Téléchargement illégal : un avertissement d’Hadopi, ça calme

Téléchargement illégal : un avertissement d’Hadopi, ça calme

Comme les années précédentes, la Hadopi estime, chiffres à l'appui, que la riposte graduée est efficace et agit sur les comportements – hormis l'achat de contenus légaux. Et non, les abonnés ne se sont pas réfugiés vers d'autres modes de téléchargement.

La question est posée depuis sa création – et l'était même avant : alors, Hadopi, efficace ou pas ? Et la réponse est toujours un peu la même. Durant un temps, l'Autorité a toutefois pu bénéficier du soutien – entier ou non – des ayants droit.
Désireux de voir le gouvernement durcir la législation à l'égard du téléchargement illicite, et de la transférer au CSA, ces derniers se montrent désormais plus acerbes quant aux résultats obtenus par la Hadopi et la riposte graduée. La toute récente étude de l'Alpa en est une bonne illustration.

10% des abonnés avertis une fois récidivent
Et celle qui défend le mieux le bilan de la Hadopi, c'est encore la Hadopi elle-même – sous une précédente majorité, elle pouvait en outre compter sur le soutien du ministre de la Culture. A l'occasion de la dernière publication des chiffres clés de la riposte graduée, la Haute Autorité en arrive donc cette année encore à la même conclusion : ça marche.
Ainsi 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.

Un abonné averti rentrerait donc dans le rang et cesserait de partager illégalement des contenus sur les réseaux P2P. Et selon la Hadopi, un autre chiffre souligne « le caractère dissuasif de la riposte graduée » : la part d'abonnés avertis contactant l'autorité. Ce taux de contact est de 43,5% en phase 3 et de 4,2% après la 1ère recommandation. Un avertissement ça va, trois bonjour les dégâts.

Avertis, 70% diminuent leur consommation illicite
Alors convaincu ? Pas encore ? Pour convaincre les sceptiques (et les autres), la Hadopi a commandé un sondage CSA auprès de 1059 français. Sur ce panel, 47 ont effectivement reçu un 1er avertissement, soit environ 4,4% d'entre eux – donc moins que les 8,9% d'abonnés français à Internet déjà avertis une fois depuis 2010.
Or 70% des destinataires d'un premier avertissement affirment avoir diminué leur « consommation illicite de biens culturels dématérialisés ». Et cette part grimpe même à 88% parmi les 9 français de l'échantillon avertis deux fois. Le sondage n'a pas étudié si cette diminution du téléchargement illicite était oui pérenne ou seulement provisoire.

En revanche, la Hadopi s'est intéressée à une possible évolution des usages en matière de consommation illicite. La riposte graduée ne portant que sur le P2P, les abonnés, en particulier ceux destinataires d'un avertissement, ne seraient-ils pas tentés d'utiliser d'autres moyens, dont le streaming ?

Pas plus de consommateurs ?
D'après les résultats du sondage, la réponse est majoritairement non (73%). D'ailleurs, toujours pour la Hadopi, l'audience, plutôt en baisse des sites de téléchargement (P2P, DDL et streaming), confirmerait cette analyse.
Mais si les internautes ne cherchent a priori pas le moyen de continuer à consommer des contenus piratés, ils ne se précipitent pas non plus sur l'offre légale. Dommage puisqu'il s'agissait d'un des objectifs recherchés par la loi. Après un avertissement, ils sont 23% à déclarer se tourner vers une offre légale.

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

Source : http://www.zdnet.fr/actualites/telechargement-un-avertissement-d-hadopi-ca-calme-39803911.htm
Par Christophe Auffray

La cybercriminalité en débat

La cybercriminalité en débat

Instaurer un organisme spécifique tel qu'une commission nationale indépendante pour la lutte contre la cybercriminalité est l'une des recommandations principales des intervenants, lors de la journée d'étude sur la cybercriminalité organisée le 14 décembre 2014, au centre des œuvres sociales de la wilaya, par l'ordre des avocats au barreau de Tizi-Ouzou.

Une journée où l'aspect préventif et le principe de sensibilisation sur ce phénomène, qui tend à prendre de l'ampleur, ont été mis en avant. Le thème, d'actualité, est un risque auquel il n'est pas possible d'échapper, notamment avec la recrudescence de l'utilisation des outils informatiques et autre procédés de sauvegarde des données issues du développement.

