La France, terrain de jeu privilégié des espions chinois

La France, terrain de jeu privilégié des espions chinois

Au début du mois, « l'Obs » dévoilait l'existence d'un centre d'écoutes des services de renseignement chinois en banlieue parisienne. Si la Chine a démenti les affirmations de l'hebdomadaire, l'exécutif français n'a absolument pas réagi. Une passivité qui dit bien la liberté d'action dont bénéficient en France les espions chinois. Impossible de prendre le risque d'une brouille diplomatique avec Pékin pour une vague affaire d'espionnage compte tenu des enjeux commerciaux.

Lors de la visite du président chinois, Xi Jinping, à Paris en mars 2014 – Orban Thierry-POOL/SIPA

Une annexe de la « NSA chinoise » en banlieue parisienne ! Au début du mois de décembre, l'Obs dévoilait l'existence de ce que l'hebdomadaire croyait être un centre d'écoutes des services de renseignements chinois.

« C'est une totale invention !, tonne Monsieur Wu, chargé de communication de l'ambassade de Chine en France, Ces installations ne font qu'assurer le système de communication de l'ambassade. Cela permet des connexions sécurisées. Cela a été fait en totale conformité avec la législation française. Nous respectons les lois françaises. J'ai sous les yeux les papiers datés du 11 octobre 2002 qui attestent de l'autorisation donnée par l'Autorité de régulation des télécoms qui est parfaitement au courant de ces installations. Il n'y a là bas que des diplomates, aucun militaire. Tout est transparent ». Quand nous lui demandons, si la totale transparence et la bonne volonté chinoise pourraient aller jusqu'à nous laisser visiter ces installations, Monsieur Wu hésite tout de même… avant de répondre par la négative ! La transparence a des limites…

Paradoxalement, du côté français, on est encore moins prolixe. Interrogé sur l'existence supposée d'un bâtiment des renseignements chinois sur le territoire français, le quai d'Orsay répond « pas de commentaires ». En théorie, le ministère de l'Intérieur, les Affaires étrangères et les services de renseignement français sont parfaitement au courant de l'existence de cette annexe de l'ambassade de Chine et les autorités françaises auraient même validé l'installation de ces antennes.

Les « grandes oreilles » de Pékin en France… *par LeNouvelObservateur*

Si l'Obs surévalue sans doute en partie la menace représentée par les trois paraboles perchées sur ce bâtiment de Chevilly-la-Rue au point d'en faire une annexe de la « NSA chinoise » – on « souhaite » à Pékin de disposer d'autres moyens pour espionner Paris –, l'article de l'hebdomadaire, que l'on sent largement alimenté par la DGSI, dit bien toute la frustration et l'impuissance du contre-espionnage français face au pillage d'informations exercées par l'Empire du Milieu en France. Compte tenu du poids économique que représente la Chine pour la France, les espions chinois opèrent en effet relativement tranquillement sur le territoire français au grand dam du contre-espionnage français.

La France n'a tout simplement pas les moyens de se payer une brouille diplomatique avec Pékin au prétexte de trois paraboles installées en banlieue parisienne. Les milliards de contrats commerciaux signés avec les Chinois valent bien quelques sacrifices… Ce laisser-faire relève néanmoins de l'humiliation permanente pour les services français, contraints d'avaler toutes les couleuvres chinoises.

Non que Pékin ne possède pas, comme les Américains, mais aussi comme la France, de « grandes oreilles » un peu partout dans le monde, et prioritairement dans les pays et les dictatures amies du régime. En 2008, dans son ouvrage Les services secrets chinois, Roger Faligot estimait déjà que la Chine jouait dans la cour des grands avec les Etats-Unis et la Russie en matière de renseignement électro-magnétique. Six ans plus tard, les budgets du renseignement chinois ont explosé et les techniciens ont progressé, formés depuis les années 80 par le BND allemand et même jusque dans les années 90 par… la NSA américaine.

