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

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

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

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

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

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

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

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

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

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

**Risques liés à la cybercriminalité**

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

**Risque de renvoi ou de poursuites judiciaires**

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

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

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

---

# L'attaque DDoS sur PSN et Xbox Live s'est appuyée sur… des routeurs domestiques

L'attaque DDoS sur PSN et Xbox Live s'est appuyée sur… des routeurs domestiques

**Pour réaliser leurs attaques, les pirates de Lizard Squad ont créé un botnet qui s'appuie en majorité sur des modem-routeurs hackés. Leur malware a exploité une faille dans la configuration du système d'exploitation Linux.**

Fin décembre dernier, les pirates de Lizard Squad ont mis en ligne un service DDoS payant appelé « Lizard Stresser ». Disponible à partir de 5,99 dollars/mois, cet « outil » avait fait ses preuves quelques jours auparavant, en mettant à genoux les réseaux de Playstation Network et Xbox Live. Mais où ces pirates ont-ils trouvé leur puissance de feu ? Principalement dans les petits routeurs domestiques, révèle ainsi KrebsOnSecurity.com.
Avec l'aide de quelques chercheurs en sécurité, le site spécialisé a réussi à mettre la main sur le malware qui a permis de construire le botnet de « Lizard Stresser ». Le logiciel malveillant exploite ainsi une faille de sécurité dans Linux pour prendre le contrôle d'objets connectés, et se diffuse de proche en proche comme un ver.
Après analyse, il s'avère que les routeurs domestiques sont très largement surreprésentés dans ce botnet, sans doute en raison de leur nombre et de leur faible niveau de protection. En effet, l'un des vecteurs d'infection du malware est d'utiliser les identifiants par défauts de ces équipements grand public, tels que « admin/admin » ou « root/12345 » !

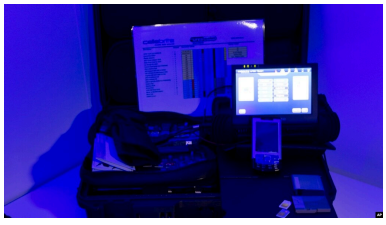
**Lizard Squad a également piraté le cloud de Google**
Cette découverte montre – une fois de plus – qu'il est important de bien configurer et protéger tous ses équipements informatiques, et pas uniquement ses ordinateurs. Selon une récente analyse de l'éditeur Avast, plus de la moitié des modem-routeurs en France ont conservé leur configuration d'origine, et sont donc potentiellement vulnérables. D'ailleurs, se retrouver avec un modem-routeur zombie fait encore partie des choses les moins désagréables. D'autres pirates utilisent des équipements pour réaliser des attaques par détournement DNS, ce qui permet de quantité de données sensibles : mots de passe, informations bancaires, etc.
Mais Lizard Squad ne s'attaque pas seulement aux pauvres particuliers, mais visent également les géants du web. Selon KrebsOnSecurity, les pirates reptiliens ont utilisés des numéros de carte bancaire volés pour créer, fin décembre dernier, des milliers de serveurs virtuels sur le cloud de Google (« Google Compute Engine »). Cette fois, en revanche, le but n'était pas de faire des attaques DDoS, mais de créer des relais Tor. Ce qui a beaucoup énervé les développeurs de ce service d'anonymisation, car cet ajout massif avait pour effet de le fragiliser. Heureusement, Google a rapidement remarqué le subterfuge.

