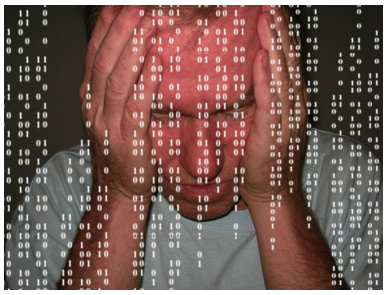
Le cybervandalisme envahit internet

	**Le cybervandalisme envahit internet**

Après le piratage du site de Sony Pictures et les cyberattaques de nombreux sites internet français, le piratage est de plus en plus présent sur internet. Depuis ces événements, on entend de plus en plus parler de « cyberguerre » ou de « cybervandalisme », mais qu'en est-il vraiment ? Voici quelques réponses.

Le « cybervandalisme » plutôt qu'une « cyberguerre »

Les Etats-Unis contre la Corée du Nord, les Anonymous contre l'Etat Islamique, on pourrait assimiler le piratage informatique à une sorte de guerre virtuelle tant les conséquences sont importantes. Le piratage de Sony Pictures a d'ailleurs pris une tournure politique : Barack Obama a pris officiellement la parole sur ce sujet et a préféré associer ce phénomène à du « cybervandalisme » et non à un acte de guerre. Le hacking de Sony Pictures a été conséquent puisqu'il a retardé la diffusion du film The Interview, une comédie à propos d'un complot fictif de la CIA pour assassiner le leader de la Corée du Nord Kim Jong-Un. De nombreuses informations privées ont également été dérobées.

La lutte contre les cyberattaques ne fait que commencer, mais des moyens sont mis en place pour éviter le piratage de nombreux sites internet ou comptes Facebook. Ce concept recoupe la réflexion sur la guerre économique et la stratégie d'intelligence économique, qui accordent, entre autres, une place prépondérante à la cybersécurité et transformation numérique. L'essentiel pour dominer aujourd'hui serait de posséder l'information, avant de posséder des territoires ; et le web est une mine d'or pour partir à la recherche de données confidentielles et capitales, que ce soit en politique ou pour le lancement d'un nouveau produit.

Comment se prémunir contre les cyberattaques ?

Au travers des entreprises attaquées, c'est tout un chacun qui peut être touché. En effet, le nombre de fraudes à la carte bancaire lors d'un achat sur internet a fortement augmenté ces dernières années. Les entreprises possédant des sites internet ou boutiques en ligne doivent les sécuriser au maximum afin d'éviter toute cyberattaque. Elles stockent et protègent les données personnelles des clients pour que les hackers ne puissent y accéder. Les pirates informatiques tentent en effet de dérober les codes bancaires des internautes par l'intermédiaire de cyberattaques.

Lorsque les internautes se retrouvent sur une boutique en ligne pour acheter un billet d'avion, une voiture ou des vêtements, ils doivent avoir la possibilité de payer en toute sécurité. Si ce n'est malheureusement pas toujours suffisant, plusieurs moyens de payement alternatifs ont été développés et sont mis à la disposition de tout acheteur, afin d'éviter de dévoiler les données personnelles de leurs cartes bancaires.

Plusieurs sites comme Paysafecard.com proposent des cartes prépayées pour faciliter les paiements en ligne. Il suffit de se créer un compte pour obtenir une carte de crédit prépayée qui se recharge à tout moment. Vous pouvez mettre le montant que vous désirez et payer en ligne sur des sites partenaires. Le système 3D Secure est également un bon moyen d'éviter tout piratage lors d'un paiement en ligne. Il vous permet même d'effectuer des achats rapidement sur la toile. Ces systèmes sont donc recommandés pour pallier les attaques des hackers à petite échelle.

Le meilleur moyen également de prévenir tout piratage est de choisir avec soin son mot de passe.

