La cybersécurité a-t-elle une obligation de résultat ?

La cybersécurité a-t-elle une obligation de résultat ?

Obligation de résultat ou obligation de moyens : qu'est-ce que cela implique en matière de cybersécurité ? Olivier Iteanu, avocat à la Cour (www.iteanu.com), nous livre son analyse et revient sur la sanction infligée à Orange par la Cnil.

Chacun conviendra qu'il est absurde de considérer que la sécurité en général, et plus particulièrement celle attachée aux systèmes d'information, soit soumise à une obligation de résultat. Aucune technologie, aucun système de défense n'est capable de garantir une fiabilité à 100 % contre toute attaque. L'éditeur d'une solution ou le prestataire qui prétendrait le contraire serait tout simplement un menteur. L'esprit humain est ainsi fait, et c'est tant mieux, qu'un jour ou l'autre, l'attaquant, venu de l'extérieur ou plus encore, de l'interne, trouve le moyen de contourner les meilleures protections techniques et organisationnelles mises en place.
Le pendant de l'obligation de résultat ou son contraire, est l'obligation de moyens. Dans le cas de l'obligation de moyens, si l'attaque a causé des dommages à des tiers, ceux-ci ne peuvent se retourner contre le maître du système attaqué pour obtenir réparation que si une négligence ou une faute prouvées peut être retenue contre lui. Dans le cas de l'obligation de résultat, le tiers n'aura qu'à démontrer l'existence de l'attaque et son dommage, pour engager la responsabilité du maître du système, sans même avoir à démontrer que ce dernier a commis une faute. Evidemment, on comprend ici que les conséquences de l'un ou de l'autre régime juridique sont radicalement différentes.
On est en droit de se demander si le système plein de bon sens de l'obligation de moyens en matière de cybersécurité, n'est pas remis en cause par une décision récente de la Commission Nationale de l'Informatique et des Libertés du 7 août 2014, qui a sanctionné Orange pour manquement à l'obligation de sécurité prévue à la Loi informatique et libertés.
http://www.cnil.fr/fileadmin/documents/approfondir/deliberations/Formation_contentieuse/D2014-298_avertissement_ORANGE.pdf

Que dit la loi ?
Pour mémoire, la Loi du 6 janvier 1978 en son article 34 prévoit que « Le responsable du traitement est tenu 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. » Le défaut de prendre « toutes précautions utiles » est sanctionné des peines maximales de 5 ans de prison et de 300 000 € d'amende par l'article 226-17 du Code pénal. Et comme la matière informatique et libertés prévoit une double peine aux contrevenants à la Loi, la Cnil peut également prendre une sanction dite administrative à l'encontre du responsable du traitement défaillant. Les sanctions de la Cnil peuvent être pécuniaires, jusqu'à 300 000 € en cas de récidive et portent surtout atteinte à l'image du condamné, car ces sanctions sont publiques, donnent lieu à publication, et sont régulièrement reprises par la presse et les médias.

Orange attaqué… et condamné
Une décision récente de la Commission Nationale de l'Informatique et des Libertés du 7 août 2014 a sanctionné Orange pour manquement à l'obligation de sécurité prévue à la Loi informatique et libertés. Dans l'affaire jugée, Orange était alertée en mars 2014 par un client et découvrait que le serveur d'un prestataire de l'opérateur « chargé de réaliser certaines campagnes de marketing direct » par courriel avait été piraté. Plus de 1,3 millions de clients d'Orange étaient impactés par cette attaque. L'enquête révélait qu'Orange avait confié à un premier prestataire la mission de réaliser des campagnes de emailing auprès de ces clients. Ce prestataire avait lui-même sous-traité la prestation à un prestataire secondaire. C'est ce dernier qui était piraté.

Le lien de désinscription, qui se trouvait au bas du courriel de prospection, menait par une modification de l'URL aux 700 fichiers de prospects et de clients d'Orange, permettant à l'indélicat à les aspirer. Le 25 avril 2014, Orange notifiait la faille de sécurité à la Cnil comme elle y est contrainte depuis le Paquet Télécom d'août 2011 et un Règlement 611/2013 de la Commission européenne du 24 juin 2013. Le 5 mai 2014, la presse s'emparait de l'affaire. Une semaine plus tard, la Cnil diligentait sur deux jours un contrôle dans les locaux d'Orange qui révélait les circonstances dans lesquelles les 700 fichiers de clients et prospects avaient été aspirés. Orange déposait une plainte pénale. Mais Orange était également convoquée devant la formation contentieuse dite restreinte de la Cnil, qui lui infligeait un avertissement public le 9 août 2014 pour manquement à l'obligation de sécurité.

Orange se trouvait donc à la fois victime et responsable. Ce qui nous interpelle dans cette décision, ce sont les motifs retenus par la Cnil pour sanctionner Orange. Le premier grief est que selon l'autorité française, Orange « n'a pas fait réaliser d'audit de sécurité sur la version de l'application technique spécifiquement développée par son prestataire secondaire. » Face à la généralité de l'obligation imposée par la Cnil, on cherche désespérément la base légale à ce grief. Mais à supposer celui-ci fondé, on peut penser que le prestataire secondaire a, quant à lui et en sa qualité de professionnel, procédé à cet audit. Tenir Orange, le client dans cette relation, responsable au motif qu'elle n'a pas procédé à cet audit devrait glacer le sang de tous les clients utilisateurs. Le second motif nous paraît, quant à lui, lunaire. La Cnil reproche à Orange d'avoir « communiqué de manière non sécurisé les mises à jour de ses clients » à ses prestataires. L'enquête avait certes révélé qu'Orange avait transmis les 700 fichiers de ses clients et prospects par simple courriel, mais la même enquête a établi que ce n'est pas durant cette communication que les fichiers ont été captés. Cette communication ne serait donc pas en cause. Enfin, la Cnil reproche à Orange « qu'aucune clause de sécurité et de confidentialité des données n'était imposée à son prestataire secondaire »,c'est-à-dire au sous-traitant du sous-traitant d'Orange, c'est-à-dire la société avec laquelle elle n'a pas de contrat … C'est compte tenu de ces « défaillances » que la Cnil entre en voie de condamnation à l'encontre d'Orange.