Selon Roger Faligot, la Chine a mis en place au fil des ans une « armée populaire des cyberguerriers » : « Ce service dépend de l'armée populaire de libération. Il est organisé en deux départements qui travaillent sur le renseignement de guerre et l'interception des communications. Ils procèdent en envoyant des virus qui permettent de pirater des informations ou de bloquer des sites gênants. Ils opèrent également en mode "testing" en piratant des systèmes pour étudier la capacité de réaction de l'ennemi. Nous sommes ici en plein volet de guerre psychologique et idéologique ».

Une guerre surtout économique désormais, comme l'avait illustré en septembre dernier une enquête de Franck Renaud et Hervé Gattegno parue dans Vanity Fair. Les journalistes avaient mis la main sur un rapport de la délégation interministérielle à l'intelligence économique (D2IE) sur les objectifs et méthodes chinoises pour piller les innovations technologiques françaises. Un espionnage d'une toute autre ampleur que le renseignement d'origine électro-magnétique. Cette instance signale chaque année plusieurs dizaines de vols ou tentatives de vols de données par captation ou indiscrétion. Toutes les techniques d'espionnage seraient utilisées. De la simple « oreille baladeuse » chinoise dans les trains Thalys ou Eurostar largement fréquentés par les industriels, aux « agents de charme » chargés de séduire les élites industrielles, à l'organisation de voyage de tourisme industriel, l'infiltration d'étudiants chinois dans les universités françaises, le vol de matériels informatiques ou bien encore des méthodes de « phishing » très sophistiquées. Il faut aussi ajouter l'incroyable « pouvoir de persuasion » des Chinois pour imposer à leurs partenaires des transferts de technologies lors de la signature de contrats commerciaux ou la création de joint-ventures, de filiales communes.

« La Chine est déterminée à devenir indépendante de l'Occident en matière d'innovation technologique. Elle est donc avide de connaissances, de savoir-faire et de procédés à faire venir en Chine ou à absorber à l'étranger » précisait le rapport de la D2IE. De leur côté, « les entreprises françaises, attirées par ce marché qu'elles envisagent immense (…) et par les coûts de main-d'œuvre locaux inférieurs aux coûts européens, sont souvent prêts à transférer leur technologie et leur savoir-faire, fournissant ainsi un avantage à leurs concurrents chinois ».
Paris se rassure en estimant que Pékin n'a pas encore les capacités d'exploiter à plein les renseignements politiques, économiques ou industriels qu'ils obtiennent, la Chine se limitant pour l'instant à du rattrapage technologique et à des copies de mauvaise qualité. Mais les énormes moyens affectés à la cyberguerre servent aussi le renseignement économique notamment par le biais de piratages informatiques massifs ainsi que le vol de propriété intellectuelle.

