dans la nature. Or, de manière assez curieuse, Lizard Squad n’a pas jugé nécessaire de se protéger contre le piratage : ses fichiers sont stockés en clair.

Ceux-ci ayant rapidement été publiés, tout le monde a pu voir que les affaires marchaient plutôt bien. Au moment du piratage, LizardStresser comptait la bagatelle de 14 241 membres. Beaucoup, toutefois, n’étaient que des curieux. Comme le pointe KrebsonSecurity, ils n’étaient « que » quelques centaines à avoir alimenté leur compte dans le but de financer une attaque. En tout, Lizard Squad aurait perçu un peu plus de 11 000 $, versés en bitcoins.
Bien sûr, le collectif de pirates n’a que modérément apprécié de voir de ses précieuses données étalées sur la toile. Une copie des documents, en particulier, était disponible sur Mega. Le groupe ne s’est donc pas démonté et a formulé une requête au titre de la loi DMCA, qui protège le droit d’auteur en imposant aux hébergeurs de retirer les contenus publiés illégalement. Comble de l’absurde, celle-ci a été acceptée. De nombreuses copies, néanmoins, demeurent disponibles sur d’autres sites.

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

Source : http://www.lesnumeriques.com/lizard-squad-service-ddos-a-demande-pirate-n38817.html

L’UE doit-elle obliger les géants de l’Internet à céder leurs clés de chiffrement ?



Council of the European Union
General Secretariat

Brussels, 17 January 2015
(OR. en)

DS 1035/15

LIMITE

MEETING DOCUMENT

From: EU Counter-Terrorism Coordinator
To: Delegations
Subject: EU CTC input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015

This is a first paper for discussion in COSI on 20 January 2015. It does not yet include the Commission's proposals which will be discussed in the College on 21 January, nor the contributions from the Member States. The document which will be submitted to the informal meeting of JHA ministers in Riga on 29/30 January will be shorter, include the outcome of the COSI discussions as well as contributions from the Member States and the Commission.

Europe is facing an unprecedented, diverse and serious terrorist threat. The horrific attacks that took

L’UE doit-elle obliger les géants de l’Internet à céder leurs clés de chiffrement ?

La montée en puissance du terrorisme en Europe relance le débat sur le chiffrement des communications et la création de backdoors réservés aux forces de l’ordre européenne. Le coordinateur antiterrorisme de l’UE, Gilles de Kerchove, demande sans détour un accès aux clefs de chiffrement des géants de l’Internet.

Les géants de l’Internet vont-ils bientôt être obligés de partager leurs clés de chiffrement avec la police et les agences de renseignement européennes pour les aider à lutter contre le terrorisme ? C’est en tout cas une recommandation ferme de Gilles de Kerchove, le coordinateur antiterrorisme de l’Union Européenne. C’est une suggestion étonnante quand on se souvient que les entreprises comme Google ou Facebook ont commencé à chiffrer leurs communications pour lutter contre la curiosité des agences de renseignement chinoises mais aussi américaines, anglaises, allemandes, hollandaises et françaises comme l’ont indiqué les documents révélés par Edward Snowden.

L’association de protection des droits civils Statewatch
a divulgué un document rédigé par le coordinateur
antiterroriste Gilles de Kerchove.

Gilles de Kerchove suggère que la Commission européenne « devrait revoir ses règles pour obliger les entreprises de l’Internet et des télécommunications opérant dans l’UE à fournir … aux autorités nationales compétentes un accès à leurs communications [c’est à dire leurs clefs de chiffrement] », selon un document divulgué par l’association de protection des droits civils Statewatch. Dans ce document, M. de Kerchove expose ses vues sur les mesures anti-terrorisme à prendre dans l’UE en vue d’une réunion des ministres de la Justice et de l’Intérieur de l’UE à Riga, la semaine prochaine.