Cette décision nous amène à deux commentaires sous formes de conclusions.
D'une part, il y a un auteur à cette infraction, « quelque part dans le monde » qui a accédé illicitement aux serveurs et a procédé à l'aspiration des fichiers. Les adresses IP relevées par les serveurs du prestataire attaqué ont désigné des pays lointains. Dans ce genre d'affaires, l'enquête judiciaire est souvent en panne. L'enquête bute en effet sur des difficultés de coopérations policières et judiciaires en termes de délais, de paperasserie et de coûts quasi insurmontables, sans compter que certains pays ne coopèrent tout simplement pas. Dans ce contexte, le seul condamné de l'histoire a toutes les chances d'être la victime, Orange. Il y a tout de même ici quelque chose de choquant sur le fond. En outre, c'est Orange qui a notifié elle-même la faille à la Cnil par application de la Loi certes. Si chaque notification donne lieu à condamnation de son auteur, ceux-ci risquent désormais de réfléchir à deux fois avant de se lancer dans ce qui apparaît comme « la gueule du loup ».

D'autre part, les griefs retenus à l'encontre d'Orange nous paraissent d'une interprétation des plus sévères des précautions utiles de l'article 34 de la Loi de 1978 et surtout très généraux, laissant dans le désarroi et l'insécurité juridique tous utilisateurs des systèmes d'information et de leurs services. Enfin, faire tenir Orange responsable des agissements du sous-traitant de son sous-traitant paraît déraisonnable.

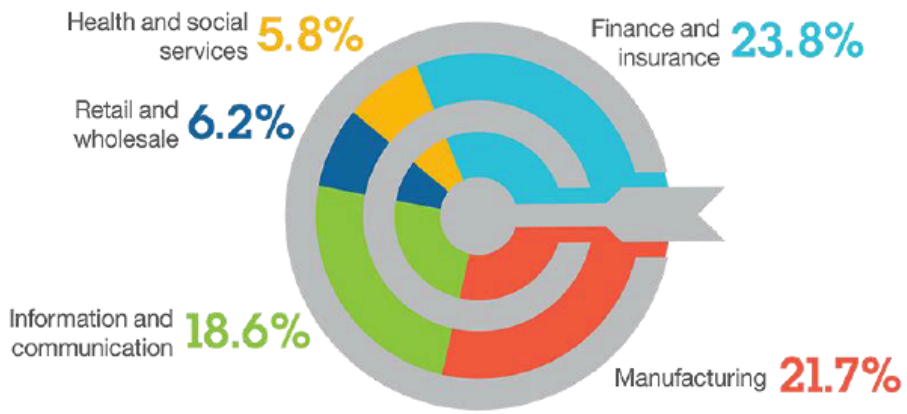
En conclusion, on a le sentiment ici que le cri des victimes et des médias a couvert tout raisonnement juridique. Il fallait un responsable. L'auteur de l'infraction introuvable, c'est sur la victime qu'on se rabat. C'est un mode de fonctionnement regrettable sur le plan des principes et qui ne devrait pas se généraliser.

A défaut, oui, la cybersécurité deviendrait synonyme d'obligation de résultat.

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

Source : http://www.solutions-logiciels.com/actualites.php?titre=La-cybersecurite-a-t-elle-une-obligation-de-resultat-&actu=15232
par Juliette Paoli

Cyber sécurité : Le Maroc doit bien s'armer



Cybersécurité : Le Maroc doit bien s'armer

Le coût de la cybercriminalité dans le monde s'est chiffré en 2013 à 350 milliards de dollars*. Au-delà de l'enjeu économique colossal, la multiplication des cyber-attaques et de quelques cyber-guerres pose la question du «contrôle» de ce nouvel espace de souveraineté, créé par l'Homme.

Le Maroc classé 49e pays mondial à risque en matière de sécurité Internet et 3e au niveau africain dans le dernier rapport de Symantec (Symantec Corporation – Internet Security Threat Report 2013). Le risque d'une attaque virtuelle est bien réel, et les PME sont les premières cibles des cyberattaquants.
Au Maroc, le niveau des organisations marocaines par rapport à la norme ISO 27002 est encore trop faible. En effet, rares sont les entreprises marocaines ayant mis en place à ce jour une Politique de Sécurité des Systèmes d'Information (PSSI).
Pourtant la protection face aux cyber-menaces et leur évolution constante (globalisation, …) apparaît comme une initiative majeure : les attaques informatiques contre les infrastructures nationales représentent des menaces réelles. La prévention et la réaction aux attaques informatiques sont une priorité absolue des dispositifs de cyber-sécurité, en particulier les structures organisationnelles.

Aujourd'hui, les entreprises repensent leurs tactiques de cybersécurité
Selon l'étude IBM CISO (Chief Information Security Officer) parue en décembre 2014 qui visait à découvrir et à comprendre comment les entreprises se protègent actuellement contre les cyber-attaques. Elle révèle que 70% des responsables de la sécurité pensent avoir des technologies traditionnelles matures, qui mettent l'accent sur la prévention des intrusions réseau, la détection avancée des logiciels malveillants et l'analyse de la vulnérabilité du réseau.
Cependant, près de 50% reconnaissent que le déploiement de nouvelles technologies de sécurité est prioritaire pour leur entreprise. Ils ont identifié trois principaux domaines nécessitant un changement drastique : la prévention des fuites de données, la sécurité du Cloud et la sécurité des appareils et des mobiles.