Derrière chaque touriste chinois, un espion potentiel ?
En 2013, la société de sécurité américaine Mandiant publiait un rapport documenté (accessible librement http://intelreport.mandiant.com/Mandiant_APT1_Report.pdf) sur l'unité 61398 du renseignement chinois. Chargée du « suivi » des pays de langue anglaise, l'unité aurait compromis jusqu'à 141 entreprises dans vingt grands secteurs industriels, en dérobant un volume considérable d'informations relevant de la propriété intellectuelle. L'infrastructure de commandement et de contrôle de cette unité compterait de 850 à 1 000 machines situées dans 13 pays. Le coût de ce pillage informatique des entreprises américaines était estimé à au moins 24 milliards de dollars en 2012. L'unité 61046, chargée notamment du suivi de l'Europe, fonctionne sans doute sur le même principe avec la même efficacité, mais est moins connue.
Elle a néanmoins permis aux espions chinois d'accéder aux ordinateurs du président de la Commission européenne, du ministère français des Finances en mars 2011et même de l'Elysée en juillet 2012, causant à l'époque une panique certaine dans les couloirs de la présidence. Chaque attaque est l'occasion pour les services occidentaux d'identifier les priorités des services chinois ainsi que les commanditaires pour mieux connaître leur organisation encore très nébuleuse.
Un an plus tard, dans une mise à jour de son rapport, la société Mandiant disait avoir constaté une « mise en sommeil » pendant quelques mois des activités de l'Unité 61398 suite à la publication de son rapport et aux protestations américaines. De même, toutes les adresses IP des cyberattaques chinoises qui ont frappé les Etats-Unis depuis ont été modifiées, suggérant un changement de stratégie des renseignements chinois.
Mais l'espionnage informatique continue. En octobre dernier, une société américaine de cybersécurité privée identifiera une nouvelle unité de espions informatiques chinois baptisée « groupe Axiome » : « Axiome est chargé de diriger les opérations de cyberespionnage très sophistiquées contre de nombreuses grandes entreprises, des journalistes, des groupes écologistes ou pro-démocratie, des sociétés de logiciels, des établissements universitaires et des organismes gouvernementaux dans le monde entier ». Cibles prioritaires : les Etats-Unis, l'Europe et les voisins asiatiques.
Le Washington Post dévoilera quelques jours plus tard une note du FBI destinée aux industriels américains les alertant sur cette unité de cyberpirates que le FBI considérait comme directement liée aux services de renseignements chinois et jugeait plus performante que l'unité 61398.

Une forme d'espionnite aigüe qui oblige les services français à une attention de tous les instants. Très récemment la lettre spécialisée Intelligence online rapportait l'escapade à Saint-Nazaire d'une équipe du service culturel de l'ambassade de Chine, venue célébrer l'anniversaire de la construction d'un bateau de croisière chinois. La délégation se serait tellement attardée à « mitrailler » le porte-hélicoptères Mistral destiné à la Russie que cela aurait fini par éveiller les soupçons de la DGSI. De la surveillance à la paranoïa, il n'y a parfois pas loin…

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

Source : http://www.marianne.net/La-France-terrain-de-jeu-privilegie-des-espions-chinois_a243309.html
par Régis SOUBROUILLARD – Marianne

Cyberviolence : les parents ne sont pas désarmés

Cyberviolence : les parents ne sont pas désarmés

Un collégien sur cinq déclare avoir été insulté ou humilié sur internet ou par des SMS. Pour répondre à ce phénomène en augmentation, les parents d'élèves ont à leur disposition des outils pour prévenir et agir avant un drame.

«Demain, à l'arrêt de bus, t'es morte ». La violence des mots est inouïe. Ils ont été envoyés par SMS à une collégienne de cinquième vivant en région parisienne. Insultée également sur Facebook, la jeune fille s'est suicidée après deux années d'enfer où les insultes sur internet se sont ajoutées à un harcèlement « classique » au collège. Car la cyberviolence peut pousser un jeune à commettre l'irréparable. « Les suicides sont rares, fort heureusement, tempère Catherine Blaya, présidente de l'Observatoire international de la violence à l'école, mais mettez-vous à la place d'une jeune fille de 14 ans qui voit sur un réseau social une photo d'elle trafiquée à moitié nue avec un message qui la traite de ''chaudasse''. Quand elle retournera au collège, toutes les personnes qu'elle croisera seront susceptibles d'être au courant ».

Un collégien sur trois ne dit rien

Si, selon une enquête du ministère de l'Éducation nationale publiée le 27 novembre 2014, la cyberviolence est en progression et a touché en 2013 un collégien sur cinq en France, les parents se sentent souvent désarmés pour répondre aux souffrances de leurs enfants et réagir.
Encore faut-il que les parents soient au courant. Un collégien sur trois ne dit rien à personne sur sa situation, selon l'enquête du ministère. « Tous les parents n'ont pas accès au profil Facebook de leur enfant. Certains ne savent même pas qu'ils en possèdent un », souligne Christine Sené, la présidente de l'association Noélanie qui combat toutes les violences à l'école.
En prévention, pour en parler avec ses enfants, il existe plusieurs outils, comme le site internet créé par Facebook « takethislollilop.com ». « On y visionne un clip très dissuasif qui montre une sorte de psychopathe qui cherche et vole des informations sur le compte Facebook de sa victime. C'est un clip interactif. Pour les enfants, les adolescents, cela a beaucoup d'impact », insiste Catherine Blaya.