Parmi les intervenants dans cette journée d'étude, et après avoir présenté les aspects juridiques de la cybercriminalité, le bâtonnier, M. Chellat Smaïn, a largement abordé «les structures de lutte contre la cybercriminalité». Il a d'ailleurs profité de l'occasion pour rappeler qu'en Algérie, il n'existe pas de structure ou d'organe bien précis, indépendant et organisé pour la lutte contre ce fléau. Chose qui rend d'ailleurs la lutte contre la cybercriminalité encore plus difficile, estimera-t-il. Le conférencier ajoutera que cette carence se combine au fait que « côté législation les lois existantes ne suffisent pas».
L'intervenant tout en rappelant que la mission est actuellement affectée aux services et équipes de la Gendarmerie et de la Sûreté nationales, a expliqué qu'il serait souhaitable, vu le développement du crime «informatique» que «le législateur mette en place un organe spécifique pour se pencher sur la question».
Le bâtonnier appellera d'ailleurs à la mise en place d'une commission nationale de lutte contre la cybercriminalité. Un organisme comme il en existe d'ailleurs un peu partout dans le monde. L'intervenant cite à cet effet l'exemple des USA avec la création d'Interpol, ou de l'Union européenne avec, entre autres, l'Europol. Une organisation des mécanismes qui facilitera la lutte contre la cybercriminalité, mais aussi, et dans un travail de prévention, permettra de délimiter les infractions commises.
Le bâtonnier classera les crimes informatiques en quatre (04) catégories :
• les infractions informatiques (telle la falsification),
• les infractions du contenu (la pornographie infantile, les propos racistes, la propagande et l'incitation au djihadisme),
• l'atteinte à la propriété culturelle protégée et,
• en dernier lieu, l'atteinte à la confidentialité, à l'intégrité et aux données d'un système donné.
Le bâtonnier a par ailleurs souligné, lors de son intervention, la difficulté de surveiller, de contrôler et de lutter contre le fléau. Ceci, a-t-il expliqué, étant donné que sur le terrain le travail est compliqué par des facteurs spécifiques à la cybercriminalité. Il citera d'ailleurs le caractère vaste du réseau informatique, la rapidité avec laquelle l'infraction est commise ne laissant pratiquement aucune trace, en plus de la difficulté de rassembler des preuves. De son côté, Amrane Naït Ali, avocat et enseignant à la faculté de droit de Boukhalfa, a insisté sur la nécessité d'une large sensibilisation, à l'égard des utilisateurs, notamment les adolescents, des technologies de l'information et de la communication. Une sensibilisation qui permettra de prévenir ce genre de crimes punis par la loi. Au terme de sa communication, inscrite sous le thème de ''L'atteinte à la vie privée dans le cadre de la cybercriminalité'', il affirmera que le danger guette le pays suite à une menace grandissante du crime informatique. Ceci, alors que «notre pays n'est malheureusement pas prêt à y faire face», conclura-t-il.

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

Source : http://www.depechedekabylie.com/evenement/146226-la-cybercriminalite-en-debat.html
Par Tassadit. Ch

La cyber-guerre est déclarée

	La cyber-guerre est déclarée

« La cybercriminalité est un fléau mondial. » Le constat dressé par Jean-Louis Bruguière, Premier Vice-Président honoraire du Tribunal de Grande Instance de Paris, est sans appel. Et l'ancien coordinateur du pôle antiterroriste l'a martelé à la tribune de l'EMLyon, à l'invitation d'Acteurs de l'Économie et du cabinet d'avocats d'affaires CMS Bureau Francis Lefebvre.

Avec la cybercriminalité, une nouvelle forme de guerre est ouverte. « On dénombre près de 120 000 cyber-attaques par jour dans le monde. Et la courbe est exponentielle », selon les chiffres rapportés par Jean-Louis Bruguière. Différentes menaces existent et touchent les États, les entreprises et leurs collaborateurs. Les attaques contre les États et leurs institutions sont généralement l'œuvre d'États étrangers ou d'organismes dépendants de ces États et relèvent d'une véritable cyber-guerre.