Toujours selon l'étude IBM CISO :
La sécurité du Cloud reste en tête de l'ordre du jour : bien que la préoccupation liée à la sécurité du Cloud reste forte, près de 90% des personnes interrogées ont adopté le Cloud ou sont actuellement en train de mettre en place des initiatives en la matière. Dans ce groupe, 75% des responsables s'attendent à voir leur budget dédié à la sécurité du Cloud augmenter, voire de manière significative dans les 3 à 5 ans à venir.
La sécurité intelligente basée sur l'analyse des données est prioritaire : plus de 70% des responsables de la sécurité déclarent que les renseignements de sécurité en temps réel sont de plus en plus importants pour leur entreprise. Malgré cette constatation, l'étude révèle que des domaines tels que la classification et la découverte des données ainsi que l'analyse des renseignements de sécurité sont relativement peu matures (54%) et ont fortement besoin d'être améliorés ou transformés.
Les besoins dans la sécurité mobile restent importants : malgré une main-d'oeuvre de plus en plus mobile, seulement 45% des responsables de la sécurité déclarent qu'ils ont une approche efficace de la gestion des terminaux mobiles. En fait, selon l'étude, lorsque l'on adresse le sujet de la maturité, la sécurité des mobiles et des appareils arrive en fin de liste (51%).

Au Maroc, les structures organisationnelles s'organisent
La nouvelle stratégie "Maroc Numeric 2020" que le ministère de l'Industrie, du commerce, de l'investissement et de l'économie numérique, est en train de préparer, devra continuer à positionner le Maroc comme un hub technologique régional, en réalisant des progrès en termes de "transformation sociale" et d'accompagnement de l'entreprise et des différents chantiers de l'E-gouvernement. Surtout ce dernier, s'inscrit dans la poursuite des progrès réalisés depuis des années en matière des technologies de l'information, de sécurité en continuant à positionner le Maroc comme hub régional et à fournir des services aussi bien au citoyen qu'à l'entreprise, particulièrement la Petite et Moyenne.

Les PME, cible privilégiée et pourtant…
Paradoxalement alors que le Maroc est 3,5 fois plus vulnérable aux logiciels malveillants que la moyenne mondiale**, les PMEs, 1er tissu économique marocain, la cyber-criminalité, les défaillances techniques ou informatiques sont peu préoccupantes et donc peu prises en compte.

IBM a bien compris les enjeux de la sécurité des données en entreprise : « ces nouvelles offres sont conçues pour protéger les données et applications vitales de l'entreprise grâce à des techniques analytiques avancées, développées au sein même de l'entreprise, dans les clouds publics et privés, et dans les terminaux mobiles. » Actuellement, 75% des failles de sécurité nécessitent plusieurs jours, semaines voire mois pour être détectées, ce qui peut causer d'importants dommages.

Une gestion proactive de la sécurité par IBM
Les solutions proposées par IBM devraient permettre d'apporter une vue d'ensemble de l'état de la sécurité informatique, pour savoir qui utilise le cloud et de quelle façon. Les nouveaux outils peuvent être déployés dans le cloud ou sur site, pour s'adapter aux environnements informatiques des entreprises. Par ailleurs, les éventuelles menaces peuvent être identifiées en temps réel, grâce aux données d'analyse mises à disposition par IBM, appuyées sur 20 milliards d'événements quotidiens repérés dans plus de 130 pays***

Les offres de sécurité IBM apportent la sécurité intelligente pour aider les organisations à protéger les personnes, les données, les applications et les infrastructures. Les solutions IBM couvrent la gestion des identités et des accès, le SIEM (Security Information and Event Management), la sécurité des données, la sécurité des applications, la gestion du risque, la gestion des terminaux, la nouvelle génération de protection contre les intrusions, la lutte contre la fraude financière avec le rachat de Trusteer et d'autres sujets. IBM dispose d'une des plus importantes organisations de recherche et développement et de mise en oeuvre dans le domaine de la sécurité.

La cybercriminalité reste la deuxième forme la plus répandue de criminalité économique selon PwC;
La cyber-criminalité coûterait **327 milliards d'euros** par an. Selon un rapport publié par le « Center for Strategic and International Studies »;
 65% des utilisateurs d'internet ont été victimes d'une cyberattaque (virus, fraude à la carte de crédit en ligne, vol d'identité)- Soit 1.5 millions de personnes par jour (Mashable); Aux Etats-Unis, 40 millions de personnes ont été victimes de vols de données personnelles.

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

Source : http://lobservateurdumaroc.info/2014/12/23/cyber-securite-le-maroc-doit-bien-sarmer/
* (Le coût des failles informatiques selon l'étude menée pour le compte de Microsoft en 2013, par l'observatoire IDC (International Data Corporation)
** Source Microsoft
*** Source http://ibm.com/fr/security

Wifi en libre accès : conseils pour ne pas se faire épingler par la Cnil pour « des manquements récurrents »

Wifi en accès libre : conseils pour ne pas se faire épingler par la Cnil pour « des manquements récurrents »

La Commission nationale de l'informatique et des libertés (Cnil) a de bons côtés, parmi lesquels sa volonté inébranlable de garder la pêche. Chaque jour que Dieu fait, elle constate des entorses aux règles qu'elle est censée faire respecter, mais ne se décourage pas.