« Il existe aussi des outils pédagogiques très intéressants sur le site ''agircontreleharcelementalecole.gouv.fr''. Les parents peuvent s'en servir pour entamer un dialogue », souligne Eric Debarbieux, le délégué ministériel chargé de la prévention et de la lutte contre les violences en milieu scolaire.

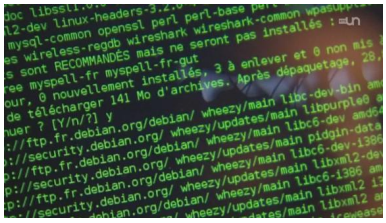
Il est également possible de faire stopper rapidement certains actes de cyberviolence. « Le plus efficace pour supprimer une vidéo dégradante est le site internet-signalement.gouv.fr », conseille Christine Sené dont l'association a un forum rassemblant près de 3500 familles. Alertée, l'association « e-enfance » peut aussi réagir rapidement pour faire suspendre une page Facebook dans les 24 heures.

« Reste que seuls les parents peuvent porter plainte », rappelle Eric Debarbieux. « Pour les aider dans leurs démarches juridiques, par expérience, les gendarmes de la Brigade de prévention de la délinquance juvénile sont très précieux et efficaces », conseille Christine Sené.

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

Source : http://www.ledauphine.com/faits-divers/2014/12/14/cyberviolence-les-parents-ne-sont-pas-desarmes
Par Patrice BARRÈRE

Réseaux Wifi: gare aux pirates!

	**Réseaux Wifi: gare aux pirates!**

Aujourd'hui, on se déplace avec son Smartphone dans la poche, et de plus en plus souvent avec son ordinateur portable sous le bras. On veut pouvoir surfer sur le Net dans les gares, les aéroports, les cafés ou les chambres d'hôtel. Plusieurs grandes villes offrent même un accès wifi public et gratuit. Nos cartes bancaires sont aussi équipées de puces permettant le paiement sans contact. Mais attention, ce sont autant de nouvelles possibilités offertes aux pirates informatiques !

Le piratage informatique augmente
De l'aveu des experts, les antivirus ne savent pas s'adapter à toutes les nouvelles menaces. Il faut d'abord subir une attaque et ses conséquences avant de trouver la parade. Les criminels ont donc pratiquement toujours un temps d'avance. Et les portes d'entrée vers vos données confidentielles se multiplient. Les accès wifi « malicieux », ou encore les virus et autres applications permettant de récupérer vos données de carte de paiement sans contact (NFC)sont des méthodes récentes de piratage qui viennent s'ajouter à une liste déjà longue. Démonstrations.

Votre wifi peut vous rendre suspect
Un soir, madame T. a la mauvaise surprise d'être accueillie par des inspecteurs de la police judiciaire lors de son retour à son domicile. Des images pédopornographiques ont transité par son accès wifi! Bien que protégé, l'accès wifi a été piraté puis utilisé par un cybercriminel. Madame T a rapidement été mise hors de causes, mais reste choquée par cette aventure. Témoignage.

Wifi gratuits: Attention! Le point avec Luc Mariot, journaliste et producteur d'ABE

Les wifi gratuits contrôlés: CFF (en gare de Genève), Aéroport (GVA), Ville de Genève, Ville de Lausanne, Ville de Vevey, Starbucks, Mc Donald, Manor, Centre La Praille.