Jean Louis Bruguière, 1er vice président honoraire du TGI de Paris, ancien coordinateur du pôle antiterroriste.

Impossible répression

Dans des situations de crise internationale, des stratégies cybernétiques d'attaque émergent. Leurs auteurs sont difficiles à identifier, d'où une impossible répression. De plus, celle-ci nécessite une coopération judiciaire internationale, compliquée à mettre en œuvre. C'est donc en totale impunité que les criminels agissent. « Chine, Corée du Nord, Iran, Russie… les pays agresseurs sont connus », dénonce Jean-Louis Bruguière. Quelles ripostes existent ? Les États européens ont agi en ordre dispersé et moins précocement que les États-Unis. En France, l'Ansi se charge de la lutte contre la cybercriminalité. Cette entité s'est développée de façon rapide et efficace. Mais Internet a profondément bouleversé la stratégie opérationnelle des organisations terroristes, qui ont mis en place des sites web impossibles à décrypter destinés au recrutement des djihadistes ou au maniement des engins explosifs et qui utilisent les réseaux sociaux pour diffuser leur propagande.

Vulnérabilité française

« Les entreprises sont-elles de simples victimes ou doivent-elles se considérer comme de véritables acteurs dans la lutte contre ces attaques ?, interroge Jean-Louis Bruguière. C'est tout l'enjeu de la lutte contre la cybercriminalité. » Les cyber-attaques sont très variées de la part de hackers qui s'adaptent toujours à la riposte. La France figure au 15e rang mondial des attaques, et dans le top 5 européen des attaques ciblées. « La vulnérabilité française vient du fait de la mollesse des cibles nationales », analyse l'ancien juge. Parmi les attaques : le phishing ou hameçonnage, la captation de données, l'interception de communications, le « rançogiciel ».

Culture de la sécurité

Les sociétés attaquées doivent bénéficier du concours des États et de leur fournisseur d'accès pour se protéger. Elles doivent aussi remédier aux failles de sécurité de leur système. La responsabilité des entreprises s'élargit à celle de leurs collaborateurs. « Les collaborateurs doivent prendre conscience du rôle qu'ils ont à jouer dans la sécurité informatique. » Ainsi, ne pas exposer son matériel informatique, générer de solides mots de passes, encadrer l'utilisation des réseaux sociaux. De même, ne pas utiliser des terminaux professionnels dans la sphère privé. « Sachez qu'un smartphone est un espion à distance. »

Gisèle Ducrot, expert en ingenierie et prévention

Typologie du cybercriminel

Répondant à Jean-Louis Bruguière, Gisèle Ducrot, experte en ingénierie et prévention, Philippe Eyraud, président de Mixel Agitateurs, Xavier Vahramian, avocat associé CMS Bureau Francis Lefebvre Lyon, Yves Veret, Senior Advisor de l'information Calao Finance, et André Viau, président de Sofired, ont débattu sous la houlette de Bernard Jacquand. Et sont revenus dans le détail sur la prévention de la cybercriminalité. Selon André Viau, il est difficile d'évaluer les cas de cybercriminalité, « car ils sont peu déclarés ». Les motivations des cybercriminels sont variables : goût du hacking, défense d'une idéologie, recherche de gain. Et Xavier Vahramian de dresser une typologie des attaques : escroqueries, vol de données, y compris par des salariés de l'entreprise, attaques à la réputation des entreprises. Ou de leurs dirigeants, comme le rappelle Philippe Eyraud, victime d'une campagne diffamatoire de la part d'un ancien salarié pour le faire accuser de pédophilie.

Philippe Eyraud, président de Mixel agitateur

Analyse de vulnérabilité

Les entreprises, leurs dirigeants et leurs collaborateurs sont exposés à des menaces sans en avoir vraiment connaissance, déplore Gisèle Ducrot, qui préconise une « nécessaire éducation aux cyber-risques ». « Contre lesquels des solutions existent », rassure Yves Veret, qui insiste sur la nécessité d'utiliser des outils de protection de confiance et certifiés par l'Ansi et préconise de procéder à une analyse systématique de vulnérabilité des systèmes. Car l'entreprise et leurs dirigeants sont responsables de leur cyber-sécurité. Des obligations s'imposent d'ailleurs aux entreprises, rappelle Xavier Vahramian, au titre des lois Informatique et Libertés et celle sur l'Économie numérique, telle la déclaration de fichiers de données personnelles. Et Philippe Eyraud de rappeler la responsabilité du chef d'entreprise quant à la vérification de la nature des données contenues sur ses serveurs, « surtout en cas de contenus illicites téléchargés par des collaborateurs ».