Des keyloggers pour suivre les échanges

Cette proposition est controversée parce que, comme le note le coordinateur, la généralisation du chiffrement pour les échanges sur Internet rend très difficile, voire impossible, les interceptions légales par les autorités nationales compétentes. Nous avons discuté de ces questions avec les cybergendarmes de Paris (Section de recherche de Paris et ses spécialistes N-Tech) et de Rosny Sous Bois (C3N). Sans coopération des fournisseurs de services (Whatsapp, Skype ou encore iMessage), il est très difficile de lire les messages échangés. La solution la plus facile – pour les forces de l’ordre – est aujourd’hui l’installation d’un cheval de Troie ou keylogger (un enregistreur de frappes) sur les terminaux des suspects, smartphones, tablettes ou PC. Une opération toujours délicate puisqu’elle doit être effectuée à l’insu des utilisateurs.
« Whatsapp ou Viber commencent à être très utilisés par les criminels avec des mobiles jetables », nous avait confié le major Etienne Neff de la section de Paris. « Les criminels sont aujourd’hui plus sophistiqués et utilisent également des solutions payantes ». Les forces de l’ordre peuvent toujours accéder aux métadonnées fournies par les opérateurs mais il faut séparer le flux et le reconditionner pour le traiter.

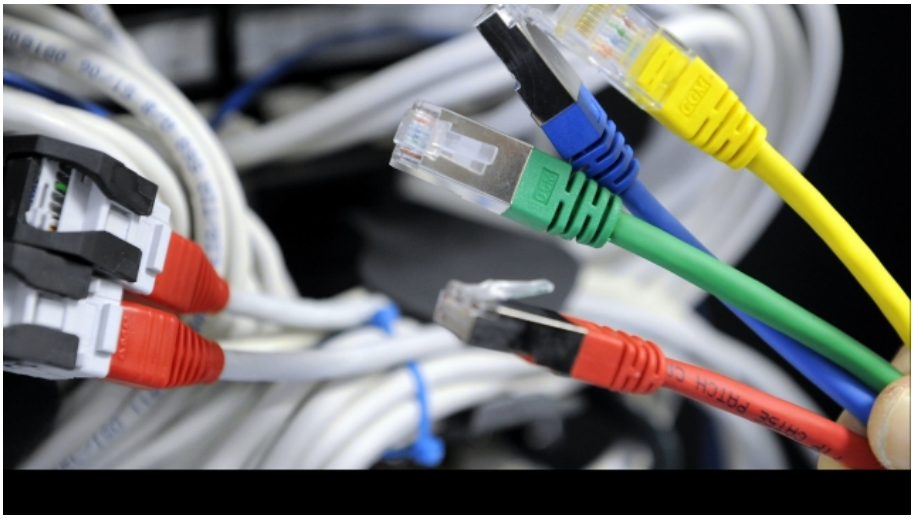
Les entreprises également sous surveillance

L’appel à plus de surveillance des échanges sur Internet est revenu sur le devant de la scène en Europe suite aux assassinats perpétués dans les bureaux du magazine satirique Charlie Hebdo et à l’épicerie HyperCacher à Paris. Après les deux attentats, les ministres de la Justice et de l’Intérieur de l’UE avaient publié une déclaration commune dans laquelle ils soulignaient qu’il est essentiel « d’entretenir une étroite collaboration avec les FAI pour endiguer la propagande terroriste en ligne ».
Si la Commission a refusé de commenter les plans anti-chiffrement de M. de Kerchove, le document fuité contient des détails supplémentaires comme le contrôle du « chiffrement décentralisé » des entreprises. Cela pourrait être une référence au chiffrement de bout-en-bout utilisé par certaines entreprises sensibles pour verrouiller leurs communications.