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

Source : http://www.01net.com/editorial/640591/l-attaque-ddos-sur-psn-et-xbox-live-s-est-appuyee-sur-des-routeurs-domestiques/
Par Gilbert Kallenborn

---

# Les particuliers, pierre angulaire de la lutte contre la cybercriminalité



Les particuliers, pierre angulaire de la lutte contre la cybercriminalité

**En fin de compte, constate Mary Galligan des services de cybersécurité de la société Deloitte, c'est aux particuliers d'assumer leurs responsabilités.**

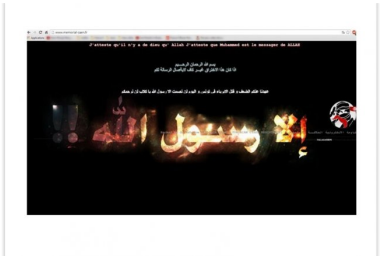
La cybercriminalité est partout, ont constaté les participants. Même le Pentagone en fait les frais puisque lundi, les comptes Twiter et YouTube du Commandement Central (CENTCOM) ont été piratés. Comment mieux se protéger ? Souvent, fait valoir l'expert Austin Berglas, qui travaille pour le FBI, un employé tout à fait innocent prend une décision fatale.
« Peu importe combien d'argent une organisation consacre à la cyber-sécurité ; c'est encore et toujours un employé, ou le dernier utilisateur de l'ordinateur, qui clique sur un lien malveillant » explique Austin Berglas.
Malheureusement, il n'en faut pas beaucoup pour sombrer dans la cybercriminalité : un serveur, qu'on peut louer, un code malicieux, qu'on distribue par e-mail – et voilà, le cybercriminel prend le contrôle de votre ordinateur.
En fin de compte, constate Mary Galligan des services de cybersécurité de Deloitte, c'est aux particuliers d'assumer leurs responsabilités.
« Nous devons commencer à réfléchir à ce que faisons-nous pour protéger nos informations. Nous nous attendons à ce que les milieux d'affaire fassent le nécessaire pour nous, mais nous ne sommes pas disposés à prendre les mesures de sécurité les plus simples », constate Mme Galligan. Pour commencer, il faut que les usagers comprennent que rien n'est secret sur le web, et qu'ils prennent des mesures en conséquence.

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

Source : http://www.lavoixdelamerique.com/content/les-particuliers-pierre-angulaire-de-la-lutte-contre-la-cybercriminalite/2596924.html

---

# Charlie Hebdo : Des cyberpirates musulmans répondent aux Anonymous



## Charlie Hebdo : Des cyberpirates musulmans répondent aux AnonymousInformatique

**Quelques jours après le tragique attentat de Charlie Hebdo et celui qui a frappé la supérette casher de la porte de Vincennes, les Anonymous ont débuté un combat contre les sites d'entreprises et d'organisations en lien avec ces attaques terroristes. Des cyberpirates musulmans, regroupés sous l'étendard de la Middle East Cyber Army, ont quant à eux entrepris des actions pour montrer que l'Islam n'est pas synonyme de terrorisme, tout en envisageant une attaque massive le 15 janvier…**

La France vit en ce moment des heures très sombres mais elle se relève. Après le tragique attentat de mercredi dernier à Charlie Hebdo qui a coûté la vie à 12 personnes, mais également celui qui a frappé une supérette casher porte de Vincennes, les Français ont défilé en masse dimanche pour défendre la liberté avec plus de 3 millions de personnes dans les rues. Depuis mercredi dernier, on a toutefois vu se multiplier des actions de piratage, émanant de groupes islamistes – ou se revendiquant comme tels – mais également des Anonymous et de cyber-hackers musulmans.
Des centaines de sites d'organisations publiques et privées (des sites de l'Université Paris Sud, Memorial de Caen, Palais des papes, plus de 200 médiathèques, la Fondation Jacques Chirac, les communes de Goussainville, Ézanville, Jouy-le-Moutier…) ont par exemple été piratés. Sur le site du Memorial de Caen, la page d'accueil a été altérée par la « Fallaga Team », affichant un message en arabe, traduit par France 3 Basse-Normandie, sur fond noir.
Face à ces opérations, le collectif des Anonymous, regroupé pour l'occasion sous le hashtag #OpCharlieHebdo, s'est élevé et a publié une vidéo en ligne dans laquelle il expose un message très clair : « Le 7 janvier 2015, la liberté d'expression a été meurtrie […] Il est de notre devoir de réagir. Charlie-Hebdo, une figure historique du journalisme satirique a été pris pour cible par des lâches. Anonymous a toujours combattu pour la liberté d'expression et la liberté de la presse. Nous ne renoncerons pas. Attaquer la liberté d'expression, c'est attaquer Anonymous. Nous ne le permettrons pas. Toutes entreprises et organisations en lien avec ces attaques terroristes doivent s'attendre à une réaction massive d'Anonymous. Nous vous traquerons. Nous vous trouverons et nous ne lâcherons rien. »