Xavier Vahramian, avocat associé CMS bureau Francis Lefebvre Lyon

Degré d'exposition

Réseaux sociaux, clouding, smartphones… les degrés d'exposition aux cyber-risques sont exponentiels. Cependant, pour Yves Veret, « on ne peut pas fuir l'évolution des technologies, même si elles sont génératrices de risques. Il faut donc être capable de les mesurer pour pouvoir y répondre ». Ainsi, l'externalisation du stockage de données doit être entourée de mesures drastiques de sécurité, insiste Xavier Vahramian. Et André Viau de conclure sur la correspondance des stratégies de défense des espaces cyber et maritimes. Outre la défense embarquée, un système de vigie peut également être mis en place, complété par l'assistance des institutions publiques, jusqu'à la poursuite physique des cybercriminels.

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

Source : http://acteursdeleconomie.latribune.fr/debats/conferences/2014-12-15/la-cyber-guerre-est-declaree.html
Par Nicolas Rousseau

La Corée du Nord totalement coupée d'Internet

La Corée du Nord totalement coupée d'Internet

Quelques jours après que les Etats-Unis ont accusé le régime nord-coréen d'être à l'origine du piratage informatique de Sony Pictures, plusieurs analystes rapportent, lundi 22 décembre, que les connexions Internet en Corée du Nord sont très mal en point, le résultat d'une possible cyberattaque.

Selon la société américaine Dyn Research, spécialisée dans la cybersécurité, les connexions Internet entre la Corée du Nord et le reste du monde ne fonctionnent plus. Doug Madory, chargé des questions internet, explique à l'AFP :
« En général, on détecte de courtes interruptions, mais jamais de problèmes continus de connexion. Je ne serais pas surpris qu'ils soient en train d'encaisser une attaque à l'heure actuelle. »
Interrogée par le New York Times, CloudFlare, une compagnie similaire installée à San Francisco, rapporte que le peu de connexions qui existent en Corée du Nord – officiellement, il y a 1 024 adresses IP selon le régime – sont « cramées ». Ils n'écartent pas un problème technique majeur de routeurs pour expliquer la disparition subite de ces connexions, mais comme le souligne Doug Madory, cette coupure « dure depuis plusieurs heures, et empire au lieu de s'améliorer ».

« PARMI NOS RÉPONSES, CERTAINES SERONT VISIBLES, D'AUTRES PAS »
Le président américain Barack Obama a promis une réponse « proportionnée » à la cyberattaque, la plus grave jamais survenue aux Etats-Unis, sans toutefois en préciser la nature. Lors d'une interview à CNN, dimanche, il a dit qu'il « ne pense pas que cela ait été un acte de guerre [mais] un acte de cyber-vandalisme qui a été très coûteux ».
Au département d'Etat, la porte-parole adjointe, Marie Harf, a dit ne pas être en mesure de pouvoir commenter les informations sur une coupure de l'accès à Internet en Corée du Nord. L'administration Obama « examine une série d'options » pour répondre à la cyberattaque, a-t-elle poursuivi. « Parmi nos réponses, certaines seront visibles, d'autres pas », avait-elle poursuivi.
Comme le souligne le New York Times, si « l'attaque était d'origine américaine, ce que les Etats-Unis ne reconnaîtront probablement jamais, ce serait une tentative inédite des Etats-Unis d'attaquer les connexions Internet d'un pays souverain. Jusqu'ici, la plupart des opérations menées par les Etats-Unis se sont résumées à du cyberespionnage pour collecter des informations ou des communications de personnes soupçonnées de terrorisme ».
Pour le département d'Etat américain, le gouvernement nord-coréen « a une longue histoire en matière de dénégations de responsabilité » et il devrait admettre sa responsabilité, ce que Pyongyang dément fermement. Il propose une enquête conjointe avec les Etats-Unis, assure être en mesure de prouver son innocence et met en garde contre les « graves conséquences » qu'aurait la poursuite des accusations à son encontre.

