Que risquez-vous si vous égarez une clé USB, un disque dur, ou si on vous vole les données de votre entreprise ?

Que risquez-vous si vous égarez une clé USB, un disque dur, ou si on vous vole les données de votre entreprise ?

Si votre système informatique se fait pirater (comme l'ont été les sites Internet de SONY, Orange, Google, Bercy, le ministère des Finances…), les auteurs de l'attaque ne sont pas les seuls à être inquiétés d'une telle fuite. Les responsables du traitement peuvent en effet avoir à fournir quelques explications à la CNIL. Même sanction, si vous perdez votre clé USB, disque dur externe ou pire, votre ordinateur portable. Et pour cause, si vous manipulez des données qui permettent d'identifier une personne, communément appelées des données personnelles), vous êtes tenus à une série d'obligations de sécurité afin d'éviter la violation de données à caractère personnel (destruction, perte, altération, divulgation, accès non autorisé).

L'article 34 bis de la loi Informatique et Libertés les oblige par exemple à avertir sans délai la CNIL et à tenir à jour un registre des incidents. En principe, les particuliers, victimes collatérales de cette faille, doivent également être informés sans délai, sauf si la CNIL « a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation ». En clair, pas d'alerte direct des clients si les rustines ont été correctement appliquées.

Plus globalement, l'article 34 de la loi Informatique et Libertés impose au responsable d'un traitement de prendre toutes précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Évidemment, cette protection diffère selon la nature des données et des risques présentés par le traitement.

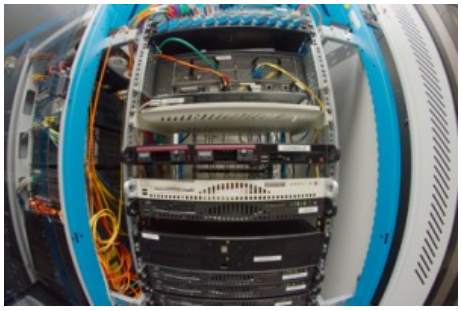
Enfin, selon l'article 226-17 du Code pénal, le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.

Etonnant non ?

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

Source : http://www.nextinpact.com/news/91600-un-partenaire-tf1-pirate-quelles-consequences-juridiques.htm
Extrait de Marc Rees adapté par Denis JACOPINI

Assurer la sécurité informatique et la sauvegarde des données

	Assurer la sécurité informatique et la sauvegarde des données

Cyber-attaques, vols ou incendies… Garantir la protection des données numériques, notamment à caractère personnel, devrait être une priorité pour les collectivités.

Insultes à l'encontre de la France mais aussi des États-Unis et d'Israël : le 24 janvier 2023, au lieu d'accéder au site internet de la ville de Fruges (62), c'est ce type de message que les internautes découvrent. Plus tôt dans le mois, c'est le site de l'office de tourisme du Sancerrois qui était victime d'un piratage entraînant la suppression de l'agenda des animations et un surcroît de travail pour les agents.
« Partout en France les collectivités, insuffisamment protégées, sont visées par des cyber-attaques. Or elles les décrédibilisent et peuvent avoir des conséquences très graves », constate le commandant Rémy Février, ancien chargé de mission intelligence économique à la région de gendarmerie Nord-Pas-de-Calais(1). Selon lui, la commune est l'échelon territorial le plus fragile, détenant beaucoup de données sensibles avec de faibles moyens de protection.

Courriels contaminés
Les sites internet sont souvent une voie royale pour les hackers. « Si l'arborescence n'a pas été verrouillée, il est facile de remonter à l'ensemble du système d'information et d'accéder aux fichiers et aux mots de passe », met en garde Rémy Février. Les pirates peuvent aussi prendre le contrôle d'ordinateurs via des virus « troyens » contractés par des courriels ou des sites web contaminés.
« La récupération illicite d'informations est un enjeu majeur de nature à induire des répercussions civiles et pénales pour les élus locaux. Les vols de données à caractère personnel peuvent par exemple conduire à des vols d'identité », précisent le « cyber-gendarme » qui déplore le manque de statistiques fiables sur ces sujets.