Nouvel exemple : l'autorité administrative indépendante a contrôlé des points où internet est disponible en libre accès – restaurants, hôtels, bibliothèques – via le wifi ou des postes informatiques dédiés. Sans surprise, elle a découvert « des manquements récurrents » :
• de nombreux opérateurs « conservent des données portant sur le contenu des correspondances échangées ou des informations consultées (URL) alors qu'ils ne sont pas autorisés à le faire » ;
• ils ne doivent conserver que les données de connexion, pendant un an. Or, la plupart les gardent indéfiniment ;
• les utilisateurs sont mal informés ;
• plusieurs opérateurs utilisent « des outils de surveillance » des postes informatiques comme la « prise en main à distance » et le « contrôle de l'historique de navigation ». C'est-à-dire qu'ils ont accès, de fait à des données sensibles : « identifiants-mots de passe, numéros de compte bancaire, etc ». La Cnil aimerait qu'ils arrêtent.
• les réseaux wifi, sans chiffrement et facilement accessibles, sont de vraies passoires. Il n'est pas difficile d'en prendre le contrôle.
Plutôt que de paniquer devant tant d'amateurisme, la Cnil garde le cap et donne cinq conseils pour améliorer les choses.

Au restaurant, à l'hôtel ou dans les bibliothèques, il est souvent possible d'utiliser un réseau internet wi-fi ou des postes informatiques en libre accès.
La CNIL a décidé d'intégrer dans son programme annuel des contrôles la thématique de l'internet en libre accès. Elle a effectué plusieurs contrôles des modalités de mise en œuvre de ce type de service auprès d'organismes privés et publics.

Lors de ces contrôles, l'attention de la CNIL a principalement porté sur :
• le type de données collectées,
• leur conservation,
• le niveau d'information des utilisateurs
• la qualité des mesures de sécurité qui y sont associées.

Plusieurs manquements récurrents ont été identifiés lors de ces contrôles. Au vu de ces constations, la CNIL rappelle aux fournisseurs de services d'internet en libre accès les mesures à adopter pour se mettre en conformité.

1. Conserver seulement les données de trafic
Les organismes qui mettent à disposition du public un service de libre accès à internet (postes informatiques, wi-fi, etc.) sont considérés comme opérateurs de communications électroniques (OCE) et sont soumis aux obligations prévues à l'article L. 34-1 du code des postes et des communications électroniques (CPCE). A ce titre, ils doivent conserver les données de trafic répondant aux » besoins de la recherche, de la constatation et de la poursuite des infractions pénales » et destinées aux autorités légalement habilitées.
La CNIL a constaté lors des contrôles que de nombreux opérateurs de communication électronique conservaient des données portant sur le contenu des correspondances échangées ou des informations consultées (URLs) alors qu'ils ne sont pas autorisés à le faire (article L. 34-1 VI du CPCE consultable sur http://www.legifrance.gouv.fr/affichCodeArticle.do?cidTexte=LEGITEXT000006070987&idArticle=LEGIARTI000006465770&dateTexte=&categorieLien=cid).
Les fournisseurs de service ne doivent pas collecter de telles données et supprimer celles qui auraient été conservées.

2. Définir une durée de conservation des données limitée et proportionnée
La plupart des fournisseurs de service conservent les données issues des journaux de connexion sans qu'aucune durée de conservation n'ait été définie.
Or, les données de trafic doivent être conservées pendant 1 an à compter du jour de leur enregistrement (Article R. 10-13 du Code des postes et des communications électroniques consultable sur http://legifrance.gouv.fr/affichCodeArticle.do?idArticle=LEGIARTI000006466369&cidTexte=LEGITEXT000006070987&dateTexte=20110909&oldAction=rechCodeArticle)
Les autres données collectées dans le cadre de l'offre d'internet en libre accès, telles que les informations d'abonnement, etc. doivent être supprimées régulièrement (article 6-5° de la loi n°78-17 du 6 janvier 1978 modifiée consultable sur http://www.cnil.fr/documentation/textes-fondateurs/loi78-17/#Article6) lorsqu'elles ne sont plus nécessaires (désinscription ou inutilisation prolongée de l'abonnement).

3. Fournir une information complète sur les traitements de données :
Les contrôleurs de la CNIL ont observé que l'information fournie aux utilisateurs des services d'internet en libre accès, ne s'avérait pas toujours satisfaisante, voire inexistante.
Les opérateurs de communication électronique doivent délivrer une information aux utilisateurs de leur service sur les modalités de traitement de leurs données (article 32 de la loi n°78-17 du 6 janvier 1978 modifiée). Le support de cette information doit être le formulaire d'inscription au service. A défaut, l'information doit être fournie par voie d'affichage, dans une charte informatique, etc. (Voir les modèles de mention d'information sur http://www.cnil.fr/vos-obligations/informations-legales/).
Par ailleurs, les opérateurs de communication électronique doivent prévoir des procédures de gestion des demandes d'accès, de rectification et de suppression des données par leurs utilisateurs (art. 38 à 40 de la loi n°78-17 du 6 janvier 1978 modifiée).

4. Veiller à la conformité des outils utilisés, notamment aux outils de surveillance :
Plusieurs opérateurs de communication électronique contrôlés utilisaient des outils de surveillance afin d'assurer la sécurité des postes informatiques, la gestion des tarifications, les impressions, etc.
L'utilisation de tels outils (consultation ou prise en main à distance, contrôle de l'historique de la navigation, etc.) est susceptible de donner accès à un grand nombre d'informations excessives au regard de la finalité pour laquelle elles sont collectées (identifiants-mots de passe, numéros de compte bancaire, etc). Le recours à de tels outils doit être évité ou un paramétrage limité doit être mis en place.