**Des sites de Carrefour et de BNP Paribas piratés**
Les Anonymous ont ainsi commencé leur riposte samedi 10 janvier avec l'altération de plusieurs sites radicaux dont celui du djihadiste français Ansar-alhaqq.net qui pointe toujours ce lundi après-midi vers le moteur de recherche DuckDuckGo. Mais les Anonymous ne comptent pas en rester là. Au-delà de leurs opérations classiques d'altération de sites ou d'attaques DDoS pour saturer les sites, le collectif prévoit aussi d'en extraire des bases de données d'adresses et de contacts pour les transmettre aux forces de l'ordre.
Depuis hier, on a par ailleurs vu fleurir des attaques de sites revendiquées par différents pirates (AnaCoNdA, kh.mar.404, RebelGhost DX, Scream4.0.4, Silent Killer, Hamooda El Bess…) regroupés derrière le groupe MECA pour Middle East Cyber Army. Objectif, selon son porte-parole interrogé par nos confrères de Zataz, « prouver au monde que l'Islam n'est pas synonyme de terrorisme. Un musulman n'est pas un terroriste. C'est exactement l'inverse de l'Islam. Notre religion est paisible, toute personne qui a lu le Coran comprend cela. » Un postulat qui n'empêche pas cependant ce groupe de mener des actions sur les sites de la filiale géorgienne de Carrefour, de Terraillon, du Centre National de Ressources Biologiques Marines et de plusieurs filiales étrangères de Peugeot mais également de l'espace Cash Management de BNP Paribas, pour lequel ce groupe indique être en possession de « toute la base de données ».
Le 15 janvier, MECA ainsi que plusieurs autres groupes annoncent une attaque massive : « Nous avons déjà piraté des milliers de sites, mais ce qui va venir le 15 janvier sera beaucoup, beaucoup plus important ».

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

Source : http://www.lemondeinformatique.fr/actualites/lire-charlie-hebdo-des-cyberpirates-musulmans-repondent-aux-anonymous-59874.html
Par Dominique Filippone

---

# Les comptes Twitter et Youtube du commandement de l'armée US piratés


# Les comptes Twitter et Youtube du commandement de l'armée US piratés

**Le groupe de pirates informatiques Cyber Caliphate, qui se réclame de l'Etat islamique, s'est emparé, hier soir, des comptes Twitter et Youtube du commandement central de l'armée américaine (Centcom).**

**Un acte symbolique plus qu'une réelle cyberattaque**

Dans un billet publié sur Pastebin, les pirates revendiquent le hack du réseau du Pentagone.

Rien de moins. Et de révéler ce qui est présenté comme des données confidentielles avant de menacer : *« Soldats américains, nous arrivons, surveillez vos arrières ! Nous sommes dans vos PC, dans vos bases militaires. »*

Un acte qui pourrait s'apparenter au début d'une cyberguerre, mais qui est plutôt considéré par le commandement de l'armée américaine comme du cybervandalisme.


**Pourquoi minimiser ainsi les faits ?**

Parce qu'à y regarder de plus près, les informations dévoilées sont au pire, non sensibles, ou mieux, carrément publiques. Seul un dossier contenant les données personnelles de plusieurs généraux (en activité ou à la retraite) pose problème, bien que ces informations ne soient pas classées.