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

Source : http://www.archimag.com/vie-numerique/2015/01/29/fleau-cybercriminalite-comment-se-premunir

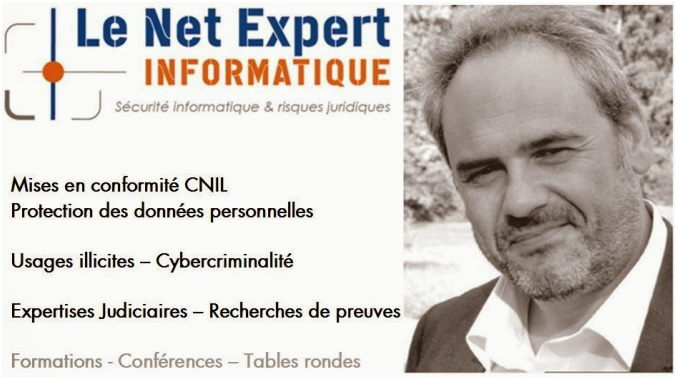
Prévenir les cyber-attaques avec Denis JACOPINI – Conférence le 10 février

	Prévenir les cyber-attaques avec Denis JACOPINI – Conférence le 10 février

La plateforme Initiative Cavare et Sorgues (ICS) accueille dans ses rangs un nouvel expert Denis JACOPINI, diplômé en droit de l'Expertise Judiciaire et en Cybercriminalité, pour sensibiliser les entreprises sur ce sujet d'actualité.

Les attaques informatiques ont toujours existé mais aujourd'hui elles sont très nombreuses.
En effet, que l'on soit une institution, une collectivité, un particulier ou une entreprise nous sommes tous des proies potentielles.
Que cela soit par méconnaissance des risques, sous-estimation des conséquences, ou bien par pure négligence, les faits sont là et nous sommes tous concernés. Piratage de serveurs, vol de données, arnaques financières en tout genre utilisant Internet… Le cyber-crime a couté plus de 327 milliards d'euros dans le monde en 2013.
Plus de 25 000 sites internet récemment défacés. Pourtant, il est possible d'enrayer ce phénomène qui semble incoercible.
Avec un peu de sensibilisation, beaucoup de bon sens et une information bien choisie, les chefs d'entreprises peuvent facilement reconsidérer l'importance de la sécurité numérique dans leurs priorités et ainsi rapidement repousser les principaux vandales du numérique.

« Nous accompagnons et finançons essentiellement des entreprises de moins de 10 salariés sur le territoire des 2 intercommunalités de l'Isle sur la Sorgue et de Cavaillon, quasiment toutes communique par l'intermédiaire entre autre d'un site internet, il nous a semblé important de les sensibiliser car il est possible d'enrayer ce phénomène » précise la directrice Anne-Laure STRETTI BOUSCARLE.
« Nous sommes très heureux que Denis JACOPINI viennent élargir les rangs des professionnels experts qui interviennent chez nous au même titre que les experts comptables, notaires, avocats, assureurs…et qu'il mette au service du plus grand nombre ses compétences pour les aider à lutter contre ces cyber-attaques».



Denis JACOPINI – Le Net Expert Informatique

Cet ancien chef d'entreprise Cavaillonnais d'une entreprise d'informatique, il a choisi après 17ans d'activité de se tourner vers son domaine de prédilection : l'expertise en sécurité informatique et en protection des données personnelles.
Diplômé en droit de l'Expertise Judiciaire et en Cybercriminalité il est à ce titre assermenté auprès des Tribunaux et spécialiste en sécurité informatique, en protection des données personnelles et en Informatique légale.
Il intervient auprès du Master II en Commerce électronique à l'Université d'Avignon, à l'Ecole de Formation des Avocats Centre Sud (EFACS), au CNFPT (Centre National de la Fonction Publique Territoriale) et est Formateur auprès de nombreux organismes dont des Centres de Gestion Agréés.
www.lenetexpert.fr

1ère session de sensibilisation le 10 février 2015 à 18 h30 dans les locaux d'ICS
Conférence débat au cours de laquelle seront évoquées les différentes techniques notamment celles qui consistent à détourner un site internet.
Inscription au préalable auprès de la plateforme
Pour vous inscrire :
Initiative Cavare et Sorgues
111 boulevard Paul Doumer 84300 CAVAILLON
Tel : 04 90 78 19 61