Plan de continuité
Avec le développement de l'e-démocratie, de l'e-administration ou de la dématérialisation des appels d'offres, le « cyber-risque » est multiplié. « Qu'est ce qui empêchera demain une entreprise d'aller voir frauduleusement l'offre de ses concurrents ? » s'interroge Rémy Février.
En dehors de la malveillance, la simple sécurisation des données numériques est problématique. Incendie, inondation, explosions, vols… « Je recueille beaucoup de témoignages d'élus ayant perdu tout ou partie de leurs données », constate Maurice de Bosscher, responsable technique au centre de gestion du Nord.
« Pour une remise en route rapide en cas de sinistre, il est impératif de posséder des sauvegardes hors site. La collectivité doit prévoir un plan de continuité d'activité englobant ses systèmes d'information. C'est encore trop peu souvent le cas », insiste Rémy Février.

Trois conseils

Développer une culture de la sécurité
« Le bon sens prévient 80 % des problèmes : ne laissons pas le mot de passe visible, vidons de leurs données les ordinateurs avant de s'en débarrasser », dit Rémy Février, chargé de mission intelligence économique. Il s'agit de créer une culture de la sécurité des systèmes d'information à tous les niveaux et de former le personnel, avec des élus moteurs.
Dans chaque collectivité, un correspondant responsable de la sécurisation du réseau à intérêt de se rapprocher des services de l'État pour bénéficier d'informations récentes et de formations spécifiques. Il peut aussi trouver appui auprès de l'Agence nationale de la sécurité des systèmes d'information (Anssi).
« On ne peut faire l'économie d'une charte définissant le bon usage des systèmes d'information, ce qu'il est possible ou non de faire, et cependant 90% des communes n'en possèdent toujours pas, assure en outre Hervé Fortin, responsable sécurité des systèmes d'information du conseil général (CG) de l'Aisne qui conseille d'intégrer dans le plan de sécurisation les recommandations du référentiel général de sécurité (RGS) et de la Cnil.

Connaître son parc et sécuriser l'intégrance
Un schéma directeur informatique recensant matériel et câblages permet une remise en route rapide. « Sans cela, un simple dysfonctionnement peut prendre des proportions fâcheuses », explique Rémy Février. Choisir de faire suivre son matériel en intégrance implique d'obtenir un maximum de garanties sur la sécurité offerte par le prestataire, avec clauses de confidentialité et vérification de la qualité du service.
« Il est utile de s'appuyer sur les services des renseignements généraux pour bénéficier de leurs connaissances », conseille Johann Protin, responsable sécurité des systèmes d'information du conseil général des Hauts-de-Seine.

Sécuriser les postes nomades
« Les outils nomades multiplient les risques de vols et de pertes de données. Il est préférable d'équiper les collaborateurs de terminaux fournis par la collectivité et de les former au risque », conseille Hervé Fortin.
Des outils facilitent la sécurité : chiffrement des données ou une clef USB de type ID. Dotée d'un mot de passe, elle contient les applications nécessaires et crée sur le disque dur de l'ordinateur d'accueil une zone mémoire temporaire sécurisée sur laquelle il ne reste aucune trace une fois la clef ôtée.

Systèmes d'information : la responsabilité pénale des élus
Avoir insuffisamment protégé ses systèmes d'information peut entraîner la mise en examen des élus responsables.
Les élus peuvent par exemple être mis en cause si des sites illégaux sont consultés alors qu'aucune mesure de restriction d'accès à internet n'a été mise en place. « La réglementation dans ce domaine est jurisprudentielle et il ressort clairement de cette jurisprudence qu'un élu, au même titre qu'un chef d'entreprise, peut être mis en examen pour ne pas s'être suffisamment protégé », met en garde Rémy Février, chargé de mission intelligence économique, qui estime que la majorité des élus ne connaissent pas les responsabilités qui leur incombent.
« Même si l'élu délègue un responsable sécurité des systèmes d'informations, la responsabilité de protéger les données, notamment celles à caractères personnelles, reste au final de son ressort », insiste-t-il.
Au-delà de ces aspects juridiques, les élus ont la responsabilité de protéger la nouvelle valeur publique qu'est la « cyber-confiance ».
« Il existe une responsabilité collatérale des élus en cas de rupture des activités numériques ; la plupart n'en sont pas conscients », estime Richard Ekiznwski, le conseiller communautaire délégué à la prévention des risques de Lille métropole.