Le commandement de l'armée a donc réagi avec mesure : « Nous pouvons confirmer que nos comptes Twitter et Youtube ont été compromis. Nous prenons les mesures appropriées pour adresser ce problème. » Et ont ajouté « Nous voyons cela comme un acte de cybervandalisme. Aucune information classée n'a été postée et aucune des données dévoilées ne proviennent des serveurs du Centcom. »

Le message posté par le groupe Cyber Caliphate semble indiquer que les pirates ont d'autres informations à partager. Nous verrons si elles se révèlent plus stratégiques que celles fournies jusque là. À moins qu'ils n'aient pas le temps d'agir : les Anonymous ont le groupe de hackers en ligne de mire.

Après cette lecture, quel est votre avis ?

Cliquez et laissez-nous un commentaire…

Source :
http://www.clubic.com/antivirus-securite-informatique/virus-hacker-piratage/piratage-informatique/actualite-749439-piratage-cyber-caliphate.html?estat_svc=s%3D223023201608%26crmID%3D639453874_822822691

---

# Comme les États-Unis en 2001, ira-t-on vers un « Patriot Act » ?

# Comme les États-Unis en 2001, ira-t-on vers un « Patriot Act » ?

**Les communications téléphoniques et sur Internet sont des vecteurs parfois utilisés par les terroristes. Après l'attentat de la semaine dernière, la France pose la question du renforcement de la surveillance.**

Sous l'émotion des attentats du 11 septembre 2001 aux États-Unis, l'administration Bush avait adopté, sept semaines plus tard, une loi d'exception. Elle renforçait les pouvoirs du FBI, de la CIA et de la fameuse NSA, afin de lutter plus efficacement contre le terrorisme. Prévue, initialement, pour une durée de quatre ans, elle fut reconduite plusieurs fois. En 2015, le « Patriot Act » existe encore, et pourrait faire un émule en France.
Après l'attentat du 7 janvier contre Charlie Hebdo et les assassinats qui ont suivi, la classe politique française commence à formuler des propositions en ce sens. L'une des personnalités les plus unanimes sur le sujet est sans doute Valérie Pécresse, ministre UMP de l'Enseignement supérieur de 2007 à 2011. Sur Twitter, elle écrit ce lundi : « Il faudra bien entendu un Patriot Act à la française. Il faut une réponse ferme et globale ».

**« Des mesures à prendre sur le Net »**
En matière de renseignement, la surveillance des communications joue un rôle central. Alors que le suivi des frères Kouachi, suspectés d'avoir perpétré la tuerie à Charlie Hebdo, aurait connu un arrêt durant l'année 2014, le Premier ministre, Manuel Valls, considère qu'il y a une « faille » et appelle à « travailler à de nouveaux dispositifs pour être encore plus efficace ». Il suppose que des mesures seront prises pour combattre la diffusion de messages de « haine » sur Internet. « Il y a des mesures à prendre en plus sur le Net, car cela a un effet de contamination, de mimétisme », ajoute le ministre des Affaires étrangères, Laurent Fabius.

**Des prises de position rejointes par l'opposition**
L'ancien chef de l'Etat, Nicolas Sarkozy, s'exprimant au sujet d'Internet, a demandé à « surveiller ce qu'il s'y passe ». « Ce n'est pas parce que c'est virtuel que l'on peut s'exonérer des règles que l'on a mis plusieurs siècles à établir », a-t-il poursuivi. Si les débats ont commencé cette semaine au niveau politique, ces pistes sécuritaires ont suscité des réactions sur les réseaux sociaux.

