Etude d’impacts sur la vie privée : découvrez la méthode | Le Net Expert Informatique

17

	Etude d’impacts sur la vie privée : suivez la méthode de la CNIL

La CNIL publie sa méthode pour mener des PIA (Privacy Impact Assessment) pour aider les responsables de traitements dans leur démarche de mise en conformité et les fournisseurs dans la prise en compte de la vie privée dès la conception de leurs produits.

De l'application de bonnes pratiques de sécurité à une véritable mise en conformité
La Loi informatique et libertés (article 34), impose aux responsables de traitement de « prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données ».
Chaque responsable doit donc identifier les risques engendrés par son traitement avant de déterminer les moyens adéquats pour les réduire.
Pour aider les TPE et PME dans cette étude, la CNIL a publié en 2010 un premier guide sécurité. Celui-ci présente sous forme de fiches thématiques les précautions élémentaires à mettre en place pour améliorer la sécurité d'un traitement des données personnelles.
En juin 2012, la CNIL publiait un autre guide de gestion des risques sur la vie privée pour les traitements complexes ou aux risques élevés. Il aidait les responsables de traitements à avoir une vision objective des risques engendrés par leurs traitements, de manière à choisir les mesures de sécurité nécessaires et suffisantes.

Une méthode plus rapide, plus facile à appliquer et plus outillée
Ce guide a été révisé afin d'être plus en phase avec le projet de règlement européen sur la protection des données et les réflexions du G29 sur l'approche par les risques. Il tient aussi compte des retours d'expérience et des améliorations proposées par différents acteurs.
La CNIL propose ainsi une méthode encore plus efficace, qui se compose de deux guides : la démarche méthodologique et l'outillage (modèles et exemples). Ils sont complétés par le guide des bonnes pratiques pour traiter les risques, déjà publié sur le site web de la CNIL.

Un PIA (Privacy Impact Assessment) ou étude d'impacts sur la vie privée (EIVP) repose sur deux piliers :
1.les principes et droits fondamentaux, « non négociables », qui sont fixés par la loi et doivent être respectés. Ils ne peuvent faire l'objet d'aucune modulation, quelles que soient la nature, la gravité et la vraisemblance des risques encourus ;
2.la gestion des risques sur la vie privée des personnes concernées, qui permet de déterminer les mesures techniques et d'organisation appropriées pour protéger les données personnelles.

Pour mettre en oeuvre ces deux piliers, la démarche comprend 4 étapes :
1.étude du contexte : délimiter et décrire les traitements considérés, leur contexte et leurs enjeux ;
2.étude des mesures : identifier les mesures existantes ou prévues (d'une part pour respecter les exigences légales, d'autre part pour traiter les risques sur la vie privée) ;
3.étude des risques : apprécier les risques liés à la sécurité des données et qui pourraient avoir des impacts sur la vie privée des personnes concernées, afin de vérifier qu'ils sont traités de manière proportionnée ;
4.validation : décider de valider la manière dont il est prévu de respecter les exigences légales et de traiter les risques, ou bien refaire une itération des étapes précédentes.

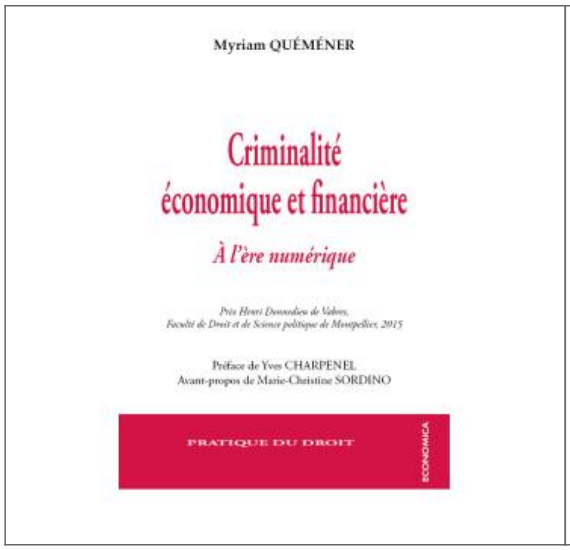
L'application de cette méthode par les entreprises devrait ainsi leur permettre d'assurer une prise en compte optimale de la protection des données personnelles dans le cadre de leurs activités.

PIA, LA MÉTHODE
PIA, L'OUTILLAGE

Source : http://www.newspress.fr/Communique_FR_289793_1332.aspx

---

La criminalité économique et financière à l'ère numérique | Le Net Expert Informatique



La criminalité économique et financière à l'ère numérique

Les banques, les compagnies d'assurances, les sites gouvernementaux, les compagnies pétrolières et, maintenant, l'industrie aéronautique avec la cyberattaque de la compagnie polonaise LOT : le cybercrime cible des secteurs de plus en plus sensibles, sources de dégâts humains majeurs. Au-delà des pertes financières, c'est le cœur du système politique, économique et juridique qui est aujourd'hui menacé par ce fléau.

Que fait l'État, la justice, pour enrayer ces comportements ? Fabriquer des lois en série est-elle « la » solution face à l'existence de cyberparadis, d'une cyberéconomie souterraine de plus en plus puissante, et à la volatilité des preuves ? Le Point.fr a interrogé Myriam Quemener, magistrate, auteur d'un ouvrage de référence sur le sujet : La criminalité économique et financière à l'ère numérique*.

Le Point.fr : « Certaines formes de cybercriminalité sont le fait de réseaux mafieux structurés issus de pays n'ayant pas de législation dédiée à ce phénomène », écrivez-vous. Le décalage entre les législations étatiques est-il surmontable et à quelle échéance ? Que font les autorités françaises en attendant une prise en charge globale et harmonisée de cette délinquance ?
Myriam Quemener : Les pays européens ont harmonisé leurs législations et la coopération internationale se renforce en permanence. La Convention de Budapest, seul traité relatif à la lutte contre la cybercriminalité, a déjà été signée par 46 pays, et d'autres États sont actuellement en négociation pour y adhérer. Pour ce qui concerne la France, notre pays dispose d'un arsenal ancien, en particulier la loi de 1988 dite « loi Godfrain » qui permet de réprimer les piratages informatiques et les cybermenaces. Cet arsenal s'est progressivement enrichi et perfectionné pour permettre le recours à des procédures adaptées à l'univers numérique. De nouvelles structures sont nées, comme l'Anssi, qui met en œuvre la stratégie gouvernementale en matière de cybersécurité, mais aussi une nouvelle sous-direction de lutte contre la cybercriminalité et un pôle numérique au parquet de Paris qui a vocation à s'étoffer. On a aussi créé le procureur de la République financier à compétence nationale exclusive en matière de délits boursiers et pour les affaires économiques et financières complexes qui sont aussi souvent à dimension internationale.

Quels sont les nouveaux moyens d'investigation des enquêteurs pour déjouer les attaques ?
Sur le plan procédural, le législateur a transposé le régime des interceptions téléphoniques à Internet. Il a aussi innové en prévoyant l'infiltration numérique, qui est une enquête sous pseudonyme. Elle permet à l'enquêteur d'utiliser un nom d'emprunt pour entrer plus facilement en contact avec le cyberdélinquant. Depuis la loi du 13 novembre 2014, l'enquête sous pseudonyme jusqu'alors utilisée en matière de pédopornographie et de contrefaçon s'applique à l'ensemble des procédures de criminalité organisée.