Centre de gestion du Nord : un coup de pouce pour les petites collectivités
Ordinateur infecté par des virus troyens, PC volés ou endommagés par une inondation. Nous constatons tous les jours que les communes ne sont pas assez protégées », explique Maurice de Bosscher, responsable technique de Creatic.
Le centre de ressources du centre de gestion (CDG) du Nord, créé en 2000, épaule les collectivités en matière de nouvelles technologies de l'information et de la communication. « Nous avons créé une plate-forme d'échange pour faciliter la dématérialisation. Pour qu'elle fonctionne de façon sécurisée, il faut auparavant résoudre les problèmes de sécurité de base », constate Maurice de Bosscher, ajoutant que dans le département, plus de 500 collectivités n'ont pas de responsable informatique.

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

Source : http://www.courrierdesmaires.fr/61602/dossier-la-securite-informatique-et-la-sauvegarde-des-donnees/

Protection des données : le Cese préconise un renforcement de l’éducation au numérique

Protection des données : le Cese préconise un renforcement de l’éducation au numérique

Dans un avis adopté à l'unanimité le 13 janvier intitulé « Données numériques : un enjeu d'éducation et de citoyenneté », le Conseil économique social et environnemental (Cese) appelle le gouvernement à déclarer l'éducation au numérique pour tous grande cause nationale 2016.

Une prise de position qui arrive en pleine actualité sur fond de terrorisme, mais aussi dans le contexte de l'affaire Prisme qui met en accusation les agences américaines du renseignement sur la surveillance des citoyens, des entreprises et des Etats. Elle relance le débat sur la question des données et des équilibres à établir entre leur bonne exploitation par tous dans une optique d'intérêt général et la protection des libertés individuelles.
Les opportunités du numérique sont considérables. La multiplication des données statistiques, des échanges collaboratifs dans le monde, a fait sensiblement progresser la recherche sur le traitement de certaines maladies. Les villes sont désormais mieux à même de gérer l'espace public, l'énergie ou la mobilité des citoyens. L'éducation bénéficie d'un immense apport de connaissances. « Mais dans le même temps, les sujets relatifs à la protection de la vie privée et le risque que ces données révèlent une partie de nous-mêmes et de notre vie privée montrent aussi qu'il y a danger », tempère Eric Peres, le rapporteur de la section de l'éducation, de la culture et de la communication du Cese qui présentait le projet d'avis en assemblée plénière.

En mettant l'accent sur ce sujet, le Cese « ne veut pas stigmatiser, mais plutôt contribuer à mieux gérer le déluge de données numériques à la fois pour en faire des opportunités d'intérêt général et aussi protéger les citoyens ».

Dans cette perspective, l'avis met l'accent sur quelques préconisations prioritaires.
L'école reste un lieu sensible à la fois « pour faire de l'information numérique un véritable outil de savoir et permettre dès le plus jeune âge d'apprendre à maîtriser l'usage des outils et aussi celui des données personnelles numériques ». Le Cese reprend pour l'essentiel des propositions déjà formulées dans d'autres instances, notamment la généralisation du brevet informatique (B2i) ou encore, dans l'enseignement supérieur, l'augmentation du volume d'heures d'informatiques dans les classes préparatoires scientifiques et le développement de formations spécialisées autour de la donnée (data scientist, data broker).