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

Source : Anne-Laure STRETTI BOUSCARLE

Denis JACOPINI Intervient au Salon du numérique 2015 le 3 février et coanime une conférence avec Orange

	Denis JACOPINI Intervient au Salon du numérique 2015 le 3 février et coanime une conférence avec Orange

10h00 – 10h45 – Cybercriminalité, protection des données personnelles et Réputation
Imaginez un instant que vous soyez consommateur. Vous découvrez soudain que vos données (coordonnées personnelles, bancaires ou encore médicales) se trouvent diffusées sur le net, sans votre accord, à cause de la négligence d'un professionnel.
Imaginez maintenant que ce professionnel c'est vous, malgré la mise en application imminente du projet de règlement Européen sur la Protection des données personnelles, le risque d'anéantir votre réputation et de vous sanctionner lourdement. Certes, le mal est fait mais pire, les Cybercriminels sauront en profiter !
Venez découvrir, comment ne pas être ce professionnel négligeant en protégeant le patrimoine le plus précieux de votre entreprise : Votre réputation
Présenté par Denis JACOPINI (Le Net Expert) et Eric Wiatrowsi d'Orange

Le 3ème Salon du Numérique en Vaucluse c'est Mardi 3 février 2015 de 9 h à 20 h à la salle polyvalente de Montfavet – Rue Félicien Florent, 84000 Avignon

Entrée libre, inscription obligatoire ! 600 m² – 35 stands – 16 conférences – Le rendez vous incontournable du numérique pour votre entreprise.

Entrée gratuite, inscription obligatoire
http://www.salon-du-numerique.fr/reservez-votre-place

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

Programme et infos pratiques : http://www.salon-du-numerique.fr/le-programme/

La CNDP va-t-elle finir par prendre le taureau par les cornes ?

	La CNDP va-t-elle finir par prendre le taureau par les cornes ?

Au Maroc, la loi 09-08 sur la protection des données à caractère personnel sur Internet enregistre encore des carences dans son application. En effet, tout le monde s'accorde à dire qu'il y a matière à faire et des lacunes sont encore à combler. Ce constat a été corroboré dans le dernier rapport de la Commission nationale de contrôle de la protection des données personnelles (CNDP).