5. Assurer la confidentialité et la sécurité des données :
Plusieurs lacunes en termes de sécurité et de confidentialité ont été révélées lors des contrôles :
• L'absence de chiffrement des réseaux wi-fi ;
• L'accessibilité du BIOS (absence ou faiblesse du mot de passe) permettant de modifier la configuration basique du système ;
• La possibilité de prendre le contrôle de la machine en démarrant un système d'exploitation depuis une clé USB ; etc.
Pour y remédier, les opérateurs de communication électronique doivent inclure une clause relative à la sécurité des données dans le contrat conclu avec le prestataire réseaux (voir le modèle de clause de confidentialité sur http://www.cnil.fr/documentation/fiches-pratiques/fiche/article/sous-traitance-modeles-de-clauses-de-confidentialite).
Par ailleurs, ils doivent adopter des mesures de sécurité afin de (voir les guides sur » La sécurité des données personnelles » sur http://www.cnil.fr/documentation/guides/) .

Au travers de missions de mise en conformité ou de formation d'un futur correspondant CNIL (Correspondant Informatique et Libertés dit aussi CIL), Denis JACOPINI se charge de mettre en conformité votre établissement avec la Loi Informatique et Libertés auprès de la CNIL.
Vous souhaitez vous mettre en conformité avec la CNIL, contactez-nous

---

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

Source : http://rue89.nouvelobs.com/2014/12/22/wifi-libre-acces-cnil-epingle-manquements-recurrents-256697

STAPLES précise les conditions de la faille informatique dans 115 de ses magasins en août et septembre

STAPLES précise les conditions de la faille informatique dans 115 de ses magasins en août et septembre

Staples a apporté vendredi soir de nouveaux éléments dans le cadre de l'enquête sur la faille de sécurité qui a exposé un mois durant, de mi-août à mi-septembre derniers, des données de paiement de ses clients. L'enseigne américaine de matériel et fournitures de bureau a ainsi indiqué qu'un programme informatique malveillant avait été introduit dans le système de 115 de ses 1 400 points de vente aux Etats-Unis, touchant 1,16 million de transactions par carte bancaire.

Cette cyber-attaque a permis aux pirates de récupérer des noms de clients, mais leur numéro de carte, la date de péremption de celle-ci et leur code de vérification, dans 113 boutiques du 10 août au 16 septembre. Les deux autres magasins touchés ont été exposés aux mêmes indiscrétions du 20 août au 16 septembre.

Au travers de conférences ou de formations, Denis JACOPINI sensibilise des directeurs, des cadres et des salariés aux risques induits par les nouveaux usages de l'informatique en entreprise et dans les collectivités, ainsi que leurs responsabilités pénales.
Contactez-nous

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

Source :
http://www.zonebourse.com/STAPLES-INC-4904/actualite/STAPLES–precise-les-conditions-de-la-faille-informatique-dans-115-de-ses-magasins-en-aout-et-septe-19577610/

Plaidoyer pour une législation spécifique à la cybercriminalité

Plaidoyer pour une législation spécifique à la cybercriminalité

Ordre des avocats au barreau de Tizi Ouzou : Les intervenants ont relevé l'insuffisance des moyens de lutte contre ce phénomène. Ils plaident pour une législation plus significative.

La Cellule de lutte contre le cyber-crime relevant de la Sureté de wilaya de Tizi Ouzou a enregistré 23 infractions en cybercriminalité en 2014, contre 12 en 2013. Ce phénomène est nouveau en Algérie. Les moyens de lutte en termes de législation et des structures existantes s'avèrent «insuffisants», indique-t-on. C'est ce qui ressort d'une journée d'étude sur «la cybercriminalité», organisée par l'Ordre des avocats au barreau de Tizi Ouzou, samedi dernier, au Centre des œuvres sociales. Présenté comme la forme de crime du 21e siècle, ce phénomène s'opère à l'aide des outils des technologies de l'information et de la communication (TIC). Il reste de l'avis des intervenants à cette rencontre «un véritable défi», car les auteurs des infractions susceptibles d'être menées ne sont pas facilement identifiables avec la procédure judiciaire classique actuelle.

Pour ce faire, il faudra «constituer des organes de lutte contre la cybercriminalité. L'Algérie est en retard par rapport à cette question. Il n y a que la gendarmerie et la sûreté nationales qui sont chargées de contrer ce phénomène», soutient Chellat Smaïn, bâtonnier à Tizi Ouzou, en parlant des «aspects juridiques de la cybercriminalité». Et de préconiser : «Il serait intéressant aux législateurs de créer une commission à laquelle on donnera la latitude d'agir, et tous les éléments à même de prévenir ce genre de crimes et d'assister la sureté judiciaire dans l'échange et la coordination des informations», ajoutera l'orateur en donnant l'exemple de structures existantes aux USA (Interpol) et en Europe (Europol). Il n'est pas toujours facile de surveiller, d'identifier où de réunir des preuves nécessaires incriminant le mis en cause, compte tenu, explique le bâtonnier, de l'ampleur du réseau informatique, de l'absence de traces, de la rapidité d'exécution du délit …etc.
S'agissant des attaques, l'atteinte à la vie privée semble la plus répandue. En effet, depuis l'avènement des TIC, les moyens d'attaque informatique sont développés et ont amplifié le phénomène pour devenir transnational. «Où que tu sois, tu peux faire l'objet d'une atteinte à ta vie privée au niveau de n'importe quel point du globe», explique quant à lui, Naït Ali Amrane, avocat et enseignant à la Faculté de droit de Tizi Ouzou, dans sa communication sur : «L'atteinte à la vie privée dans le cadre de la cybercriminalité», en citant des intrusions pour vol des informations personnelles à partir de divers supports de stockage de données.
Aussi, explique-t-il, des informations d'un compte rendu médical ou d'une carte d'assurance sociale peuvent être soustraites illégalement à une personne. Abordant à son tour la question de la lutte contre le phénomène, l'orateur a indiqué qu'à défaut de moyens suffisants, «les adolescents et les enfants doivent être sensibilisés pour prévenir contre ces attaques, car nous ne sommes pas encore prêts pour contrer ce genre de délits», a-t-il ajouté. Cet avis n'est pas partagé par les représentants de la gendarmerie et de la sûreté nationales, puisque dans leurs communications, ils ont abordé l'expérience des services de sécurité dans la lutte contre le cyber crime.