Co-régulation des données personnelles dans les villes
L'entreprise et l'administration ont aussi rôle à jouer, mais cette fois, dans la « gestion éthique des données ». En assurant des pratiques « loyales, licites, transparentes et encadrées », elles amélioreraient leur image vis à vis du public et pourraient en tirer quelque avantage. Le rôle du correspondant informatique serait sensiblement renforcé. Par ailleurs, les membres du conseil recommandent un encadrement plus strict de la gestion des données transmises par les objets connectés « en faisant de la protection un réglage par défaut ». Ils militent également « pour un droit des citoyens au silence des puces » et souhaitent la généralisation du consentement préalable de l'usager (Opt-in) pour l'exploitation des données personnelles.
Pour tout cela, une régulation normative est nécessaire. Aussi le conseil réaffirme-t-il son soutien à la sortie du projet de règlement européen sur la protection des données. Au niveau national, il préconise un renforcement de la Cnil, notamment à travers son pouvoir de sanction financière. Et il encourage aussi des voies plus originales « permettant de rendre aux individus le contrôle de l'utilisation de leurs propres données ».
A cette fin il propose la création de plateformes publiques assurant la gestion de données sensibles telles que les données de santé. Au niveau local, il suggère même la mise en place de solutions de co-régulation à travers des régies locales jouant le rôle de tiers de confiance. Elles seraient chargées de conserver et de gérer les données personnelles, utiles par exemple à l'amélioration des services d'une ville. Les citoyens accepteraient de mettre en commun leurs données dans le cadre de projets d'intérêt général, sur la base d'une gouvernance solidaire et coopérative.

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

Source :
http://www.localtis.info/cs/ContentServer?pagename=Localtis/LOCActu/ArticleActualite&jid=1250268282051&cid=1250268279645
Par Philippe Parmantier / EVS

La Cnil lance un nouveau label sur la gestion des données

La Cnil lance un nouveau label sur la gestion des données

Face à la prolifération des données qu'une entreprise a à gérer et à la complexité réglementaire qui l'accompagne, la Cnil lance un nouveau label visant à prouver la conformité de sa gouvernance.

Garantir à ses clients que l'on est conforme aux bonnes pratiques de la Cnil en matière de gestion des données personnelles, c'est l'objet de ce nouveau label « Gouvernance Informatique et Libertés » dévoilé par la Commission. Après les labels « formation », « procédure d'audit » et « coffre-fort numérique », la Cnil veut maintenant donner au Correspondant Informatique et Libertés (Cil) un autre moyen d'améliorer la gestion.
Pour rappel, le Cil est depuis 2005 la personne intermédiaire entre une entreprise et la Cnil. Du coup, ce nouveau référentiel s'adressera forcément aux organisations possédant un tel référent (plus de 10 000 à ce jour). La création de ce nouveau label est partie du constat du régulateur que les entreprises et organismes publics avaient de plus en plus besoin « d'identifier clairement les procédures à mettre en place pour une bonne gestion des données personnelles ». Pour y prétendre, 25 exigences (.rtf) ont été définies par la Cnil.
Celles-ci sont organisées en trois thématiques : l'organisation interne liée à la protection des données, la méthode de vérification de la conformité des traitements à la loi Informatique et Libertés et la gestion des réclamations et incidents. Pour le régulateur, ce label témoignera « de la volonté de l'organisme d'innover et de traiter les données personnelles de manière responsable » et constituera donc un atour pour ses clients.

Tous les organismes, publics ou privés ayant désigné un correspondant informatique et libertés peuvent prétendre à ce label.
Téléchargez le dossier de candidature
Une fois complété, envoyez le dossier
soit par le biais du formulaire de dépôt en ligne
soit par courrier postal (CNIL, 8 rue Vivienne, CS30223, 75083 paris Cedex 02)

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

Source : http://pro.clubic.com/legislation-loi-internet/donnees-personnelles/actualite-749887-cnil-gestion-donnees-personnelles-entreprise.html

Obama cherche à renforcer la protection des données personnelles

	Obama cherche à renforcer la protection des données personnelles

Face au nombre record de piratages sur le sol américain en 2014 et aux milliers de données personnelles lâchées dans la nature, Barack Obama a présenté un panel de lois destinées à renforcer la cyber-sécurité des entreprises et à réguler leur comportement.