Pour rappel, il y a quelques mois, cette dernière a commandité une opération de contrôle qui a concerné environ 104 sites web. Figuraient parmi les catégories de sites, ceux d'annonces, de voyage et d'hôtellerie, de cabinets de recrutement et d'emploi, de vente en ligne, de deals, de marketing, ainsi que des sites d'organismes publics, de banques, de transport et logistique, de santé, de télécoms et de location de voitures.
A travers cette campagne, il a ainsi été démontré que seulement 22% des sites web au Maroc affichent une mention relative à la protection des données personnelles conformément aux exigences de la loi.
C'est, en effet, grâce à cette campagne de contrôle qu'il a été également possible de constater que dans 28% des cas, la mention est présente, mais incomplète. Dans ce sens, la CNDP a précisé que 50% des sites contrôlés n'affichent pas de mention relative à la protection des données à caractère personnel.
Les résultats dudit contrôle ont ainsi dévoilé que très peu de sites web au Maroc (1%) se soucient de recueillir le consentement des internautes à collecter et traiter leurs données personnelles.
Dans la foulée, la commission a révélé que 71% des sites ne communiquent aucune «information sur l'identité du responsable du site web, les finalités du traitement, les destinataires des données collectées et autres renseignements ». Elle a, aussi, précisé que même pour le reste des sites (29 %), lesdites informations ne sont que partielles. Et d'ajouter qu'en matière de «demande de consentement des internautes à collecter et traiter leurs données personnelles», tandis que 80% des sites web ne l'évoquent pas, cette demande est même aléatoire pour 19%.
Le rapport fait état aussi des internautes qui sont, somme toute, privés de leurs droits. En effet, les résultats obtenus sont loin d'être reluisants en montrant que les internautes sont privés de l'exercice de leurs droits d'accès, de rectification et d'opposition auxquels la loi accorde pourtant une importance particulière. De ce fait, ces droits ne sont malheureusement pas assurés par l'écrasante majorité des sites web au Maroc, à savoir 95%. En ce qui concerne l'hébergement des sites à l'étranger (transfert de données personnelles à l'étranger), il est constaté qu'aucun des sites concernés n'a obtenu l'autorisation requise auprès de la CNDP.
Toujours est-il, ce contrôle a permis de porter sur le haut du pavois d'autres irrégularités qui concernent le principe de proportionnalité (collecte excessive de certaines données et injustifiée par le traitement) ainsi que les règles de la prospection directe et l'utilisation des cookies.
Ce faisant, la CNDP a décidé de prendre les mesures légales qui s'imposent à l'encontre des différents responsables de traitements qui ne procèdent pas à la mise en conformité de leur site web. Même si ces procédures disciplinaires peuvent déboucher sur un avertissement, un avertissement public, un blâme, voire le transfert du dossier à la justice, elles ne sont pas pour effaroucher certains, loin de vouloir se mettre au diapason de la loi n° 09-08.
Et sachant que dans l'article premier de cette dernière, il y est clairement stipulé que l'informatique est au service du citoyen (…), qu'elle ne doit pas porter atteinte à l'identité, aux droits et aux libertés collectives ou individuelles de l'Homme et qu'elle ne doit pas constituer un moyen de divulguer des secrets de la vie privée des citoyens, c'est dire qu'au Maroc, l'application de la présente loi traîne encore le pas.
D'où l'importance de susciter le débat qui aura donc le mérite de discuter des questions que soulève réellement cette loi.
Dans ce sens, l'AMISE (Association marocaine des Instituts de sondages et études de marché) co-organise une conférence-débat en collaboration avec la Fédération de commerce et de service de la CGEM et qui aura lieu dans la matinée de demain mercredi, au siège de la CGEM à Casablanca. Cette rencontre sera animée par la responsable de la communication de la CNDP, et a pour objectif premier de permettre aux participants de mieux comprendre les tenants et aboutissants de la loi 09-08 et d'examiner l'applicabilité de certaines dispositions de cette loi aux études de marché et sondages d'opinion, ainsi que leurs impacts sur les relations entre les instituts d'études et leurs clients.

Pour rappel, Denis JACOPINI, spécialisé en protection des données personnelles est mobile et disponible pour venir assurer des actions de mise en conformité ou de supervision de mise en conformité des traitements informatiques par rapport aux mesures de sécurité à mettre en place pou rassure rune meilleure sécurité et protection des données à caractère personnel.

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

Source : http://www.libe.ma/La-CNDP-va-t-elle-finir-par-prendre-le-taureau-par-les-cornes_a58378.html
Par Meyssoune Belmaza

Les entreprises doivent construire un modèle d'exploitation de leurs données

Les entreprises doivent construire un modèle d'exploitation de leurs données

Face au Big Data, monétisation, confidentialité et gouvernance sont au menu des préoccupations des entreprises françaises en 2015.

En 2014 déjà, 43% des décideurs français interrogés considéraient la gestion des données et leur analyse comme une priorité selon une étude réalisée par MARKESS*. Aujourd'hui, les directions générales de nombreuses entreprises françaises le clament : l'année 2015 sera l'année du Big Data. Dans le rapport Data & Analytics Trends 2015 élaboré par le cabinet Deloitte, ces dernières voient en effet se dessiner un grand potentiel économique derrière la masse de données qu'elles génèrent. Les sociétés ressentent le besoin d'analyser les données qu'elles collectent pour créer de la valeur : anticiper des événements futurs, gérer les ressources, limiter les risques voilà autant de finalités à l'exploitation de ces données pour l'entreprise. Reste à savoir comment les exploiter au mieux. Et les solutions technologiques ne manquent pas.