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

Source : http://www.elwatan.com/regions/kabylie/tiziouzou/plaidoyer-pour-une-legislation-specifique-a-la-cybercriminalite-22-12-2014-282428_144.php

---

Des plans de réacteurs nucléaires ont été piratés

Des plans de réacteurs nucléaires ont été piratés

Des documents internes de Korea Hydro & Nuclear Power Co. (KHNP), notamment des plans de réacteurs nucléaires sud-coréens, ont été dérobés et publiés de nouveau vers 1h30 ce dimanche sur Internet, pour la quatrième fois depuis le 15 décembre.

Un internaute, qui serait à l'origine de ces vols de données, a publié sur le réseau social Twitter des documents internes concernant le Réacteur 2 de la centrale de Kori, le Réacteur 1 de la centrale de Wolsong et le manuel informatique utilisé dans les centrales nucléaires du pays.
Le soi-disant «président du groupe antinucléaire à Hawaï» a demandé d'arrêter le fonctionnement des premier et troisième réacteurs à Kori et le deuxième à Wolsong à partir du jour de Noël, en menaçant d'effectuer une deuxième série de «destructions» si les réacteurs ne sont pas arrêtés.
KHNP a indiqué hier que la publication de ces documents qui ne contiennent pas d'informations confidentielles n'affectera pas la sécurité des centrales nucléaires dans un communiqué de presse. La société a néanmoins dit qu'elle effectuerait un exercice de simulation général contre l'éventualité d'une cyberattaque en vue de renforcer ses contre-mesures.
Le ministère du Commerce, de l'Industrie et de l'Energie Yoon Sang-jick a présidé lui aussi une réunion extraordinaire pour vérifier la cybersécurité hier matin suite à la fuite des documents internes en convoquant des chefs d'entreprises publiques spécialisées dans la production d'électricité et d'énergies, dont Korea Electric Power Corp. (KEPCO).

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

Source : http://french.yonhapnews.co.kr/national/2014/12/21/0300000000AFR20141221000200884.HTML

Le régulateur mondial d'internet victime d'une attaque informatique

Le régulateur mondial d'internet victime d'une attaque informatique

Le régulateur mondial d'internet, l'Icann, a annoncé que des pirates informatiques avaient réussi à pénétrer dans ses ordinateurs.

Une attaque par « hameçonnage » a en effet visé l'agence américaine et plusieurs de ses employés ont reçu des courriels destinés à ressembler à ceux envoyés par un de leurs collègues avec une adresse se terminant en « icann.org », selon le blog de l'Icann.

« Plusieurs employés ont vu leurs références dérobées », a précisé l'agence.
L'attaque a, semble-t-il, commencé en novembre. Typiquement, les attaques par hameçonnage sont destinées à duper les gens en les conduisant à cliquer sur des pages factices où ils rentrent leurs adresses et mots de passe, qui sont ainsi récupérés par les pirates informatiques.
Cette ruse a permis aux hackers de récupérer les adresses et mots de passe de plusieurs employés de l'Icann. Ils ont donc pu s'introduire plus avant au sein du système informatique de l'organisation.
Ils ont ainsi pu pénétrer dans des serveurs sécurisés où ils ont récupéré des dossiers sur des noms de domaines, des adresses et des mots de passe d'utilisateurs, a encore indiqué l'Icann.
Le blog et l'annuaire n'ont pas été trafiqués, a encore noté l'Icann sans préciser qui pourrait être à l'origine de l'attaque.
L'Icann, dont la mission est d'attribuer les noms de domaines des sites internet, devrait quitter le giron américain en fin d'année prochaine. Washington a en effet annoncé en mars qu'il pourrait ne pas renouveler son contrat avec la société basée à Los Angeles si un système de contrôle indépendant est en place pour assurer la fiabilité du système d'attribution des adresses.

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

Source :
http://www.7sur7.be/7s7/fr/4134/Internet/article/detail/2156470/2014/12/18/Le-regulateur-mondial-d-internet-victime-d-une-attaque-informatique.dhtml

---

Live streaming illégal : un coût considérable pour l'économie mondiale

Live streaming illégal : un coût considérable pour l'économie mondiale

Une étude du Center for Strategic and Internationals Studies (CSIS) faisait grand bruit lors de sa sortie, en juin dernier. Elle évaluait à 445 milliards de dollars, soit 327 milliards d'euros, le coût global de la cybercriminalité sur l'économie mondiale. S'il semble compliqué de lutter contre ce fléau sans visage, la limitation de certains comportements à risque permettrait de réduire substantiellement la note pour les industries du secteur, mais aussi et surtout pour les internautes. Ainsi en va-t-il du live streaming illégal, plébiscité mais toxique.

Radiographie de la cybercriminalité mondiale

Sans surprise, les pays les plus exposés aux méfaits des cybercriminels sont les grandes puissances. A eux seuls, Etats-Unis, Chine et Allemagne concentrent 200 milliards de pertes dues à des piratages en tout genre, même si essentiellement par vol de propriété intellectuelle.