Les données personnelles sont considérées comme « l'or noir du XXIe siècle ». La semaine dernière, une importante base de données américaine abritant les coordonnées, données de santé et autres informations personnelles d'environ 20 millions de fonctionnaires a été piratée. Quel usage les cyberdélinquants font-ils des données récupérées, et à quoi peut-on s'attendre dans les années qui viennent ?
Ils récupèrent ces données et les revendent sur les marchés noirs du Web (Darknet) qui sont des réseaux parallèles aux réseaux ouverts du type Google. Cela permet par exemple de faire des achats sous de fausses identités ou d'obtenir des virements en se faisant passer pour une entreprise connue. Les données personnelles servent aussi à créer de faux profils, et tout cela se répercute sur l'e-réputation des entreprises. L'usurpation d'adresses IP (spoofing) qui permet de commettre des fraudes à la téléphonie mobile se développe aussi de manière considérable.

Quels sont les prochains défis de la criminalité astucieuse sur Internet ?
En cette période où le terrorisme frappe de façon dramatique, il est important de s'attaquer avec vigueur au financement du terrorisme, et cette lutte passe par une politique publique pragmatique et déterminée contre des phénomènes comme le cyberblanchiment ou les escroqueries aux faux ordres de virement.
Il faut par ailleurs être attentif et vigilant face à des outils numériques comme le crowdfunding (financement participatif) ou les crédits à la consommation. Les sommes obtenues au travers de ces formes de prêt peuvent en effet servir à financer des activités illicites. Il en est de même du « trading haute fréquence » qui permet d'envoyer des ordres d'achat à une vitesse de l'ordre de la nanoseconde, grâce à des algorithmes superpuissants, permettant des manipulations de cours. Le courtage à haute fréquence a aussi ses dérives : un courtier londonien a récemment été arrêté pour une manipulation sur le marché des contrats à terme électroniques aux États-Unis, qui avait contribué au mini-krach de mai 2010 à Wall Street.
Il faut aussi suivre avec attention le développement de ces fameuses « monnaies virtuelles » qui contournent le système bancaire et permettent d'échapper à tout contrôle étatique en raison de l'absence de traçabilité. Les objets connectés, qui favorisent l'usurpation de profils complets, et le cloud computing qui contient des données sensibles à valeur commerciale sont aussi des cibles potentielles de cyberattaques. D'autant que de nombreuses failles de sécurité existent et peuvent être exploitées par les cybercriminels.

Qu'est-ce qui dissuade vraiment les délinquants, qu'ils soient isolés ou membres d'organisations criminelles ?
La mise en place d'une stratégie globale au niveau des services de l'État est de nature à dissuader les cyberdélinquants, de même que les condamnations et démantèlements de réseaux de cybercriminels qui ne cessent d'augmenter grâce aux moyens d'investigation et à l'expertise de plus en plus pointue des enquêteurs dédiés.

Pensez-vous que l'Internet a démultiplié les risques, ou les a-t-il seulement déplacés ?
L'absence de confrontation physique auteur-victime, propre à Internet, facilite le passage à l'acte. Le système des rencontres virtuelles attire des personnes mal intentionnées qui peuvent plus facilement extorquer de l'argent, notamment via des sites de vente entre particuliers. Aujourd'hui, la cybercriminalité s'industrialise et s'organise sous forme de structures hiérarchisées allant de la main-d'œuvre de base qui récupère des données jusqu'aux têtes de réseau qui donnent les ordres.

Ces phénomènes sont-ils, comme le changement climatique, irréversibles ?
Je ne le pense pas, car, actuellement, il y a une mobilisation importante, du secteur tant public que privé, pour lutter contre ces phénomènes. Il est indispensable de multiplier les actions de formation pluridisciplinaire des acteurs publics et privés qui concourent à la lutte contre ces attaques. Cependant, il ne faut pas perdre de vue que ce type de délinquance lance un défi au temps judiciaire, c'est même une course contre la montre !

L'ouvrage en vente ici

Source : http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/cybercrime-un-defi-lance-au-temps-judiciaire-13-07-2015-1943938_56.php

---

| Le Net Expert Informatique

Bercy devra gérer non pas une, mais deux lois numériques | Le Net Expert Informatique

	**Bercy devra gérer non pas une, mais deux lois numériques**

La loi numérique, tout le monde en parle. Même le chef de l'Etat a abordé le sujet lors de l'interview du 14 juillet. Désormais, il semble probable qu'au lieu d'un texte il y en ait deux. Un signé Macron pour la croissance, l'autre signé Axelle Lemaire pour les libertés.

La question revient à chaque fois qu'un journaliste rencontre un responsable gouvernemental proche du dossier. « Où en sommes-nous de la loi numérique dont on parle depuis 2013 ? » La réponse est toujours la même, ou presque : « Nous y travaillons, nous vous tiendrons informé quand nous aurons avancé ». Rien n'est vraiment officiel mais en fait, il n'y aura pas une loi, mais deux. L'une sur la transformation numérique de l'économie, l'autre sur les libertés individuelles.

Lors de la traditionnelle interview du 14 juillet, le chef de l'Etat y a fait une allusion. « Je vais préparer une loi sur le numérique, tout ce qui est activités nouvelles, tout ce qui peut provoquer de l'emploi ». Le message s'adresse clairement à Emmanuel Macron, ministre de l'économie, de l'Industrie et du Numérique.
Dès le lendemain, lors d'un point presse, le ministre est revenu sur le sujet. Sans entrer dans les détails, il a simplement précisé que les premières propositions seront faites au plus tard début 2016. Et pour calmer les impatients, il a prévenu qu'il prendra le temps nécessaire pour l'élaborer. Et en effet l'exercice promet d'être délicat.
Emmanuel Macron est parfaitement conscient du levier que représente le numérique en matière de création d'emploi. Mais il doit composer entre une nouvelle économie qui bouscule les règles des entreprises traditionnelles. Tandis que ces dernières se trouvent, elles, confrontées à une concurrence qu'elles estiment déloyale, voire illégale selon les cas.

Une loi Macron 2 pour la transformation numérique
Dans son message, François Hollande a été plutôt clair: « il faut qu'il n'y ait rien dans nos règles, dans nos formalités qui puisse entraver ». La guerre entre Uber et les taxis est l'un des exemples les plus frappants de la crainte que génère le potentiel des nouvelles technologies. Ce sera donc à Emmanuel Macron de gérer ce dossier dans une loi qui a déjà un nom: Macron 2.
Autres sujets d'importance, les données personnelles et les libertés individuelles face aux géants du Net. Ces sujets devraient faire parti d'un second texte qui sera cette fois sous la responsabilité d'Axelle Lemaire. Le cœur de ce projet devrait donner plus de poids à la Cnil dont le pouvoir, notamment celui de sanctionner, doit être renforcé. En janvier 2015, sa présidente, Isabelle Falque-Pierrotin faisait déjà des propositions sur le contenu du texte.
Mais la présidente de la Cnil est également présidente des Cnil européennes, connues sous le nom de « Groupe de l'article 29 » et dans ce cadre, elle rappelle que le texte devra être compatible avec le projet de règlement européen. « La législation sur les données personnelles ayant une portée économique croissante, les modifications éventuelles ne doivent pas créer de distorsion entre pays de l'Union. » Le cadre est posé. Reste désormais à savoir quand Axelle Lemaire présentera cette loi. Avant ou après celle d'Emmanuel Macron?