2014 se traduit par un nombre record de cyber attaques ayant ciblé plusieurs grandes entreprises, dont Target, Home Depot, Staples et bien sûr Sony. Ajoutons à cela que près de la moitié des adultes américains se serait fait hacker en 2014. A tel point que CNN est allé jusqu'à développer un outil, "What hackers know about you ?" (Que savent les hackers sur vous ?). Celui-ci renseigne l'utilisateur sur ses données potentiellement menacées selon les entreprises dont il est client. Rien de rassurant, donc.

Citant un récent sondage selon lequel 91% des américains ont aujourd'hui le sentiment d'avoir perdu le contrôle sur leurs données personnelles, le président Barack Obama a proposé la mise en place d'un Personal Data Notification & Protection Act.

Premier objectif : harmoniser la législation au niveau fédéral et fixer aux entreprises un délai maximum de 30 jours pour avertir leurs clients en cas de piratage de leurs données privées. A l'heure actuelle, 47 lois étatiques différentes légifèrent sur la question. En fonction de l'Etat dans lequel il vit, un citoyen peut donc être averti ou non en cas de problème.
Le second projet de loi est spécifiquement consacré aux étudiants. Inspiré d'une loi californienne promulguée l'an dernier, le Student Digital Privacy Act interdirait aux entreprises de vendre les données d'étudiants dans un but non-éducatif. A l'heure où tablettes et ordinateurs portables se généralisent dans les salles de classe, de plus en plus de données sont collectées, et parfois vendues à des publicitaires ou des institutions financières. Cette loi vise à éviter que les données des étudiants ne soient utilisées de manière déloyale par leurs futurs employeurs ou banquiers. Une charte circule déjà parmi les entreprises à cet effet, et 75 sociétés l'auraient déjà signée (dont Apple et Microsoft). Les entreprises assurant un service éducatif qui ne signeraient pas cet engagement pourraient être dépossédées de leur mission.
Enfin, le chef de l'Etat a également proposé la mise en place d'une déclaration des droits à la vie privée du consommateur, le Consumer Privacy Bill of Rights, qui donnerait à celui-ci la possibilité de décider quelles données personnelles sont collectées et comment elles sont utilisées. La cyber-sécurité des entreprises détenant des données personnelles serait également renforcée. « Plus nous protégerons les données des consommateurs, plus il sera difficile pour les hackers de frapper nos entreprises et d'affaiblir notre économie. » a affirmé Barack Obama. Aux entreprises également de renforcer leurs systèmes. Sony par exemple, dont la console de jeux Playstation Network a été piratée pendant Noël, promet des investissements importants dans des serveurs et des techniciens capables de les gérer en cas d'attaques.

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

Source : http://www.atelier.net/trends/articles/obama-cherche-renforcer-protection-donnees-personnelles_433077

Que risquez-vous vous égarez une clé USB, un disque dur, ou si on vous vole les données de votre entreprise ?

Que risquez-vous vous égarez une clé USB, un disque dur, ou si on vous vole les données de votre entreprise ?

Si votre système informatique se fait pirater (comme l'ont été les sites Internet de SONY, Orange, Google, Bercy, le ministère des Finances…), les auteurs de l'attaque ne sont pas les seuls à être inquiétés d'une telle fuite. Les responsables du traitement peuvent en effet avoir à fournir quelques explications à la CNIL. Même sanction, si vous perdez votre clé USB, disque dur externe ou pire, votre ordinateur portable. Et pour cause, si vous manipulez des données qui permettent d'identifier une personne, communément appelées des données personnelles), vous êtes tenus à une série d'obligations de sécurité afin d'éviter la violation de données à caractère personnel (destruction, perte, altération, divulgation, accès non autorisé).