L'importance des dégâts commis par les hackers est inversement proportionnelle au nombre d'entre eux capables de conceptualiser des programmes permettant d'exploiter des failles logicielles connues (exploits). Selon le Centre de lutte contre la Cybercriminalité d'Europol, seule une centaine de personnes serait responsable de la cybercriminalité dans le monde. Autrement dit, si d'innombrables réseaux cybercriminels s'approprient les kits d'exploits et malwares créés par d'autres, ils ne sont qu'une poignée à pouvoir être considérés comme les cerveaux du hacking international.

Europol précise que ces kits et malwares sont à ce point élaborés qu'ils peuvent facilement être adaptés aux cibles spécifiques des cybercriminels. Des cibles qui sont souvent des entreprises dont les solutions de sécurité laissent à désirer, mais aussi des particuliers, notamment via leur utilisation du live-streaming illégal, véritables supermarchés pour les hackers, qui n'ont qu'à se pencher pour se servir.

Le live streaming illégal, tête de pont de la cybercriminalité mondiale

Début octobre, l'Association of Internet Security Professionals (AISP) se fendait d'un rapport alarmant. Intitulé « Illegal Streaming and Cyber Security Risks : a dangerous status quo ? » il montrait que 500 millions d'ordinateurs étaient infectés dans le monde, soit une infection toutes les 18 secondes.

Concernant les sites de live streaming illégaux, type retransmission de matchs de sport, le rapport de l'AISP se fait très précis. Selon lui, 80 % de ces plateformes hébergeraient des malwares, visant à subtiliser des données confidentielles aux personnes les fréquentant. Avec pour but, in fine, de bombarder leurs boites mails de spams, de subtiliser leurs codes bancaires ou encore d'usurper leur identité.

67 milliards de dollars sont dépensés par an en achat de services de sécurité sur Internet. Cette somme pourrait être considérablement réduite si les internautes prenaient conscience des risques encourus en surfant, par exemple, sur des sites de live streaming illégaux.

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

Source : http://www.actu-economie.com/2014/12/18/live-streaming-illegal-cout-considerable-leconomie-mondiale/
Par Christophe Fourrier

Accord des CNIL européennes: la protection des données personnelles devient « un droit fondamental »

	Accord des CNIL européennes: la protection des données personnelles devient « un droit fondamental »	FrenchWeb.fr

«La protection des données à caractère personnel est un droit fondamental» : C'est ainsi que débute la «Déclaration commune des autorités européennes de protection des données» officialisée lundi 8 décembre par les CNIL européennes. Le texte, adopté depuis le 25 novembre 2014, est une forme de réponse à la défiance des citoyens face à la captation et à l'exploitation de leurs données personnelles. Un sujet de société qui a connu un fort regain d'intérêt depuis les révélations d'Edward Snowden.

«Les données à caractère personnel constituent la particule élémentaire de [du] monde numérique» soulignent les autorités européennes. «Le fonctionnement de l'environnement numérique repose sur des infrastructures informationnelles complexes que des acteurs privés ont développées pour leurs besoins propres. Ceux-ci amassent des quantités gigantesques de données personnelles que certains d'entre eux stockent, traitent et partagent souvent sans laisser à l'individu un niveau de contrôle suffisant et sans être soumis à une supervision effective. Par ailleurs, comme les révélations d'Edward Snowden l'ont récemment dévoilé, des autorités publiques et des services de renseignement ont exigé d'avoir un accès massif à ces infrastructures de données pour d'autres finalités, notamment celle de sécurité nationale.
C'est ainsi que les CNIL justifient cette Déclaration commune: «Le caractère massif et routinier de cet accès a choqué le monde entier. Désormais, le défi consiste à remédier à la crise de confiance que ces révélations ont générée envers les gouvernements (nationaux et étrangers) et les services de renseignement et de surveillance. Il s'agit également de régler la question sous-jacente du contrôle de l'accès à ces quantités gigantesques de données personnelles. Comment construire un cadre qui permette à la fois aux entreprises privées et aux organisations d'innover, d'offrir des produits et services qui répondent aux demandes des consommateurs et aux besoins publics, aux services de surveillance et de renseignement de remplir leurs missions dans le cadre de la loi, et de ne pas sombrer pour autant dans une société de surveillance».
Voici les 15 points clés de la Déclaration:

La protection des données à caractère personnel est un droit fondamental
Les droits des personnes au regard de la protection de leurs données doivent être combinés avec les autres droits fondamentaux

La technologie est un moyen qui doit demeurer au service de l'homme.
La confiance du public dans les produits et services de l'économie numérique dépend en grande partie du respect des règles de protection des données par l'industrie.

La prise de conscience et les droits des personnes doivent être renforcés. [Surveillance à des fins de sécurité]
La surveillance secrète, massive et indiscriminée de personnes en Europe, (…) n'est pas conforme aux Traités et législation européens.

L'accès à des données à caractère personnel aux fins de sécurité n'est pas acceptable dans une société démocratique dès lors qu'il est massif et sans condition.
Le traitement de données personnelles dans le cadre d'activités de surveillance ne peut avoir lieu que dans le cadre de garanties appropriées définies par la loi.

L'autorité publique d'un Etat non membre de l'Union ne peut par principeaccéder directement à des données personnelles couvertes par les règles européennes
Aucune des dispositions figurant dans les instruments européens visant à encadrer les transferts internationaux de données entre parties privées ne peut servir de base légale à des transferts de données vers les autorités de pays tiers pour des finalités de surveillance massive et indiscriminée

Le stockage des données sur le territoire de l'Union est un moyen effectif de faciliter l'exercice de [leur] contrôle.
Les règles de protection des données de l'Union (…) doivent être considérées comme des principes internationaux impératifs en droit international public et privé.