Source : http://bfmbusiness.bfmtv.com/entreprise/bercy-devra-gerer-non-pas-une-mais-deux-lois-numeriques-902051.html
Par Pascal Samama

Les Chiffres et Statistiques du numérique : Usages, risques, cybercriminalité (Dernière infos rajoutées le 17/07/2015)

Dernière infos rajoutées le 17/07/2015

Dans le but de vous permettre de mieux juger l'importance du Risque Informatique et de la Cybercriminalité en France et ailleurs, nous avons souhaité mettre à disposition le résultat de nos collectes successives de statistiques relativement impressionnantes.

Ces chiffres ne m'appartiennent pas et pour chacun d'eux, est indiqué la date d'ajout dans ce document et la source d'information associée. Cependant, **si vous souhaitez reprendre tout ou partie du résultats de mes recherches, je vous demanderais soit de citer « Denis JACOPINI » ou « Le Net Expert » comme source de votre information**.

Besoin d’informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

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, et ce, 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 !

Lorsque, lors de conférences, je m’adresse à des entreprises pour leur parler de sécurité informatique et de risque de piratage, les chefs d’entreprises, pourtant vêtus d’une responsabilité souvent pénale, me rétorquent du « On n’est pas concerné, on n’est pas la Nasa », du « On n’a pas de secret qui pourrait intéresser des pirates, on ne risque rien » ou bien du « de toute façon, le peu de contrôles que la CNIL fait n’aboutissent qu’à des amendes symboliques ».

De leur répondre : « Bien sur que si, vous avez des informations secrètes, et même ultra secrètes : LES DONNEES A CARACTERE PERSONNEL DE VOS CLIENTS ». Et vous avez même ente vos main quelque chose d’encore plus précieux que ça : VOTRE REPUTATION »

Trop peu respectée, la loi informatique et libertés fixe impose à tout responsable de traitement de données personnelles de mettre en place des mesures de sécurité appropriées à la protection des données à caractère personnel.

Sans cela, données non protégées = données piratées et diffusées dans la nature = risque pénal mais surtout réputation salie.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

INTERNET DANS LE MONDE EN 2014

42% de la population mondiale soit 3,025 milliards de personnes utilisent le réseau internet. (D27-S35)

Sur l'ensemble du continent africain, le taux de pénétration d'Internet est estimé à 16% en 2014 soit 167 millions d'internautes, contre 110 millions en 2010. (D27-S35)

Le nombre des utilisateurs d'Internet en Afrique devrait être

multiplié par 3.5 d’ici 2015 pour que le nombre d’internautes atteigne près de 600 millions. (D27-S35)

Nombre d’internautes : 3,001,769,770 (35% de la population mondiale). (D9-S16)

Le cap des 3,2 milliards d’internautes devrait être dépassé dans le monde en 2014

Taux de pénétration d’Internet dans le Monde :
81% en Amérique du Nord (86% au Canada, 80% aux USA) (D9-S16)
78% en Europe de l’Ouest (83% en France) (D9-S16) 18% en Afrique (D9-S16)
12% en Asie du Sud (D9-S16)
822 240 nouveaux sites Internet sont mis en ligne chaque jour (D9-S16)

Chaque minute sur Internet : (D9-S16)
2 millions de requêtes Google sont effectuées
347 nouvelles publications WordPress sont publiées
571 nouveaux sites web sont créés
2000 nouvelles photos sont ajoutés sur Tumblr
204 millions d’emails sont envoyés

Denis JACOPINI est à l’origine de cette collecte d’information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

TÉLÉCHARGEMENT ILLÉGAL ET LOI HADOPI

10% des abonnés avertis une fois récidivent. (D23-S31)

Sur les 8,9% de titulaires d'un abonnement à Internet ayant reçu un premier avertissement (entre octobre 2010 et juin 2014, soit plus de 3,2 millions d'emails envoyés), ils ne sont plus que 10,4% d'entre eux à avoir été avertis une deuxième fois – puis 0,4% à s'être retrouvés en phase 3. (D23-S31)

70% diminuent leur consommation illicite après l'avertissement 1. (D23-S31)

88% diminuent leur consommation illicite après l'avertissement 2. (D23-S31)

Après un avertissement, seulement 23% à déclarer se tourner vers une offre légale. (D23-S31)

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

LA SÉCURITÉ ET LES CERTIFICATS SSL

Jusqu’à 91% des internautes n’iront pas plus loin en cas d’avertissement au risque de malware ou de phising. (D17 – S25)

Plus des 2/3 (77%) des sites Internet propagateurs de malwares sont des sites légitimes infectés. (D17 – S25)

Un site Internet sur 8 comporte des vulnérabilités critiques. (D17 – S25)

Denis JACOPINI est à l’origine de cette collecte d’information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

LES FRANCAIS ET LE PAIEMENT SANS CONTACT NFC

15 % utilisent la fonction NFC de leur CB (D24-S32)

19 % ignorent si leur carte dispose de cette option (D24-S32)

34% estiment cette technologie utile (D24-S32)

22% des Français sont à l'aise avec le paiement sans contact (D24-S32)

44 % ont connaissance de la fonction paiement sans contact de leur carte bancaire (D24-S32)

29 % ne s'en servent pas sachant qu'ils ont cette option (D24-S32)

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être

personnalisées et organisées dans votre établissement.
Besoin d’informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

LA SÉCURITÉ ET LE BYOD

95% des entreprises se disent menacées par des problèmes de sécurité liés au BYOD. (D17-S24)

82% pensent même que le nombre d’incidents dans ce domaine va croître en 2015 par rapport à 2014. (D17-S24)

47% des entreprises ont éprouvé des intrusions suite à des brèches présentes dans des appareils mobiles. (D17-S24)

64% pensent qu’Android est toujours considéré comme le système d’exploitation le plus risqué des OS mobiles. (D17-S24)

Denis JACOPINI est à l’origine de cette collecte d’information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur

spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

LA SÉCURITÉ EN ENTREPRISE

Une étude internationale a interrogé 450 décideurs informatiques et révèle que de nombreuses sociétés se heurtent aux exigences de gouvernance et de sécurité des échanges de données. (D22-S30).

23% des entreprises ont récemment échoué à un audit de sécurité, tandis que

17 % doutent de leur capacité à réussir un audit de conformité des échanges de données.

Le coût total moyen d'une atteinte à l'intégrité des données s'élève à 2,4 millions d'euros.

La stratégie d'intégration n'est pas alignée avec les structures et les politiques de gouvernance, de confidentialité et de sécurité des données pour 71% des entreprises.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

LA CYBERCRIMINALITE ET LES MOBILES

Entre janvier et juin 2014, le nombre d'infections touchant les terminaux mobiles a progressé de 17% (20% seulement sur tout 2013. (D15-S22)

0,65% des smartphones en circulation sont infectés d'un malware. Les smartphones équipés d'Android comptent 60% des équipements mobiles infectés contre 40% pour les PC portables équipés de Windows.