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

Source : http://www.lemondeinformatique.fr/actualites/lire-l-ue-doit-elle-obliger-les-geants-de-l-internet-a-ceder-leurs-cles-de-chiffrement-59993.html
Par Serge Leblal

France Télévisions et ses sites régionaux victimes d’une attaque informatique



France Télévisions et ses sites régionaux victimes d’une attaque informatique

Les sites régionaux et ultramarins de France Télévisions ont été victimes d’une cyber-attaque hier matin.
Vous êtes nombreux à vous en être aperçus : le site internet de France 3 Pays de La Loire ne fonctionnait pas normalement ce mercredi 21 janvier. Les serveurs informatiques qui hébergent les sites régionaux et ultramarins de France Télévisions en région parisienne ont en effet été victimes d’une cyberattaque durant la nuit de mardi à mercredi.

Après interventions des services techniques, les sites régionaux et ultramarins de France Télévisions ont retrouvé leur aspect normal en tout début de matinée. Il était en revanche impossible d’y publier des informations jusqu’à la fin du processus de mise à jour des protocoles de sécurité. Le problème est désormais résolu.

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

Source : http://france3-regions.francetvinfo.fr/pays-de-la-loire/2015/01/21/france-televisions-et-ses-sites-regionaux-victimes-dune-attaque-informatique-637201.html

Forum international de la Cybercriminalité: Bernard

Cazeneuve débloque 108 millions d’euros pour aider les enquêteursNicolas Messayaz / Sipa Olivier Aballain

Forum international de la Cybercriminalité: Bernard Cazeneuve débloque 108 millions d’euros pour aider les enquêteurs

Denis JACOPINI, expert judiciaire en informatique diplômé en Cybercriminalité, était présent ce mardi au 7eme Forum International de lutte contre la Cybercriminalité.

Le repérage et la traque des réseaux jihadistes sur internet sont au programme de Bernard Cazeneuve ce mardi: le ministre de l’Intérieur a ouvert à Lille le 7e Forum international de lutte contre la Cybercriminalité (FIC).
Le rendez-vous tombe à pic, puisque Manuel Valls lui-même a rappelé le 19 janvier sur i-Télé que «ce n’est pas dans les mosquées que ces recrutements [de djihadistes] s’organisent, c’est le plus souvent sur internet».
Après une rencontre avec le ministre de l’Intérieur allemand, Bernard Cazeneuve a prononcé un discours vers 10h au cours duquel il a annoncé le déblocage de 108 millions d’euros sur 3 ans pour développer les moyens des services de l’État pour l’enquête en matière de criminalité sur internet

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

Source : http://www.20minutes.fr/lille/1521015-20150120-direct-bernard-cazeneuve-forum-international-cybercriminalite
Par Olivier Abalain

Le Forum International de la Cybersécurité FIC 2015 en vidéo

Le Forum International de la Cybersécurité FIC 2015 en vidéo

« Nous sommes tous les vecteurs de cyberattaques » pour le fondateur du Forum de la cybercriminalité »

Le ministre de l'Intérieur Bernard Cazeneuve a inauguré mardi matin le Forum international de cybersécurité à Lille. Le général Marc Watin-Augouard, fondateur du Forum FIC et directeur du CREOGN, a expliqué que « nous sommes tous les vecteurs de cyberattaques, soit directes, soit par rebonds. »

Source vidéo : « Nous sommes tous les vecteurs de cyberattaques » pour le fondateur du Forum de la cybercriminalité