**Un Patriot Act « serait un comble »**
« Après 4 millions de Français dans la rue aux cris de « liberté ! », on parle de PATRIOT Act à la française », dénonce par exemple « Maitre Eolas » sur Twitter. « Se réjouir de l'émergence d'un « Patriot Act à la française », c'est avaliser une altération programmée de la démocratie », estime pour sa part l'entrepreneur Gilles Babinet. Le blogueur Olivier Laurelli de rappeler que le Patriot Act tel que conçu aux Etats-Unis ne se limite pas à la surveillance des communications et qu'« on va pouvoir avoir un Guantanamo à la française ».
Interrogé par Petit Web, Benoit Thieulin, le président du Conseil national du numérique, estime que « ce serait un comble, après s'être opposé à la guerre en Irak et les révélations d'Edward Snowden » et souligne qu'Amedy Coulibaly, un des tueurs présumés, « ne disposait plus de smartphone depuis quelques temps déjà, afin d'éviter d'être tracé ». Mais au-delà de l'écoute des télécommunications, se pose enfin la question des prises de parole publiques sur les réseaux sociaux, telles que celle du polémiste Dieudonné ce lundi.
Sur sa page Facebook, il a affirmé se sentir « Charlie Coulibaly », détournant le slogan « Je suis Charlie » et l'associant au nom du tueur présumé. « Il ne faut pas confondre la liberté d'opinion avec l'antisémitisme, le racisme, le négationnisme », a aussitôt répliqué Manuel Valls à Dieudonné, au sujet duquel une enquête a été ouverte pour apologie d'actes de terrorisme. Bref, le débat sur le rôle d'Internet est loin d'être terminé.

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

Source : http://pro.clubic.com/legislation-loi-internet/actualite-749325-patriot-act-france.html
Par Thomas Pontiroli

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

| | |
|---|---|
|  | Antiterrorisme : les Fournisseurs d’Accès à Internet devraient travailler plus étroitement avec le gouvernement |

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

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

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

---

# L'après Charlie Hebdo, le chiffrement déjà un problème ?

L'après Charlie Hebdo, le chiffrement déjà un problème ?

**C'était prévisible. Et le fait que le premier ministre David Cameron soit actuellement en campagne pour les législatives au Royaume-Uni n'y est sans doute pas étranger. De retour de la marche organisée en France en hommage aux victimes des attentats, ce dernier a proposé de faire évoluer les lois sécuritaires au nom de la lutte contre le terrorisme.**

Et l'occasion fait le larron. Le premier ministre en profite en effet pour s'attaquer au chiffrement des communications. Ce n'est pas nouveau puisque les autorités du pays, notamment les agences de renseignement, se montraient particulièrement virulentes à l'égard des entreprises du Web très actives sur le chiffrement suite aux révélations de Snowden sur les pratiques d'espionnage des Etats.

**Pas de communications inviolables**

Ce n'est plus la coopération volontaire de ces acteurs de l'Internet qui semble désormais préoccuper David Cameron qui appelle à renforcer les lois autour du chiffrement afin de pouvoir ainsi accéder aux communications chiffrées.

« La question reste posée : allons-nous autoriser des moyens de communication pour lesquels des interceptions sont impossibles ? Et ma réponse à cela, c'est : non, nous ne devons pas. Le premier devoir de tout gouvernement est de protéger notre pays et nos concitoyens » a déclaré le premier ministre.

Le chef du gouvernement britannique ne précise toutefois pas comment il prévoit de rendre les communications chiffrées accessibles. Aux Etats-Unis, le FBI avait encouragé les éditeurs à inclure des portes dérobées dans les téléphones afin de permettre les interceptions par les autorités.

Assurément, ces attentats seront l'occasion pour le directeur du GCHQ, Robert Hannigan, d'encourager de nouveau les acteurs du web à la mise en place d'un « new deal » avec les gouvernements, ou coopération plus étroite avec le renseignement, afin de protéger les citoyens. Car après tout, déclarait-il quelques mois plus tôt, « la vie privée n'a jamais été un droit absolu ».