L'article 34 bis de la loi Informatique et Libertés les oblige par exemple à avertir sans délai la CNIL et à tenir à jour un registre des incidents. En principe, les particuliers, victimes collatérales de cette faille, doivent également être informés sans délai, sauf si la CNIL « a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation ». En clair, pas d'alerte direct des clients si les rustines ont été correctement appliquées.
Plus globalement, l'article 34 de la loi Informatique et Libertés impose au responsable d'un traitement de prendre toutes précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Évidemment, cette protection diffère selon la nature des données et des risques présentés par le traitement.
Enfin, selon l'article 226-17 du Code pénal, le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Etonnant non ?

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

Source : http://www.nextinpact.com/news/91600-un-partenaire-tf1-pirate-quelles-consequences-juridiques.htm
Extrait de Marc Rees adapté par Denis JACOPINI

Un partenaire de TF1 piraté, quelles conséquences juridiques ? – Next INpact

Que risquez-vous vous égarez une clé USB, un disque dur, ou si on vous vole les données de votre entreprise ?

Si votre système informatique se fait pirater (comme l'ont été les sites Internet de SONY, Orange, Google, Bercy, le ministère des Finances…), les auteurs de l'attaque ne sont pas les seuls à être inquiétés d'une telle fuite. Les responsables du traitement peuvent en effet avoir à fournir quelques explications à la CNIL. Même sanction, si vous perdez votre clé USB, disque dur externe ou pire, votre ordinateur portable. Et pour cause, si vous manipulez des données qui permettent d'identifier une personne, communément appelées des données personnelles), vous êtes tenus à une série d'obligations de sécurité afin d'éviter la violation de données à caractère personnel (destruction, perte, altération, divulgation, accès non autorisé).

L'article 34 bis de la loi Informatique et Libertés les oblige par exemple à avertir sans délai la CNIL et à tenir à jour un registre des incidents. En principe, les particuliers, victimes collatérales de cette faille, doivent également être informés sans délai, sauf si la CNIL « a constaté que des mesures de protection appropriées ont été mises en œuvre par le fournisseur afin de rendre les données incompréhensibles à toute personne non autorisée à y avoir accès et ont été appliquées aux données concernées par ladite violation ». En clair, pas d'alerte direct des clients si les rustines ont été correctement appliquées.
Plus globalement, l'article 34 de la loi Informatique et Libertés impose au responsable d'un traitement de prendre toutes précautions utiles pour préserver la sécurité des données et, notamment, empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. Évidemment, cette protection diffère selon la nature des données et des risques présentés par le traitement.
Enfin, selon l'article 226-17 du Code pénal, le fait de procéder ou de faire procéder à un traitement de données à caractère personnel sans mettre en oeuvre les mesures prescrites à l'article 34 est puni de cinq ans d'emprisonnement et de 300 000 euros d'amende.
Etonnant non ?

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

Source : http://www.nextinpact.com/news/91600-un-partenaire-tf1-pirate-quelles-consequences-juridiques.htm
Extrait de Marc Rees adapté par Denis JACOPINI

Vols, cybercriminalité, contrefaçons… Près de 50% des entreprises victimes de fraudes – 20minutes.fr

	Vols, cybercriminalité, contrefaçons… Près de 50% des entreprises victimes de fraudes

Près de la moitié (49%) des entreprises de distribution et de biens de consommation au niveau mondial déclarent avoir été victimes de fraudes au cours des deux dernières années, selon une étude de PwC diffusée lundi.

«Ce chiffre ne cesse d'augmenter depuis 2009 (+12 points)», note le cabinet de conseil, qui a interrogé 5.128 dirigeants d'entreprises, dont 383 du secteur de la distribution et des biens de consommation, issus de 99 pays. La fraude la plus largement commise dans le secteur est le détournement d'actifs (76%), ce qui inclut «le vol, les décaissements frauduleux et l'appropriation illicite de matériel».