La cybersécurité au Grand Palais

Orange, cybersécurité et cyberdéfense

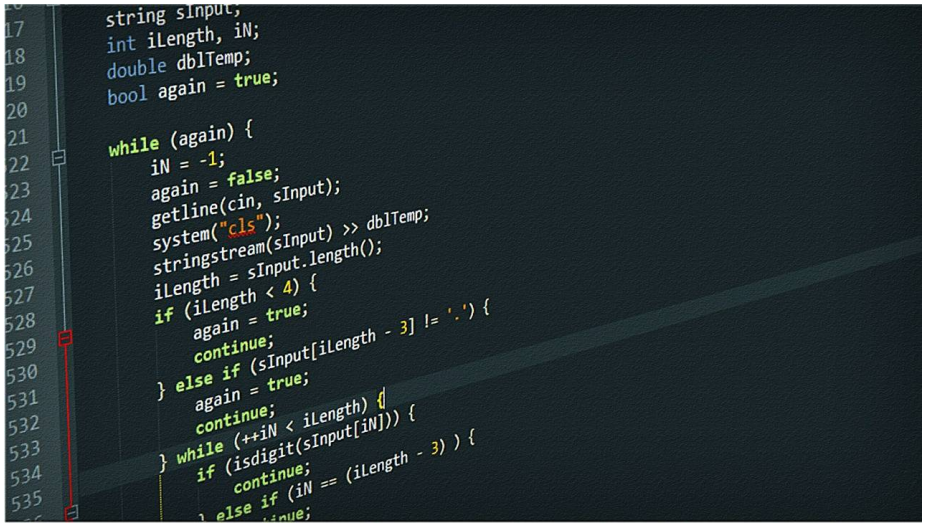
Le plateau TV pendant le Forum International de la Cybersécurité 2015 – FIC 2015
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://videos.tf1.fr/infos/2015/nous-sommes-tous-les-vecteurs-de-cyberattaques-pour-le-fondateur-8549855.html

---

Les pertes de données d'entreprise ont augmenté de

400 % depuis 2012



Les pertes de données d'entreprise ont augmenté de 400 % depuis 2012

Selon une étude menée dans une vingtaine de pays, les interruptions d'activité dues à la perte de données coûtent environ 1,5 milliard d'euros par an aux entreprises.

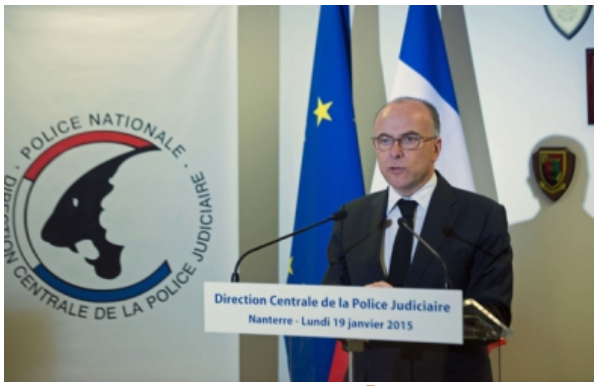
64 % des entreprises ont subi une perte de données ou une interruption d'activité en 2014. Un chiffre important qui en cache un autre : le nombre de données perdues a augmenté de 400 % depuis 2012 !
Selon une étude (1) réalisée auprès de 3 300 décideurs informatiques dans 24 pays (dont la France), ces interruptions d'activité non planifiées ont provoqué une perte de chiffre d'affaires (36 % des entreprises interrogées) et des retards dans le développement des produits (34 % des entreprises interrogées). Au total, les interruptions d'activité dues aux pertes de données coûtent plus d'1,7 milliard de dollars (environ 1,5 milliard d'euros) aux entreprises chaque année. « Cette étude souligne l'énorme impact budgétaire des interruptions d'activité non planifiées et de la perte de données dans les entreprises où qu'elles se trouvent » explique Chritian Hiller président EMC France.

Big data, mobilité et cloud hybride
A l'heure où les entreprises songent à externaliser leurs données dans les nuages, les décideurs informatiques reconnaissent les failles de leur stratégie : 51 % des entreprises interrogées ne disposent d'aucun plan de reprise après sinistre. Seules 6 % ont prévu un plan en environnement big data, mobilité et cloud hybride. Une très forte majorité des sondés (62 %) estime que ces trois environnements (big data, mobilité et cloud hybride) sont « difficiles » à protéger.
L'étude Vanson Bourne souligne enfin que c'est en Chine que l'on compte le plus grand nombre d'entreprises impliquées dans la protection de leurs données.
(1) Etude menée par le cabinet Vanson Bourne pour le compte de l'entreprise EMC.