De leur côté, les iPhone, les BlackBerry, les téléphones sous Symbian et sous Windows Phone totaliseraient moins de 1%.

Le cheval de Troie *Android.Trojan.Coogos.A!tr* représenterait 35,69% des attaques ciblant Android.

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

LE CLOUD EN ENTREPRISE

Enquête Eurostat : Utilisation des TIC dans les entreprises en 2014 (D19-S21)

19% des entreprises utilisait des services de cloud computing en 2014

45% secteur de l'information & de la communication

27% activités spécialisées, scientifiques et techniques

14% et 20% dans tous les autres secteurs économiques

Pour les 81% des entreprises n'utilisant pas le cloud, une connaissance insuffisante de ces services informatiques constituait le principal facteur bloquant.

En 2014, les proportions les plus élevées d'entreprises

utilisant le cloud ont été observées en Finlande (51%), en Italie (40%), en Suède (39%) ainsi qu'au Danemark (38%). À l'opposé, les services de cloud computing étaient utilisés par moins de 10% des entreprises en Roumanie (5%), en Lettonie et en Pologne (6% chacun), en Bulgarie, en Grèce et en Hongrie (8% chacun).
Dans seize États membres, le cloud était principalement utilisé pour les services de courrier électronique, notamment en Italie (86%), en Croatie (85%) et en Slovaquie (84%). Les services de cloud computing étaient principalement utilisés pour le stockage de fichiers dans onze autres États membres, les proportions les plus élevées ayant été observées en Irlande (74%), au Royaume-Uni (71%), au Danemark ainsi qu'à Chypre (70% chacun), tandis que l'hébergement de la base de données de l'entreprise était l'usage du cloud le plus courant aux Pays-Bas (64%).

Enquête Unitrend auprès d'entreprises (D19-S21) :

78% ont connu des coupures des applications critiques.

63% estiment que les pertes ainsi engendrées vont de quelques centaines de dollars à plus de 5 millions.

28% des entreprises touchées par un incident estiment que leurs entreprises ont été privées de fonctions clés de leurs datacenters pendant des périodes pouvant aller jusqu'à plusieurs semaines.

73% des entreprises déclarent ne pas prêtes pour la restauration après sinistre.

60% estiment qu'elles n'ont pas complètement documenté leur plan de reprise d'activité.

23% n'ont jamais testé ces plans de reprise d'activité.

Nous organisons régulièrement des **actions de sensibilisation ou de formation** au risque informatique, à l'hygiène informatique, à la cybercriminalité et à la mise en conformité auprès de la CNIL. Nos actions peuvent aussi être personnalisées et organisées dans votre établissement. Besoin d'informations complémentaires ?

Contactez-nous

Denis JACOPINI
Tel : 06 19 71 79 12
formateur n°93 84 03041 84

CE QUE PENSENT LES ENTREPRISES DE LEUR SECURITÉ

Sept entreprises sur dix seraient convaincues de disposer d'un pare-feu de nouvelle génération (*Next Generation Firewall*, ou NGFW) alors que… non, elles ne seraient en fait que 30 % à en posséder. (D16-S23)

54 % des DSI français pensent que leur pare-feu dispose de capacités de détection avancées efficaces, intégrant notamment des fonctions de sandboxing spécifiques aux fameux NGFW. (D16-S23)

31 % des décideurs IT estiment que leur entreprise utilise trop de solutions de sécurité pour gérer les menaces. (S16-S23)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

LE DROIT À L'OUBLI

Les plaintes liées au droit à l'oubli, en hausse de quatre points par rapport à 2012, ont représenté 34 % du nombre total de plaintes en 2013. (D13-S20)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

CYBERCRIMINALITÉ

5 entreprises sur 6 employant plus de 2 500 personnes ont été la cible de cyberattaques en 2014 (D28-S36)

Entre 2013 et 2014, le nombre des cyberattaques a augmenté de 120% dans le monde et le coût estimé de la cybercriminalité pour les entreprises s'élève en moyenne à 7,6 millions de dollars par an, soit une augmentation de 10% (D26-S34)

61 % des victimes d'une attaque DDoS ont temporairement perdu l'accès à des informations critiques (D25-S33)

38 % ont été dans l'incapacité de poursuivre leur activité principale(D25-S33)
33 % font état de pertes d'opportunités et de contrats (D25-S33)
Dans 29 % des cas, le succès d'une attaque DDoS a eu un impact négatif sur la cote de crédit de l'entreprise (D25-S33)
Dans 26 % des cas, a entraîné une augmentation de ses primes d'assurance (D25-S33)
A la suite d'une attaque DDOS, 49 % ont payé pour faire modifier leur infrastructure informatique, 46 % ont eu recours à leurs avocats et 41 % ont fait appel à des gestionnaires de risque (D25-S33)

72 % des victimes ont divulgué des informations relatives à une attaque DDoS contre leurs ressources. En particulier, 43 % des responsables interrogés ont informé leurs clients d'un incident, 36 % l'ont signalé aux autorités et 26 % en ont parlé aux médias. 38 % des entreprises ont subi une atteinte à leur réputation à la suite d'une attaque DDoS et près d'une sur trois a dû demander l'aide de conseillers en image (D25-S33)

48 % des attaques cibleraient directement des applications web des e-commerçants. (D20-S28)

40 % des attaques par injection SQL et 64 % des campagnes de trafic http malveillant concernent les sites de commerce en ligne. (D20-S28)

Selon l'enquête d'Imperva, les sites de commerce en ligne sont attaqués deux fois plus souvent que des sites plus classiques. Les attaques durent aussi plus longtemps : près de deux fois plus longtemps qu'en 2013. (D20-S28)

68% des internautes envisagent un achat sur internet d'ici la fin de l'année. (D20-S28)

La valeur économique pillée par la cybercriminalité en 2013 représente 190 milliards d'euros. (D18-S26)
Pour illustrer un coût :
« Sony s'est fait voler 1,5 million de données de cartes bleues. Le dommage direct : 150 millions. Mais Sony réclame à son assureur 1,3 milliard de dollars pour compenser l'arrêt complet de leur serveur pollué de e-commerce, c'est-à-dire de leurs ventes, la modification de leur système d'information et la campagne de communication qui a suivi. »

Après avoir analysé les données de plus de 100.000 incidents de sécurité sur 10 ans, Verizon a indiqué que 92 % des attaques peuvent être réparties en 9 types de menaces (les attaques de malwares, la perte ou le vol d'appareils, les attaques DDoS, les arnaques à la carte bancaire, les attaques

d’applications web, le cyber-espionnage, les intrusions, le vol interne et les erreurs humaines), ce qui signifie que les entreprises font toujours face aux mêmes risques et aux mêmes attaques, depuis tout ce temps, et à plusieurs reprises. (D12-S19)

Les fraudes en ligne par carte bancaire ont représenté 64,6% du total des fraudes en 2013, soit un rapport de un à vingt par rapport aux magasins physiques. (D11-S18)

Les e-commerçants ne sont que 43 % à utiliser ces méthodes de protection renforcés (par SMS ou par biométrie) 10 millions de français, 33% des Internautes majeurs victimes de cybercrime (Symantec/Norton 2013). (D1-S1)

47% des logiciels étaient piratés en 2005 contre 37% en 2011. (D6-S11)

Les condamnations d’entreprises ayant piraté des logiciels se sont élevées à 1,3 millions d’euros en 2013, en hausse de 30% par rapport à 2012, représentant 12% du montant des condamnations européennes. (D6-S11)

En juin 2014, 3,2 millions de premiers avertissements ont été expédiés depuis sa création et 333.723 deuxièmes avertissements (lettre recommandée) et 71 dossiers transmis à la justice. (D10-S17)

75 % des messages partent de machines classiques (ordinateurs de bureau ou portables, smartphones, tablettes), le reste provient d’appareils connectés. (D3-S6)

Dans 33% des cas, l’introduction d’un malware est réalisée au travers d’une application mobile. (D2-S5)

58% des entreprises pointent l’inefficacité des antivirus du marché pour lutter contre les malwares. (D2-S5)

56% des PC sont infectés via des emails de type « phishing ». (D2-S5)

40% des infections par Malware sont dues aux sites pornographiques. (D2-S5)

Plus de 30% de nos ordinateurs personnels stockent des fichiers illicites à notre insu. (D2-S4).