Risques liés à la cybercriminalité

La fraude aux achats arrive en deuxième position, beaucoup de répondants évoquant notamment des infractions liées à la sélection des fournisseurs (59%) ou bien aux contrats/accords de maintenance conclus avec ces derniers (39%).
Si la corruption n'est pas la fraude la plus constatée (25%), 56% des dirigeants interrogés la considèrent comme le risque le plus élevé pour une entreprise opérant à l'international.
Beaucoup de dirigeants évoquent également les risques grandissants liés à la cybercriminalité: un sur cinq déclare en avoir été déjà victime, et 27% pensent que leur entreprise y sera confrontée dans les deux années à venir.

Risque de renvoi ou de poursuites judiciaires

La perte de propriété intellectuelle (contrefaçon, vols de données clients…) fait également partie de leurs préoccupations pour l'avenir: seuls 7% en ont déjà fait l'expérience, mais 21% estiment qu'ils y seront confrontés d'ici deux ans.
L'étude montre que dans plus de deux tiers des cas (67%), les auteurs de ces infractions sont des collaborateurs internes aux entreprises. Ce taux est supérieur dans les secteurs de la distribution/biens de consommation, aux taux constatés sur l'ensemble des secteurs (56%).
«Les auteurs de ces faits occupent, pour la plupart, des postes de cadres intermédiaires et sont sévèrement punis lorsqu'ils sont démasqués: les entreprises pratiquent majoritairement le renvoi; elles se lancent parfois dans des poursuites civiles ou recourent aux autorités judiciaires», indique PwC.

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

Source : http://www.20minutes.fr/societe/1515087-20150112-vols-cybercriminalite-contrefacons-pres-50-entreprises-victimes-fraudes

---

Antiterrorisme : les Fournisseurs d'Accès à Internet devraient travailler plus étroitement avec le gouvernement

Antiterrorisme : les fournisseurs d'Accès à Internet devraient travailler plus étroitement avec le gouvernement

Les attentats perpétrés en France, la semaine dernière contre Charlie Hebdo, et à Montrouge, pourraient poser quelques questions sur le niveau de sécurité dans l'Union européenne, ainsi que sur les moyens des services de renseignement. Les FAI pourraient prochainement devoir se rapprocher davantage des gouvernements.

« Je suis fermement convaincu que le moment est venu pour l'UE de s'unir dans une action commune et cohérente contre le terrorisme ». Tels sont les propos de Rihards Kozlovskis, ministre letton de l'Intérieur, qui a représenté la présidence du Conseil de l'Union européenne à la réunion ministérielle internationale qui s'est tenue hier.
Les ministres d'Intérieur de la France, de l'Allemagne, de l'Autriche, de la Belgique, de l'Italie, des Pays-Bas, de la Pologne, du Royaume-Uni, de la Suède, de l'Espagne et du Danemark ont publié une déclaration (PDF) conjointe condamnant les actions terroristes contre le journal français Charlie Hedbo et les assassinats commis à Montrouge et Vincennes. Ensemble, ils souhaitent également affermir leur lutte globale contre la radicalisation.
Internet jouant un rôle majeur dans le déploiement de la propagande terroriste, il s'agira de l'une des pistes de réflexion privilégiée pour renforcer les mesures de sécurité. Les ministres expliquent ainsi :
« Préoccupés par l'utilisation d'Internet à des fins de haine et de violence, nous sommes déterminés à ce que cet espace ne soit pas perverti à ces fins, tout en garantissant qu'il reste, dans le strict respect des libertés fondamentales, un lieu de libre expression, respectant pleinement la loi ».
Pour ce faire, les gouvernements entendent accroître leurs travaux avec les fournisseurs d'accès à Internet pour renforcer leurs dispositifs de surveillance :
« Dans cette perspective, le partenariat avec les grands opérateurs de l'Internet est indispensable pour créer les conditions d'un signalement rapide des contenus incitant à la haine et à la terreur, ainsi que de leur retrait, lorsque cela est approprié et/ou possible. »
Depuis des années, les grandes sociétés de la Toile française ont été sensibilisées à la lutte contre l'antisémitisme. L'on se souvient notamment que l'Amicale des déportés d'Auschwitz et des camps de Haute-Silésie, le Consistoire israélite de France, et le MRAP (Mouvement contre le racisme et pour l'amitié entre les peuples) avaient déposé une plainte contre Yahoo! en 2000 pour avoir permis la vente d'objets nazis sur ses pages Internet.
Le contenu de cette déclaration commune commence à créer une certaine polémique : plusieurs internautes sur Twitter (via le hashtag #CharlieDoesSurf) soulignent le caractère contradictoire des marches républicaines pour la liberté d'expression avec des mesures de surveillance accrues pour un meilleur contrôle du Web qui se profilent à l'horizon.
Reste à connaître la nature de ces mesures qui seront décidées entre les États membres de l'Union européenne pour renforcer la vigilance des FAI, mais également des autres acteurs majeurs de la Toile.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…
Source : http://pro.clubic.com/technologie-et-politique/actualite-749239-terrorisme-fai-devront-renforcer-vigilence-collaborer-gouvernement.html
Par Guillaume Belfiore