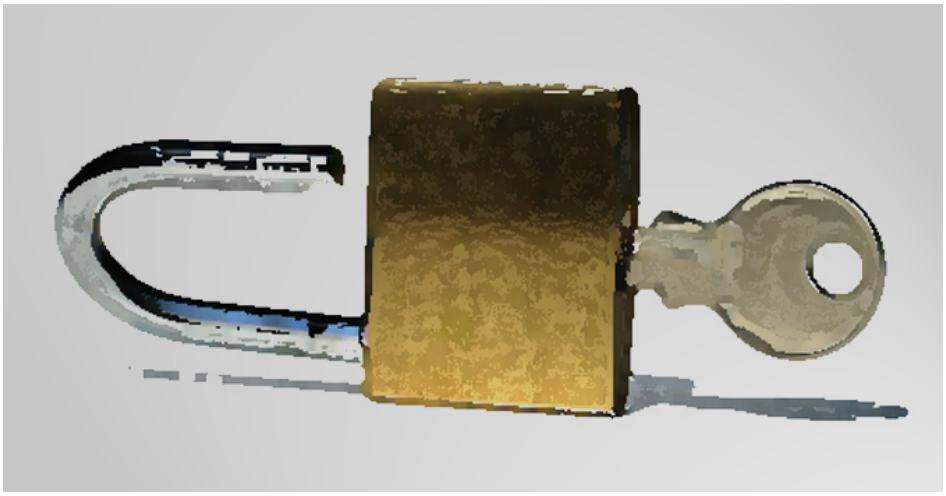
Les projets européens de règlement et de directive relatifs à la protection des données doivent être adoptés en 2015.
Le niveau européen de protection des données ne peut être érodé, en tout ou partie, par des accords bilatéraux ou internationaux, y compris des accords commerciaux sur les biens et services à conclure avec des pays tiers.

L'équilibre à établir entre protection des données, innovation et surveillance n'implique ni de reconstruire les frontières internes de l'Union ni de fermer les portes de l'Europe
Cette Déclaration devrait s'appliquer aux Etats ainsi qu'aux entreprises. Mais n'a pour l'instant aucune application directe au niveau du droit.

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

Source : http://frenchweb.fr/accord-des-cnil-europeennes-la-protection-des-donnees-personnelles-devient-un-droit-fondamental/176535

Les Français choisissent très mal leurs mots de passe



Les Français choisissent très mal leurs mots de passe

Selon Dashlane qui a réalisé une étude statistique basée sur 70 000 utilisateurs dans le monde, les Français seraient en Europe ceux qui choisissent le moins bien leur mot de passe, du point de vue des recommandations sur la sécurité.

Le prestataire Dashlane, qui propose un gestionnaire de mots de passe, a publié les résultats d'une étude réalisée en analysant la robustesse des mots de passe choisis par 70 000 clients sur les différents sites internet où ils s'inscrivent et s'identifient. En moyenne, les Français obtiennent la pire note d'Europe avec 58 points sur 100, loin derrière les 67 points obtenus par les Allemands. La France fait cependant mieux que les Etats-Unis, qui ferme la marche du classement mondial avec seulement 52 points.
Le score est calculé en prenant en compte différents critères positifs ou négatifs comme sa longueur (plus c'est long plus c'est bon), la présence de caractères spéciaux qui évitent les attaques par dictionnaire de mots, ou encore le choix de mots de passe à fuir comme 12345, motdepasse, azerty, etc.
En tirant un peu fort sur les conclusions, la société y voit la manifestation d'une différence culturelle entre des Allemands préoccupés par la protection de leur vie privée du fait de leurs souvenirs de la Stasi, alors que les Américains chercheraient avant tout l'efficacité et la rapidité. « Outre-Rhin, la sensibilité à la sécurité et à la vie privée est très développée tandis qu'aux Etats-Unis les risques sont minimisés au profit des opportunités », analyse Guillaume Desnoes, directeur de Dashlane pour l'Europe.

L'INTERNAUTE N'EST PAS LE COUPABLE
« Concernant la France, outre ses particularités culturelles, il est nécessaire de pointer du doigt le manque de pragmatisme des pouvoirs publics qui agissent peu sur le front de la sécurité en ligne se contentant surtout de publier des alertes. On est loin du modèle britannique où le gouvernement a investi 5M£ par an dans les campagnes « Cyber Streetwise » et « Get Safe Online ! » », dénonce-t-il.
Statistiquement, les femmes en France veilleraient légèrement mieux que les hommes à choisir un mot de passe plus sûr (60 points), et surtout les jeunes semblent mieux sensibilisés, avec un score de 65 points pour les moins de 25 ans. Les scores sont toutefois relativement proches, et dénotent une faiblesse générale dans le choix des mots de passe.
Or c'est une autre étude de Dashlane, beaucoup plus intéressante à nos yeux, qui montrait en juillet dernier la responsabilité des éditeurs de sites internet eux-même dans le choix des mots de passe. Résumée par l'infographie ci-dessous, elle montrait que des sites pourtant très réputés et très sensibles comme Amazon (qui stocke le numéro de carte bleue), Meetic ou ShowroomPrivé avaient une politique beaucoup trop laxiste face aux choix de leurs utilisateurs, alors qu'Apple et Microsoft étaient les meilleurs élèves.

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

Source : http://www.numerama.com/magazine/31636-les-francais-choisissent-tres-mal-leurs-mots-de-passe.html