61% des sites malveillants sont en fait des sites institutionnels. (D1-S1) (D1-S3)

1 site Internet sur 500 est infecté par de malwares (D1-S3)

Google bloque 10000 sites Internet par jour (D1-S3)

400 Millions de personnes sont concernées par des cyberattaques chaque année (D1-S3)

93 % des grandes entreprises ont été victimes d'une cyberattaque en 2012 (D1-S2)

Attaques cybercriminelles +42% en 2012. (D1-S1)

Attaques en ligne +30% en 2012. (D1-S1)

Maliciels sur mobiles +58% en 2012. (D1-S1)

31% des cibles sont des PME en 2012 contre 18% en 2011. (D1-S1)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

MESSAGERIE ÉLECTRONIQUE

144 milliards d’emails sont échangés chaque jour. (D9-S16)

68,8% d’entre eux sont des spams. (D9-S16)

Denis JACOPINI est à l’origine de cette collecte d’information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

LES VOLS

3 français sur 10 disent avoir déjà perdu ou s’être fait voler leur téléphone. (D7-S14)

630 000 vols de téléphones portables en 2011. (D5-S9)

160 000 vols de téléphones portables en 2010. (D5-S8)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

RÉSEAUX SOCIAUX

18 % des sociétés de plus de 10 salariés ont un compte dans un réseau social. (D6-S13)

Moins de 13% des sociétés dans le domaine de la construction, du transport ou de l'industrie ont un compte dans un réseau social. (D6-S13)

38 % des sociétés dans le domaine de l'hébergement et de la restauration ont un compte dans un réseau social. (D6-S13)

60 % des sociétés dans le domaine de la communication, de

l’information ou de la réparation d’ordinateurs ont un compte dans un réseau social. (D6-S13)

80% d’entres utilisent les réseaux sociaux pour développer leur image ou commercialiser leurs produits. (D6-S13)

43 % des sociétés de plus de 250 salariés ont un compte. (D6-S13)

5% utilisent les blogs et les sites Internet de partage de contenu multimédia. (D6-S13)

4% utilisent des outils de partage de connaissance. (D6-S13)

Twitter a 900 millions de comptes crées dans le monde mais seulement 241 millions sont actifs. (D5-S11)

Facebook : 1,23 milliard d’utilisateurs actifs dans le monde. (D5-S11)

LinkedIn : 150 millions d’utilisateurs actifs dans le monde. (D5-S11)

Google+ : 300 millions d’utilisateurs actifs dans le monde. (D5-S11)

Tumblr : 166 millions d’utilisateurs actifs dans le monde. (D5-S11)

Viadeo : 55 millions de membres dans le monde dont 8 millions en France et 4,4 millions de visiteurs uniques. (D5-S11)

Instagram : 200 millions d’utilisateurs actifs dans le monde. (D5-S11)

Pinterest : 20 millions d’utilisateurs actifs dans le monde. (D5-S11)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

ÉQUIPEMENTS DES FRANCAIS

Un foyer sur cinq (21,523%) en France dispose d'une tablette tactile. (D5-S11)

Ils n'étaient que 14,1% au 4e trimestre 2012. (D5-S11)

L'accès à l'Internet mobile double chaque année. (D9-S16)

70% des internautes sont des utilisateurs quotidiens. (D9-S16)

8 nouveaux utilisateurs chaque seconde. (D9-S16)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat

de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

LES BLOGS et BLOGUEURS

En France, seulement 4% des blogueurs sont des professionnels. (D4-S7)

65% des blogueurs gagnent 0€ / mois (passion). (D4-S7)

18% des blogueurs gagnent moins de 100€/ mois. (D4-S7)

10% des blogueurs gagnent entre 100€ et 1000€/ mois. (D4-S7)

7% des blogueurs gagnent plus de 1000€/ mois. (D4-S7)

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité

Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

GOOGLE ET LA PRESSE

Rappelez-vous, en février 2013, Google acceptait de verser 60 millions d'euros à la presse française sur 3 ans. (D8-S15)

Pour l'année 2013, 16 millions d'euros ont été versés. Voici comment ont été dépensés les millions pour les 12 principaux bénéficiaires (23 au total) :
Le Nouvel Observateur a reçu 2 millions d'euro pour créer une édition numérique quotidienne.
L'Express, 1,97 millions pour analyser les données utilisateurs.
Le Figaro, 1,8 millions pour renforcer son site de vidéos.
Le Monde, 1,8 millions pour une future édition du matin sur mobiles.
Ouest-France, 1,4 millions pour deux éditions en ligne par jour.
La Voix du Nord, 840.000 euros pour créer 1524 portails.
La Croix, 835.000 euros pour analyser son audience.
Slate, 758.000 euros pour analyser les conversations numériques

Denis JACOPINI est à l'origine de cette collecte d'information. Merci de le citer si vous utilisez le résultat de ce travail.

Denis JACOPINI est Expert Informatique assermenté et formateur spécialisé en mise en conformité avec la CNIL, en sécurité Informatique, en cybercriminalité et en protection des données à caractère personnel.

Posez vos questions

Date de la Mises à jour de ce document : (1) 14/03/2014 – (2) 27/03/2014 – (3) 07/04/2014 – (4) 20/04/2014 – (5) 23/04/2014 – (6) 25/04/2014 – (7) 08/05/2014 – (8) 17/05/2014 – (9) 23/06/2014 – (10) 12/07/2014 – (11) 17/07/2014 – (12) 22/07/2014 – (13) 02/09/2014 – (14) 03/09/2014 – (15) 10/09/2014 – (16) 28/10/2014 – (17) 30/10/2014 – (18) 31/10/2014 – (19) 03/11/2014 – (20) 29/11/2014 – (21) 11/12/20214 – (22) 12/12/2014 – (23) 28/12/2014 – (24) 25/01/2015 – (25) 29/01/2015 – (26) 13/02/2015 – (27) 25/05/2015 – (28) 17/07/2015