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

Source : http://www.zdnet.fr/actualites/l-apres-charlie-hebdo-le-chiffrement-deja-un-probleme-39812783.htm

---

# Les entreprises françaises sont de plus en plus victimes de hackers et d'espions

# industriels

| | |
|---|---|
|  | Les entreprises françaises sont de plus en plus victimes de hackers et d'espions industriels |

**Devant un environnement économique de plus en plus concurrentiel et incertain, les formations spécialisées en sécurité des entreprises tardent à se développer en France.**

Les entreprises françaises sont de plus en plus victimes de hackers et d'espions industriels. Le nombre d'entreprises concerné par ces piratages s'élève à 360. 300 millions d'euros c'est ce qu'ont coûté ces attaques par les gangs internationaux sur les trois dernières années. Face à ces menaces, la Direction Centrale de la Police Judiciaire (DCPJ) et le Medef vont sceller un accord pour résorber le phénomène, mercredi 14 janvier 2015. L'Office central pour la répression de la grande délinquance financière (OCRGDF) a quant à lui officialisé un accord signé avec l'Ecole des ingénieurs de numérique pour lutter contre « le fléau des escroqueries aux faux virements ».
L'Epita (l'école des ingénieurs du numérique) est aujourd'hui, un des rares établissements français à proposer un enseignement qui se focalise sur la sécurité des entreprises. « Aujourd'hui, il manque une vraie filière qui aille du niveau bac +1 à bac +5 » d'après Olivier Hassid interrogé par Le Figaro, dirigeant du Club des Directeurs de Sécurité et de Sureté des Entreprises (CDSE). D'après ses dires, la pluralité des matières permet de créer une filière avec des acquis enseignés en licence. La France montre un réel retard concernant les formations sur la sécurité des entreprises.

**Les grandes écoles intéressées par ce domaine de sécurité**
Deux raisons à ce retard, d'une part le manque de prise en compte des enjeux qui est dû à l'insuffisance de la recherche, et d'autre part le manque de besoin exprimé par les entreprises. « Les problématiques de sécurité ont réellement vu le jour dans années 2006/2007. C'est à ce moment là qu'un certain nombre de grands groupe ont créé des directions en sûreté et sécurité », explique Olivier Hassid.
« Les balbutiements de la formation en sécurité datent des années 90 avec la création de l'IHESI, aujourd'hui devenu l'Institut national des hautes études de la sécurité et de la justice (INHESJ) » raconte le dirigeant du Club. L'INHESJ est la véritable première formation française en matière de sécurité. En plus des formations de l'INHESJ, on retrouve aujourd'hui en France un Master en Gestion globale des risques et des crises à l'université Paris 1, une licence en sécurité à l'université Paris Descartes et, depuis quelques temps, un certificat du management de la sécurité et de la sûreté informatique, avec l'école Epita qui valide la qualité de la formation.
Mais selon Oliver Hassid, le développement des formations spécialisées en sécurité des entreprises doit être impératif pour peut-être un jour arriver à un cursus complet. Il indique que « Les instituts d'études politiques s'intéressent à ces problématiques, tout comme les écoles de commerces. Il y a une vraie tendance avec l'effet Snowden et les inquiétudes concernant le cyberespace. »

**Vers un rapprochement de la sécurité et l'intelligence économique**
Au vu du développement de l'enjeu sécuritaire, la notion d'intelligence économique s'est développée en France. Le concept a émergé dans la seconde partie des années 90, immédiatement, contrairement à la sécurité des entreprises, des formations ont été créées. Christian Harbulot crée en 1997 l'école de guerre économique (EGE), et d'autres également à cette période comme l'Ecole Européenne d'Intelligence Economique (EEIE). Aujourd'hui ce genre de formations est aussi retrouvé dans les grandes écoles de commerce et d'ingénieurs mais aussi à l'université.
Selon Christian Harbulot, le directeur de l'EGE, et Olivier Hassid, on se dirige vers le rapprochement de ces deux pôles stratégiques des entreprises car leur rapport à l'information est similaire. Ainsi, les futures formations devraient joindre les deux domaines à l'avenir.
Il y a bon nombre d'enjeux et les fraudes sont de plus en plus sophistiquées. La criminalité via les réseaux est en expansion, les risques géopolitiques et la sécurité des entreprises à l'international peuvent augmenter dans un contexte encore plus instable.

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

Source : http://www.digischool.fr/enseignement/securite-entreprise-vraie-filiere-peine-mettre-place-france-25849.php
Par Manare BARCHI