En milieu hospitalier notamment, où l'expérience du patient occupe une place centrale, rassembler des données, sous la forme d'un tableau de bord offrant une visualisation modulable de l'information, sur les temps d'attente des patients ou encore les facteurs d'attribution d'une chambre, peuvent permettre au personnel infirmier, aux médecins et aux administrateurs d'optimiser leur capacité de traitement des patients, note Edouard Beaucourt, account manager chez Tableau Software.

L'Open Data, soit le partage de données, reçoit un écho favorable auprès des acteurs du secteur privé et ceci à des fins d'amélioration de la qualité des services offerts. Deloitte constate d'ailleurs une recrudescence des actions collaboratives entre les sociétés et leurs partenaires en matière de partage de données. Et plusieurs discussions naissent autour de la création de centres de partage de données inter-entreprises. Ce processus de démocratisation du partage de données encore faiblement structuré est amené à se rationaliser selon Reda Gomery, spécialiste des données et de l'analyse de données chez Deloitte, auteur de l'étude.

Preuve de l'émergence d'une collaboration accrue entre les parties prenantes, Deloitte relève le projet d'une compagnie d'assurance, l'«hackathon », compétition ouverte aux développeurs de tous horizons. Leur mission consiste à réfléchir à de nouvelles applications de scoring des clients de l'entreprise à partir de données qui leur sont confiées.

Il est d'usage de dire que les crises s'accompagnent souvent d'un regain de créativité. Raison pour laquelle les entreprises cherchent une monétisation adéquate de leurs données. Les secteurs des télécoms et des services financiers ont été d'ailleurs été pionniers dans le développement de services de vente de données.
Deloitte met en avant dans son rapport l'initiative d'un opérateur téléphonique qui d'après les données fournies par ses antennes relais a su analyser la fréquentation de sites touristiques par des visiteurs étrangers, données qui ont pu être vendues par la suite à des offices de tourisme, générant ainsi de nouveaux revenus pour l'entreprise.

En 2015, les entreprises réalisent complètement la valeur des informations qu'elles possèdent pour les acteurs avec qui elles interagissent et expérimentent de nouveaux modèles. Non sans interrogations sur la confidentialité de ces données. Se pencher sur les modèles de protection pour sécuriser l'information et préserver l'anonymat des clients conduit à son corollaire : le mode de gouvernance. Les entreprises se préoccupent en effet également de chercher le cadre le plus adapté pour maîtriser ses flux gigantesques et continus d'informations.

*Etude MARKESS : Meilleures approches pour tirer parti du Big Data, France, 2014

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

Source : http://www.atelier.net/trends/articles/entreprises-doivent-construire-un-modele-exploitation-de-leurs-donnees_433304

Sénégal: La CDP continue son éducation des jeunes sur l’importance des données personnelles – Afrique IT News Afrique IT News

Sénégal: La Commission de protection des données personnelles continue son éducation des jeunes sur l’importance des données personnelles

La Journée internationale de protection des données personnelles est une initiative mondiale célébrée le 28 janvier de chaque année.

À l’instar de plusieurs autres entités de protection des données personnelles à travers le monde, au Sénégal la Commission de protection des données personnelles (CDP) compte célébrer cette journée ce mercredi sur le thème : ‘’Loi n° 2008-12 du 25 janvier 2008 sur les données à caractère personnel’’, 7 ans après : quel bilan ?’’ en recevant les étudiants des grandes écoles autour d’une table ronde.
Cette journée coïncide à quelques jours près avec la célébration de l’anniversaire de l’adoption des textes de loi sur les données personnelles. Un communiqué reçu par l’Agence de Presse Sénégalaise indique que cette rencontre est une excellente opportunité pour les acteurs du secteur de faire le bilan de l’état de la protection au Sénégal 7 ans après le vote de ladite loi.
Conformément à la loi n° 2008-12 du 25 janvier 2008 qui concerne la protection des données à caractère personnel, les missions assignées à la Commission de Protection des Données Personnelles (CDP) sont la veille, la sensibilisation, le contrôle et l’investigation.