MegaChat : la messagerie anti-NSA signée Kim Dotcom

MegaChat : la messagerie anti-NSA signée Kim Dotcom

Le sulfureux fondateur du défunt MegaUpload annonce le lancement d'une messagerie chiffrée capable d'échapper à la curiosité des services de renseignement, NSA en tête.

Kim DotCom signe son retour. Après avoir – en apparence du moins – négocié l'arrêt des attaques par déni de service contre les réseaux Sony PlayStation et Xbox Live avec les hackers de la Lizard Squad, le sulfureux fondateur du défunt site de téléchargement MegaUpload promet l'arrivée imminente d'un nouveau service de messagerie électronique et de discussion instantanée sécurisé par chiffrement. Un service baptisé MegaChat qui entre dans la croisade de Kim Dotcom visant à garantir aux internautes une confidentialité totale de leurs échanges numérique. Rappelons que ce dernier a déjà lancé un service de stockage chiffré, Mega.
Pour passer à travers les mailles du filet de la NSA et d'autres services de renseignement, cette alternative cryptée à Skype permettra aux internautes, dès début 2015, d'utiliser cette messagerie ultra-sécurisée dotée de fonctionnalités d'appels audio et de visioconférence.
Elle autorisa également « le transfert de fichiers à haute vitesse via un navigateur Web », a promis Kim Dotcom, dans un message publié sur Twitter. Pas besoin donc d'installer un logiciel spécifique sur son ordinateur ou sa tablette, notent nos confrères d'ITespresso. De manière sécurisée, les utilisateurs pourront, grâce au chiffrement intégral des données, envoyer, lire et partager des fichiers (audio, vidéos,…).

« Skype est obligé de fournir des backdoors »
« Vous ne pouvez faire confiance à aucun fournisseur de services en ligne installé aux Etats-Unis pour [garantir la confidentialité] de vos données », a souligné Kim Dotcom. « Skype n'a pas le choix. Ils sont obligés de fournir des backdoors au gouvernement américain ». A en croire l'homme d'affaires d'origine allemande, MegaChat serait donc un des seuls services Internet capables de garantir l'intégrité des données de ses membres, et de les préserver des manœuvres d'espionnage des autorités gouvernementales, Etats-Unis en tête.
Rappelons que selon des informations relayées par Der Spiegel et issues des documents confidentiels dévoilés par Edward Snowden, la NSA a réussi à contourner, dès la fin 2011, la sécurité de Skype pour permettre à l'agence américaine de mettre en place une collecte de données à grande échelle sur le système de communications, propriété de Microsoft.

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

Source : http://www.silicon.fr/megachat-messagerie-anti-nsa-kim-dotcom-104829.html