Sources :
(1)
http://www.symantec.com/fr/fr/about/news/release/article.jsp?prid=20130416_01 (2)
http://www.lemondeinformatique.fr/actualites/lire-%20cybersecurite-en-europe-les-geants-de-l-internet-%20dispenses-de-declarer-les-incidents-56868.html
(3)

https://www.symantec-wss.com/fr/cybercrime4/int/thanks#.Uyr10rK9KSP
(4) Jean-Paul PINTE le 21/03/2014 cours de Cybercriminalité UM1
(5) http://www.testsdintrusion.com/40-infections-malware-dues-aux-sites-pornographiques/
(6) http://www.tomshardware.fr/articles/internet-objet-frigo-spam,1-46695.html
(7) La Quotidienne du 14 04 2014 (France 5) source NWE
(8) http://www.sfr.fr/securite/protection-virus/protection-donnees
(9) http://www.economiematin.fr/les-experts/item/9596-kill-switch-protection-vol-telephone-legislation
(10) http://www.alexitauzin.com/2013/04/combien-dutilisateurs-de-facebook.html
(11) http://www.economiematin.fr/ecoquick/item/7764-etude-equipements-francais-smartphones-tablettes
(12) http://www.zdnet.fr/actualites/logiciels-pirates-13-million-d-euros-de-couts-pour-les-entreprises-francaises-poursuivies-39800283.htm
(13) http://www.zdnet.fr/actualites/les-entreprises-francaises-desertent-les-reseaux-sociaux-selon-l-insee-39800331.htm
(14) http://www.monreseau-it.fr/dossiers/les-antivirus-pour-smartphones-sontils-necessaires-6.htm
(15) http://ecrans.liberation.fr/ecrans/2014/05/15/le-fonds-google-a-verse-16-millions-d-euros-aux-medias-francais-en-2013_1018165
(16) http://www.blogdumoderateur.com/chiffres-internet/
(17) http://www.zdnet.fr/actualites/hadopi-la-machine-a-avertissements-bat-des-records-39803735.htm
(18) http://www.01net.com/editorial/623890/cartes-bancaires-20-fois-plus-de-fraudes-sur-internet-qu-en-magasin/#?xtor=EPR-1-[NL-01net-Actus]-20140716

(19) http://www.huffingtonpost.fr/cyrille-badeau/lutte-cybercriminalite-perdue_b_5595494.html?utm_hp_ref=france
(20) http://www.lepoint.fr/chroniqueurs-du-point/laurence-neuer/google-aux-commandes-du-droit-a-l-oubli-02-06-2014-1830043_56.php
(21) http://www.zdnet.fr/actualites/reprise-d-activite-73-des-entreprises-ne-sont-pas-pretes-apres-un-sinistre-dans-le-cloud-39805553.htm
(22) http://pro.clubic.com/it-business/securite-et-donnees/actualite-725971-etude-15-smartphones-infectes-malware.html
(23) http://www.lemagit.fr/actualites/2240233481/Securite-des-entreprises-francaises-moins-matures-quelles-ne-le-pensent?asrc=EM_MDN_35775718
(24) http://www.zdnet.fr/actualites/byod-des-couts-lies-a-la-securite-parfois-eleves-39808695.htm
(25) https://www.symantec-wss.com/campaigns/15354/fr/assets/infographic/index.html#.VFINvCKG8t4
(26) http://www.paristechreview.com/2014/10/27/espionnage-industriel/
(27) http://www.internetlivestats.com/internet-users/
(28) http://www.commentcamarche.net/news/5865731-les-e-commercants-cibles-par-les-attaques-des-cybercriminels
(29) http://epp.eurostat.ec.europa.eu/cache/ITY_PUBLIC/4-09122014-AP/FR/4-09122014-AP-FR.PDF
(30) http://www.info.expoprotection.com/site/FR/L_actu_des_risques_malveillance__feu/Zoom_article,I1602,Zoom-ce92e8de85306f8f94bb572e6ec6d325.htm
(31) http://www.zdnet.fr/actualites/telechargement-un-avertissement-d-hadopi-ca-calme-39803911.htm
(32) http://pro.clubic.com/e-commerce/paiement-en-ligne/actualite-751153-nfc.html
(33) http://www.globalsecuritymag.fr/Kaspersky-Lab-et-B2B-International,20150128,50328.html
(34) http://www.globalsecuritymag.fr/Le-groupe-Capgemini-lance-une,20150212,50774.html
(35) http://www.info-afrique.com/5336-en-afrique-communication-digitale/

(36) http://www.lesechos.fr/idees-debats/cercle/cercle-135717-comment-les-entreprises-doivent-elles-se-premunir-des-nouvelles-cyberattaques-1137238.php

Utilisation des repères : Un repère (D2-S3) indiquera qu'il fait référence à la (D)ate de mise à jour n°2 et à la (S)ource n°3 soit dans notre document, une mise à jour de notre document le 27/03/2014 et la référence https://www.symantec-wss.com/fr/cybercrime4/int/thanks#.Uyr10rK9KSP

Cet article vous à plu ? Laissez-nous un commentaire (notre source d'encouragements et de progrès)

Android : Google Photos charge les clichés même après une désinstallation | Le Net Expert Informatique

	Android : Google Photos charge les clichés même après une désinstallation

Google continue de charger sur ses serveurs les clichés capturés avec un smartphone Android même lorsque l'application Google Photos a été désinstallée.

A l'occasion de la conférence I/O, Google lançait un nouveau service baptisé Google Photos. Ce dernier, désormais dissocié de Google+, propose un espace de stockage illimité et se présente sous la forme d'une application mobile pour Android et iOS. Google est ainsi paré pour entrer en concurrence avec Facebook, Flickr, Microsoft ou Apple sur le domaine de la photo sur mobiles.
Sur le système d'exploitation Android, les développeurs ont choisi de ne pas placer les options de ce nouveau service directement au sein de l'application Google Photos mais de les ajouter dans les paramètres du compte Google. Cela signifie qu'un internaute désinstallant l'application après l'avoir testé devra effectuer une manipulation supplémentaire pour stopper le service. En effet, le magazine Nashville Business Journal explique qu'une fois l'application installée et activée, elle ajoute une option permettant d'autoriser le chargement des clichés vers les serveurs de Google. Mais lorsque Google Photos est désinstallée, l'option est toujours présente et bel et bien activée. Reste à savoir si dans une prochaine mise à jour Google rectifiera le tir.
Rappelons qu'avec Google photos, les clichés ne peuvent être publiés en privé. Google les masque en leur attribuant des URL supposées « indevinables », qu'il est possible de partager vers un tiers. Le dispositif a été révélé lorsqu'un internaute a réussi à accéder à ses photos supposées privées sans se connecter à son compte Google. Selon la firme de Mountain View, ces URL d'une quarantaine de caractères, seraient plus complexes qu'un mot de passe traditionnel.

Source : http://www.clubic.com/application-mobile/actualite-773600-android-google-photos-chargement-photos-desinstalaltion.html?estat_svc=s%3D223023201608%26crmID%3D639453874_1067015562#pid=22889469

Cyclisme et vol de données – la cyber-criminalité appliquée au sport | Le Net Expert Informatique

Cyclisme et vol de données – la cyber-criminalité appliquée au sport

Le Tour de France 2015 va-t-il connaître son premier cyber scandale ? C'est en tout cas ce que l'on peut supposer après la divulgation de certaines données de performances du cycliste Crhis Froome qui ont été dérobées, estime Tanguy de Coatpont, directeur général France & Afrique du nord de Kaspersky Lab qui partage son analyse.