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

Source : http://www.afriqueitnews.com/2015/01/27/senegal-cdp-continue-education-jeunes-limportance-donnees-personnelles/

La protection des données personnelles, un marché juteux en Suisse

La protection des données personnelles, un marché juteux en Suisse

«Données 100% stockées en Suisse.» De plus en plus d'entreprises mettent en avant sur leur site ce petit macaron aux couleurs de la Confédération helvétique, qui pourrait faire de la protection des données personnelles une nouvelle source de prospérité du pays. «Les données sont le nouvel eldorado de la Suisse. C'est un vrai boom», se réjouit ainsi Franz Grüter, directeur général de Green.ch, l'une des principales entreprises suisses spécialisées dans le stockage de données personnelles, qui connaît une croissance annuelle de 30%.

Les scandales d'espionnage généralisé à la suite des révélations de l'ex-conseiller de l'Agence nationale de sécurité (NSA) américaine Edward Snowden ont permis une prise de conscience accrue, notamment du côté des entreprises, sur la nécessité de protéger ses données personnelles et dont la Suisse compte bien tirer parti. «Les clients ont besoin de confiance, de discrétion, de fiabilité et de stabilité. Or ce sont les caractéristiques de ce pays depuis toujours», ajoute Franz Grüter, selon qui plus d'un milliard de francs (1 milliard d'euros) ont été investis ces cinq dernières années dans des centres de données informatiques du pays.

De la Silicon Valley à Zurich

«Un Etat offrant un niveau de protection élevé à ses entreprises leur offre également des avantages économiques non négligeables», estime pour sa part Jean-Philippe Walter, adjoint au Préposé fédéral à la Protection des données et à la transparence. Et avec 61 centres de données sur les 1.151 situés dans l'Union européenne (selon le site datacentermap), la Confédération se classe aujourd'hui à la cinquième place européenne. Le contexte juridique est d'ailleurs très favorable à la Suisse : sa loi sur la protection des données, l'une des plus restrictives au monde, empêche toute administration d'avoir accès à des informations personnelles sans l'autorisation d'un juge.

La Suisse utilise les anciens bunkers de la guerre froide comme coffre-fort numérique.
Ici, celui situé près d'Attinghausen, repère de la société Deltalis dont le code GPS est tenu secret.

En conséquence, certaines entreprises étrangères n'hésitent pas à se relocaliser en Suisse. C'est le cas de Multiven, l'un des leaders mondiaux de la maintenance des réseaux Internet, qui a quitté la Silicon Valley californienne pour Zurich en 2009. «Nous prévoyons un avenir dans lequel les individus, les entreprises et les organisations du monde entier chercheront à stocker leurs actifs numériques (propriété intellectuelle, inventions, secrets commerciaux…) en Suisse pour transformer le pays de sanctuaire d'actifs physiques (espèces, or, art) en sanctuaire d'actifs numériques, estime sa présidente, Deka Yussuf pour qui la majorité des actifs qui seront enregistrés en Suisse seront numériques d'ici les 25 prochaines années.

Se positionner avant la nouvelle législation européenne

Ainsi, il s'avérerait que les récentes observations faites par le Premier ministre britannique David Cameron et le président américain Barack Obama souhaitant interdire le chiffrement, inaccessible pour leur gouvernement, seraient impensables en Suisse.

Un pays qui suit désormais de près la réforme du régime européen de protection des données personnelles, qui devrait voir le jour d'ici quelques semaines. Ce nouveau cadre renforcerait la législation sur le traitement des données personnelles des citoyens européens par les entreprises et ce, indépendamment de leur localisation géographique et de leur taille. La problématique du stockage des données deviendra alors centrale en Europe; à la Suisse de se positionner en conséquence.

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

Source : http://www.20minutes.fr/monde/1524251-20150123-suisse-protection-donnees-personnelles-marche-juteux
Illustration : Sébastien SALOM

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

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

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