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

Source : http://www.lemonde.fr/pixels/article/2014/12/22/coupure-massive-de-l-acces-a-internet-en-coree-du-nord_4545129_4408996.html

Chronique de Jawad Kerdoudi, président de l’IMRI: « La cybercriminalité, migration du crime réel vers le virtuel »

	Chronique de Jawad Kerdoudi, président de l’IMRI: « La cybercriminalité, migration du crime réel vers le virtuel »

Comme chaque semaine, l'Institut Marocain des Relations Internationales (IMRI) publie une chronique sur l'actualité. Cette semaine, son président Jawad Kerdoudi s'est intéressé à « La cybercriminalité, migration du crime réel vers le virtuel ».

La récente attaque aux Etats-Unis des systèmes informatiques de Sony Pictures relance le problème de la cybercriminalité. Celle-ci est définie comme l'ensemble des infractions pénales spécifiques liées aux technologies de l'information et de la communication. Ces infractions concernent plusieurs secteurs tels que le « carding » qui porte sur le piratage des cartes bancaires, le « skimming » criminalité qui s'attaque aux automates, le « phising » qui est une pêche des informations bancaires et commerciales, et enfin les escroqueries sur internet de toutes sortes qui englobent la xénophobie, la pedopornographie, l'incitation à l'usage des stupéfiants, le proxenétisme, le terrorisme, et le piratage téléphonique au préjudice des opérateurs.
Ce phénomène prend de plus en plus d'ampleur avec le développement d'internet qui est certes un moyen formidable de communication, mais également un instrument puissant de pouvoir et de guerre. Selon le Computer Crime Research Center, seuls 12% des cybercrimes étaient connus par la police et la justice en 2004. Plusieurs scandales ont défrayé la chronique, dont celui de la NSA en 2013 provoqué par Edward Snowden. Le coût global des cyberattaques a été estimé à 300 milliards d'euros pour les entreprises en 2013. Les Etats-Unis perdent entre 17,5 à 87,5 milliards d'euros par an, et 556 millions de personnes dans le monde ont été victimes de cybercriminalité. Cette situation risque d'empirer du fait du développement extraordinaire des investissements dans le secteur technologique numérique tels que ADSL, L4G, WIFI, Cloud. Le phénomène risque de s'amplifier également par la dématérialisation des processus, le développement du e-commerce et du e-learning, la croissance des paiements en ligne, l'augmentation des utilisateurs du Web qui a enregistré un taux de croissance de 46% entre 2012 et 2013. Le haut lieu mondial de la cybercriminalité pour la création de logiciels malveillants est la Chine, suivie par la Russie, les Etats-Unis, le Brésil et le Royaume-Uni. Pour les machines détournées la première place appartient aux Etats-Unis, suivie par la Chine, la Corée du Sud, l'Allemagne et la France. Enfin par les crimes relatifs aux arnaques sur internet, la palme revient à l'Afrique en particulier la Côte d'Ivoire et le Nigeria.

MINIMISER LES CONSÉQUENCES DE L'ATTAQUE
Pour se protéger contre la cybercriminalité, il est clair que le risque zéro n'existe pas. Il faut faire en sorte que si elle arrive, les conséquences de l'attaque soient minimes. Il faut pour cela renforcer les moyens matériels et humains, procéder à une modification de la législation, développer une culture de l'informatique, et associer le secteur privé à la lutte contre ce fléau. Il faut également privilégier l'approche préventive, c'est-à-dire qu'il faut augmenter les difficultés des attaques en diminuant les profits potentiels. Cela signifié le renforcement de la robustesse des infrastructures informatiques et de télécommunications. Il faut enfin s'appuyer sur des structures de veille et d'alerte telles que le CERT/CC américain. La coopération internationale est indispensable, car les pays qui ne sont pas dotés de lois contre la cybercriminalité sont des paradis numériques, où les cybercriminels peuvent lancer des attaques informatiques ou héberger des sites illicites en toute impunité. Elle a déjà commencé par la Convention de Budapest du 23 Novembre 2001 sur la cybercriminalité qui a le mérite de régler les problèmes de compétence et d'entraide entre Etats, et de les obliger à conserver certaines données pour permettre le traçabilité de l'information. Elle énumère plusieurs infractions (accès illégal, interception illégale, atteinte à l'intégrité des données et des systèmes) pour lesquelles chaque pays doit avoir un volonté politique et une coopération efficace de leurs services de justice et de police. Cette coopération internationale pose le problème de la gouvernance d'internet sur le plan mondial. Certains s'interrogent sur la pertinence d'une réglementation, d'autres demandent qu'elle soit déclarée comme un bien commun, et placée sous le contrôle de l'ONU ou d'un organisme intergouvernemental autonome.