« Depuis plusieurs années, le sport connaît un engouement croissant auprès des publicitaires et des entreprises qui y investissent massivement, attirant par conséquent des cybercriminels poussés par l'appât du gain ou une volonté de nuire. Il n'est également pas difficile d'imaginer les conséquences psychologiques que peut avoir un vol de données sur un athlète dont le succès repose en partie sur sa concentration.
Les rumeurs concernant le possible piratage des données sportives de Chris Froome viennent nous rappeler que de nombreux aspects de la vie moderne, y compris le sport de haut niveau, sont de plus en plus connectés. Il y a quelques années, l'idée que les données d'un coureur du Tour de France soient dérobées aurait semblée anecdotique mais avec l'avancée des technologies et l'émergence des solutions d'analyse des performances qui sont aujourd'hui critiques à l'entraînement de nombreux sportifs, ce n'est plus surprenant. Ces sportifs doivent également faire face à une autre réalité : alors qu'ils sont maintenant élevés au rang de célébrités, les informations concernant leurs performances intéressent tout autant que celles qui concernent leur vie privée.
En sachant cela, tout individu ou entreprise doit prendre les mesures qui s'imposent pour protéger ses données informatiques. Même lors d'événements sportifs, où les données doivent être transmises et analysées quasiment en temps réel, il est impératif de prendre en compte les questions de sécurité informatique pour protéger les informations sensibles que sont les performances des athlètes mais également protéger les systèmes sur lesquels elles transitent.
Le partenariat entre Kaspersky Lab et l'écurie de Formule 1 de Ferrari nous a permis de mieux comprendre les défis auxquels ils sont confrontés pour sécuriser les données transmises lors des courses. Pour Ferrari, une solution de sécurité efficace est vitale afin de protéger les données qui sont une source d'information essentielle à l'équipe. Elles transitent très rapidement pour éviter d'être compromises et la solution de sécurité ne doit pas augmenter le temps de latence. Il n'est pas difficile d'imaginer que les contraintes de complexité et de performance sont similaires dans d'autres sports comme le cyclisme professionnel. »

Source : http://www.itrmanager.com/articles/157190/cyclisme-vol-donnees-cyber-criminalite-appliquee-sport.html

Prévention des risques : les dispositifs d’alerte à la population | Le Net Expert Informatique

Prévention des risques : les dispositifs d’alerte à la population

Face aux risques (inondation, canicule, attaque terroriste, incident nucléaire, épidémie…) susceptibles de mettre en danger les populations, les maires peuvent constituer deux registres nominatifs destinés à faciliter les secours. La Commission nationale de l'informatique et des libertés (Cnil) fournit un cadre à la constitution de ces registres qui ne doivent pas être prétextes à la création de « fichiers de population ».

L'utilisation des ces registres est strictement limitée aux secours déclenchés par le maire en cas d'alerte. Les habitants doivent avoir sollicité leur inscription par une démarche volontaire.

Pour la collecte des informations nécessaires, la Cnil a établi deux formulaires :
l'un au titre du « plan d'alerte et d'urgence au profit des personnes âgées et des personnes handicapées en cas de risques exceptionnels ». Il s'agit d'une reprise du « registre canicule » prévu par le décret n° 2004-926 « canicule », abrogé par le décret n° 2005-1135 ; (http://www.courrierdesmaires.fr/wp-content/uploads/2015/06/plan-urgence-formulaire-collecte-modele.doc)
l'autre au titre du « plan communal de sauvegarde » (PCS), dispositif d'alerte générale à la population pour faire face à la réalisation de risques connus auxquels est soumis un territoire communal (décret n°2005-1156).
(http://www.courrierdesmaires.fr/wp-content/uploads/2015/06/pcs-formulaire-collecte-modele.doc)
Les registres de population ainsi constitués collectent donc des données personnelles volontairement transmises par les personnes concernées. Celles qui n'y sont pas inscrites ne sont évidemment pas exclues du bénéfice des secours qui seront alors déclenchés.
A noter. Si la collecte de données de santé, souvent constatée, est par principe excessive et passible de sanctions pénales, une description objective des capacités des personnes sur ces registres semble néanmoins pertinente afin de prévoir le mode d'évacuation et le matériel de premiers secours.

Le maire, responsable de traitement, doit garantir la confidentialité et la sécurité des données. Toute personne accédant aux données du registre est tenue au secret. Les données personnelles ne peuvent en aucun cas être utilisées à d'autres fins que celle de constituer et déclencher le dispositif d'alerte.

Source :
http://www.courrierdesmaires.fr/51257/prevention-des-risques-les-dispositifs-dalerte-a-la-population/

La mise en place de la riposte contre la cybercriminalité | Le Net Expert Informatique

La mise en place de la riposte contre la cybercriminalité

Le 08 juillet 2015, c'est-à-dire le mercredi dernier, l'Observateur permanent du Canada au Conseil de l'Europe, Alan Bowman, a déposé l'instrument de ratification de la Convention de Budapest sur la cybercriminalité, faisant ainsi de ce pays le 47ème Etat partie à ce mécanisme international de lutte contre la cybercriminalité.

Au dernier décompte, 07 autres États ont signé la Convention et 12 ont été invités à y adhérer, ce qui porte à 66 le nombre des États Parties ou qui se sont officiellement engagés à devenir Parties au traité.
« La Convention sur la cybercriminalité, aussi connue comme la Convention de Budapest sur la cybercriminalité ou Convention de Budapest, est le premier traité international qui tente d'aborder les crimes informatiques et les crimes dans Internet en harmonisant certaines lois nationales, en améliorant les techniques d'enquêtes et en augmentant la coopération entre les nations. Il a été rédigé par le Conseil de l'Europe avec la participation active d'observateurs délégués du Canada, du Japon et de la Chine.

Qu'est ce que la cybercriminalité ?
À la fin d'août 2011, plusieurs pays européens avaient signé le traité ». Selon une revue de la littérature disponible sur la question, la cybercriminalité reste encore un concept difficile à appréhender. En France, un rapport du groupe de travail interministériel sur la lutte contre la cybercriminalité datant de février 2014 appréhende la question dans toute sa complexité. Au regard de cette complexité, le rapport note que la Commission européenne a du s'en expliquer dans une communication au Parlement européen en date du 22 mai 2007 en ces termes : "Faute d'une définition communément admise de la criminalité dans le cyberespace, les termes 'cybercriminalité', 'criminalité informatique' ou 'criminalité liée à la haute technologie' sont souvent utilisés indifféremment".
La question préoccupe aussi l'OCDE selon laquelle « la cybercriminalité renvoie à tout comportement illégal contraire à l'éthique ou non autorisé qui concerne le traitement automatique de données et/ou de transmissions de données ».