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

Source : http://www.archimag.com/veille-documentation/2015/01/07/pertes-donn%C3%A9es-entreprise-augment%C3%A9-400-depuis-2012-0
Par Bruno Texier

1.300 cyberattaques « au nom d’organisations islamistes » radicales, annonce Bernard Cazeneuve



1,300 cyberattaques « au nom d’organisations islamistes » radicales, annonce Bernard Cazeneuve

Lors d’une visite à la sous-direction de lutte contre la cybercriminalité de la police judiciaire (PJ) française à Nanterre (Hauts-de-Seine), Bernard Cazeneuve a annoncé lundi que « plus de 1.300 attaques ont été revendiquées par des équipes (de) hackers se revendiquant d’organisations islamistes » radicales. Le ministre de l’Intérieur a également indiqué que plus de 25.000 sites français avaient été piratés.

La plateforme gouvernementale nationale Pharos, où sont signalés en France les contenus illicites liés à Internet, « a traité plus de 25.000 signalements de contenus illicites sur le net », a en effet déclaré Bernard Cazeneuve, évoquant des « cyberattaques malveillantes » sur des sites institutionnels et privés. Des « contact privilégiés » ont été noués avec Facebook, Dailymotion ou Google et des « demandes de retraits en ligne » ont eu lieu par exemple de sites ou vidéos « liés aux attaques terroristes ».

Des propositions mercredi

« La puissance publique doit prendre des initiatives et affirmer sa puissance pour protéger les internautes » face aux « menaces », a réaffirmé le locataire de la place Beauvau, « dans le respect des libertés publiques ».

Mercredi, à l’issue du Conseil des ministres, des mesures antiterroristes seront présentées par le gouvernement dont certaines visant Internet, a réaffirmé Bernard Cazeneuve. La semaine dernière, Manuel Valls lui avait demandé des propositions « dans les huit jours » concernant le contrôle d’Internet. « Elles devront concerner (…) les réseaux sociaux, plus que jamais utilisés pour l’embrigadement, la mise en contact et l’acquisition de techniques permettant de passer à l’acte », précisait alors le Premier ministre.

D’ici là, Bernard Cazeneuve se rend mardi à Lille pour le Forum international « sur la cybersécurité » en compagnie de son homologue allemand, Thomas de Maizière.

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

Source : http://www.lejdd.fr/Medias/Internet/1-300-cyberattaques-au-nom-d-organisations-islamistes-radicales-annonce-Bernard-Cazeneuve-713734

Mots de passe : « 123456 » toujours le plus utilisé

Mots de passe : « 123456 » toujours le plus utilisé

Les années passent et la situation reste la même : les internautes continuent à créer des mots de passe basiques et simples à deviner. Et pourtant, toutes les conditions sont réunies pour une prise de conscience avec la multiplication des fuites de données et leur médiatisation. Sans parler des discours martelés par les experts, eux-aussi de plus en plus diffusés sur les médias dits traditionnels.

Mais rien y fait : Mme Michu continue à protéger son client mail par le mot de passe ‘123456’. C’est le constat du traditionnel palmarès (Amérique du Nord et Europe de l’Ouest) des mots de passe les plus utilisés établi par Splashdata. En seconde place, on trouve le très complexe ‘password’. Les deux lauréats occupent les deux premières positions depuis maintenant trois ans, devant le plus compliqué à trouver… ‘12345’ ou encore ‘12345678’.
Onoubliera pas non plus le célèbre ‘qwerty’ ou ‘azerty’ pour les français qui rendent hilares les pirates de la planète. Petites nouveautés dans le Top 20, la présence de noms de superhéros comme superman ou batman, très utilisés par les fans de comics mais dont la protection est quasiment aussi nulle que les autres.

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

Source : http://www.zdnet.fr/actualites/mots-de-passe-123456-toujours-le-plus-utilise-39813303.htm