QU'EN EST-IL DE CETTE QUESTION DE LA CYBERCRIMINALITÉ POUR LE MAROC ?
D'après Microsoft, le Maroc est 3,5 fois plus vulnérable aux logiciels malveillants que la moyenne mondiale. Le Maroc présente des failles touchant l'administration et les infrastructures qui constituent des menaces pour la sécurité nationale publique et économique. Preuve en est le piratage à partir du mois d'Octobre 2014 de documents confidentiels marocains relatifs à la diplomatie, au Sahara, et aux services de l'appareil de l'Etat. Le cybercriminel se fait appeler Chris Coleman, sévit sur un compte Twitter et n'a pas caché son objectif de nuire au Maroc. Une lecture officielle de ce cybercrime a été présentée le 11 Décembre 2014 devant la Chambre des Conseillers accusant les services spécialisés algériens d'avoir monté et accompagné cette opération. Dès lors, il faut que la cybercriminalité soit un chantier prioritaire pour le gouvernement, et passe du stade défensif à celui offensif. D'où la nécessité de créer une structure civile placée à un haut niveau, et qui aura par vocation la centralisation des informations et la coordination entre les services civils et militaires. Elle doit disposer également d'un centre de documentation chargé recueillir les statistiques spécifiques en vue de les analyser. Elle devra jouer un rôle opérationnel, signaler les contenus illicites sur internet, et apporter une assistance technique au profit du secteur public et privé. Elle sera également chargée de la formation et de la sensibilisation, et assurera les relations avec les Agences internationales chargées de lutter contre la cybercriminalité.

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

Source : http://www.aufait.ma/2014/12/23/chronique-de-jawad-kerdoudi-president-de-limri-la-cybercriminalite-migration-du-crime-reel-vers-le-virtuel_635947
par Jawad Kerdoudi, président de l'IMRI

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.

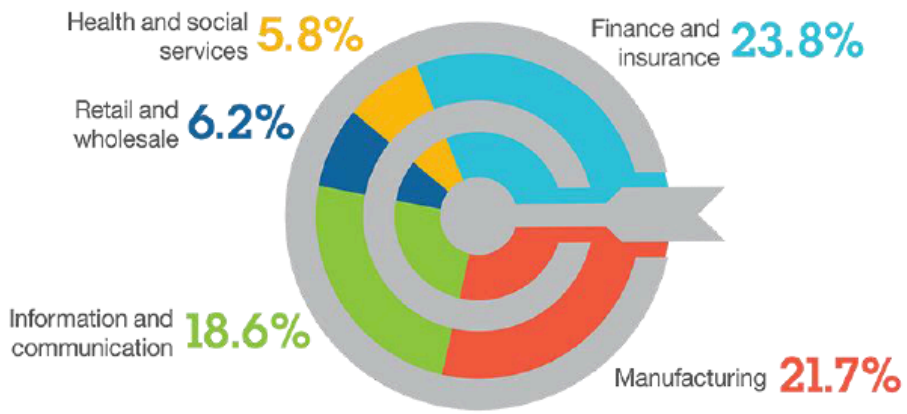
En conclusion, on a le sentiment ici que le cri des victimes et des médias a couvert tout raisonnement juridique. Il fallait un responsable. L'auteur de l'infraction introuvable, c'est sur la victime qu'on se rabat. C'est un mode de fonctionnement regrettable sur le plan des principes et qui ne devrait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

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