Que dit l'ONU ?
Pour l'organisation mondiale, tombe sous le coup de la cybercriminalité « tout comportement illégal faisant intervenir des opérations électroniques qui visent la sécurité des systèmes informatiques et des données qu'ils traitent ». Pour autant qu'elle offre des outils juridiques susceptibles d'aider les pays à enquêter sur la criminalité informatique et de poursuivre en justice les auteurs de ce crime, la Convention de Budapest est un instrument qui mérite une large vulgarisation surtout en ces temps de guerre asymétrique à l'échelle planétaire.
C'est une simple question de bon sens quand on sait que seule la coopération entre Etats est susceptible de porter un coup d'arrêt à cette nouvelle forme de criminalité aux conséquences imprévisibles. Mais un survol rapide de la liste des Etats parties ou qui s'apprêtent à y adhérer permet de réaliser, là aussi, que l'Afrique est encore à la traine. Alors qu'on arrête de geindre si les autres réfléchissent à notre place et nous imposent leurs quatre volontés.

Source : http://malijet.com/la_societe_malienne_aujourdhui/132840-chronique-du-web-la-riposte-contre-la-cybercriminalite-se-met-en.html

Avis trimestriel N° 02-2015 de la Commission de protection des données personnelles du Sénégal (CDP) | Le Net Expert Informatique

	Avis trimestriel N° 02-2015 de la Commission de protection des données personnelles du Sénégal (CDP)

Le présent avis trimestriel de la CDP concerne la période allant du 1er avril au 30 juin 2015. Il décrit les activités au sein de la Commission et les constats sur le traitement des données personnelles par les acteurs des secteurs public et privé au Sénégal.

La Commission publie ainsi ledit avis trimestriel conformément à l'article 43 de son Règlement intérieur et après en avoir délibéré en sa séance plénière du 10 juillet 2015.

1 – Compte rendu des activités :
Au cours de ce deuxième trimestre 2015, la CDP a constaté une meilleure prise de conscience des responsables de traitement. En effet, 38 structures se sont rapprochées de l'Autorité de protection afin de mieux s'imprégner de la législation et de connaitre leurs obligations déclaratives.
La Commission a traité 134 dossiers dont 89 déclarations et 45 demandes d'autorisation. A l'issue des 06 sessions plénières, les commissaires ont délivré 54 récépissés de déclaration et 28 autorisations.
Au titre des signalements et des plaintes, la CDP a enregistré l'usage illégitime de numéros courts, une arnaque sur le réseau d'un opérateur de télécommunications, la collecte non autorisée d'empreintes digitales dans un système financier décentralisé, la diffusion de fausses nouvelles, l'arnaque et le chantage sur le net, l'utilisation abusive et sans autorisation de photos et la publication dans la presse de données personnelles d'employés sans leur consentement. Ces cas d'atteinte à la vie privée ont donné lieu à des demandes d'explication qui ont abouti à des déclarations et régularisations devant la CDP. Par ailleurs, la CDP a prononcé un (01) avertissement à l'endroit d'une structure pour envoi répété de courriels et de SMS non sollicités sans mise à disposition d'une possibilité de désabonnement fonctionnel.
Dans le cadre de sa mission de sensibilisation, la Commission a initié des visites de courtoisie auprès d'acteurs institutionnels. C'est ainsi qu'elle a été reçue par la Cellule Nationale de Traitement des Informations Financières(CENTIF), l'Agence nationale de la Banque Centrale des Etats de l'Afrique de l'Ouest(BCEAO), l'Office national de Lutte contre la Fraude et la Corruption(OFNAC) et en fin le Conseil Economique Social et Environnemental(CESE). De même, la phase pilote de la campagne de sensibilisation ''Internet, c'est moi qui décide'' a été lancée en partenariat avec la société Computech Groupe au sein d'établissements secondaires de Dakar.
Enfin, la CDP a organisé un Forum africain sur la protection des données personnelles (FAPDP 2015) à Dakar les 19 et 20 mai 2015. Cet évènement a enregistré la participation de plus de 350 personnes dont des autorités de protection de 13 pays africains (33 délégués), le Conseil de l'Europe et l'Association francophone des autorités de protection des données personnelles (AFAPDP).

2 – Observations /constats :
A l'examen des dossiers reçus à la CDP, des manquements ont été relevés dans le traitement des données personnelles de quelques structures.

Du point de vue juridique, on note :
• l'installation dans un lieu de travail d'un nombre disproportionné de caméras de surveillance;
• le non-respect des conditions de la prospection directe notamment, les droits des personnes concernées (consentement, opposition, etc.) ;
• le non accomplissement des formalités déclaratives devant la CDP préalables au traitement des données ;
• la durée illimitée de conservation des données traitées ;
• l'absence d'engagement de confidentialité entre le responsable de traitement et son sous-traitant.

Sur le plan technique, la pratique de l'externalisation reste une préoccupation pour la Commission. Cette situation constitue un défi supplémentaire pour la protection des données en ce sens que le responsable de traitement n'a plus le total contrôle de son système d'information.

Concernant le traitement des données sensibles comme les données de santé et la biométrie, les responsables de traitement devraient mettre une authentification forte au lieu de recourir simplement à un login et un mot de passe.

Enfin, il a été relevé dans certaines structures, l'absence de politique formalisée d'accès aux données et de mécanismes de sensibilisation des usagers sur les mesures de sécurité mises en place. Il est important que de telles dispositions soient prises par le responsable de traitement conformément à l'article 71 de la loi n° 2008-12 du 25 janvier 2008 portant sur les données à caractère personnel et la délibération n°2014-014/CDP du 3 avril 2014 portant sur les mesures de sécurité applicables aux traitements des données à caractère personnel.

3 – Recommandations :
Au regard des constats à l'examen des dossiers instruits, la CDP formule au profit de toutes les parties prenantes, les responsables de traitement du secteur public, du secteur privé, des organismes de la société civile et autres acteurs, les recommandations suivantes :

• Préciser le lieu exact (ville ou pays) de stockage du serveur contenant les données selon qu'il appartient à la structure ou à l'hébergeur (serveur mutualisé, serveur dédié);
• Signer obligatoirement un engagement de confidentialité en cas d'intervention d'un tiers dans le système mis en place afin d'augmenter le niveau de sécurité des données;
• Utiliser un langage codé et accessible uniquement au corps médical pour les dossiers de santé et mettre en place une authentification forte dans le cadre de la collecte de données de santé;
• Informer les personnes concernées de la présence de caméras de vidéosurveillance (affiches avec indication du numéro du récépissé de la CDP, panneau de signalement) et veiller à positionner les caméras uniquement sur les parties communes et s'assurer que les parties privées ne soient pas filmées;
• Désinscrire gratuitement et systématiquement, dans le cadre de la prospection commerciale, les personnes qui en font la demande avec effet immédiat;
• Veiller à assurer une protection des données transférées dans des serveurs à l'étranger en mettant en place des mécanismes de sauvegarde et de réplication/duplication;
• Recueillir le consentement, libre et éclairé des personnes qui font l'objet de prospection, tout comme le consentement des personnes concernées avant toute publication ou communication à des tiers de leurs données personnelles (photos, vidéos, etc.);
• Ne pas publier dans la presse des décisions individuelles mettant en cause les employés/salariés sans leur consentement;
• Saisir la CDP pour la suppression de tout contenu pouvant nuire à la réputation des personnes;
• Etre prudent sur les informations à communiquer sur les réseaux sociaux;
• Se rapprocher de la CDP pour une meilleure connaissance de la législation sénégalaise sur la protection des données personnelles.

Source : http://www.actusen.com/avis-trimestriel-n-02-2015-de-la-commission-de-protection-des-donnees-personnelles-du-senegal-cdp/#