Vos données intéressent les cybercriminels
Les cybercriminels peuvent utiliser vos données de plusieurs manières. Certains rendent vos documents illisibles puis vous rançonnent en vous vendant la clé de décryptage. D'autres s'emparent tout simplement de vos coordonnées bancaires, pour ensuite les revendre ou consommer à vos frais sur la Toile. Enfin, certains s'invitent carrément chez vous ou à votre bureau, en suivant vos faits et gestes à travers votre micro et votre webcam intégrés. Comment se protéger?
Le Département du Trésor américain et l'Union Européenne annonçaient il y a 5 ans déjà que les profits générés par la cybercriminalité dépassent désormais ceux de la vente de drogue dans le monde ! Un phénomène qui ne va faire que s'amplifier dans les décennies à venir.

LE reportage qui vous dit tout

La principale faille dans les entreprises est le manque de connaissance de ces risques.
Au travers de conférences ou de formations, Denis JACOPINI vous propose de vous sensibiliser, responsable de la stratégie de l'entreprise qui DOIT désormais intégrer le risque informatique comme un fléau à combattre et à enrayer plutôt qu'une fatalité.
Contactez-nous

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

Source : http://www.rts.ch/emissions/abe/6205697-reseaux-wifi-gare-aux-pirates.html

Infographie du vol de données en 2014

Infographie du vol de données en 2014

2014: une année record !
Cette année 2014 restera dans les mémoires en ce qui concerne le vol de données informatiques. En effet, l'entêtement des cybercriminels n'a fait qu'augmenter au cours de ces douze derniers mois et 2014 restera comme l'année record en terme de quantité d'informations piratées. A Bon Escient vous partage ce soir une infographie provenant de Silicon sur le vol de données personnelles. Les temps changent, le sabotage n'est plus le but ultime d'un cyberpirate. En effet, le vol de données est dorénavant la source première de motivation pour ce type d'attaque. A ce petit jeu, le gang Russe Cybervor a frappé fort, ce dernier a revendiqué le vol de plus d'1,2 milliards de noms et mots de passe, auquel il faut ajouter pas moins de 500 millions d'adresses e-mail, tout ce butin ayant été collecté sur pas moins de 420 000 sites. Il ne faut pas non plus oublier les deux autres scandales, subis quant à eux par l'industrie américaine de la grande distribution, à savoir les affaires Target et Home Depot, les pirates ayant profité de plusieurs failles dans les lignes de caisses.

Concernant le paysage digital français, deux attaques ont marqué les esprits et concernent l'opérateur Orange, qui s'est respectivement fait pirater 800 000 et 1,3 millions de comptes. Ces attaques numériques ont un impact négatif sur l'image de l'entreprise et font baisser la réputation ce celle-ci. De plus, elles ont des répercussions économiques avec une perte de confiance de la part des clients.

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

Source : http://www.abonescient.fr/le-fil-infographique/le-vol-de-donnees-infographie/

Fichiers pédopornographiques: un habitant de Peille arrêté

Fichiers pédopornographiques: un habitant de Peille arrêté

Un jeune homme de 21 ans, menuisier, inconnu de la justice, a été interpellé par le groupe « cybercriminalité », de la police judiciaire de Nice. Il est soupçonné d'avoir téléchargé pendant un an des centaines de fichiers (images et vidéos) de viols d'enfants.

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

Source : http://www.monacomatin.mc/nice/fichiers-pedopornographiques-un-habitant-de-peille-arrete.2023663.html

---

Une charte pour protéger les données personnelles

Une charte pour protéger les données personnelles

«l'Assureur qui s'engage à respecter la vie privée lors des traitements des données personnelles», Atlanta a annoncé officiellement le 10 décembre une charte pour la protection des données personnelles.

Atlanta se positionne en protecteur des données personnelles. En effet, à l'occasion de la Journée mondiale des droits de l'Homme, la compagnie d'assurances a publié une charte régissant la protection des données personnelles de ses partenaires et ses clients. Ayant l'ambition d'être reconnu par ses clients, ses collaborateurs et ses partenaires comme «l'Assureur qui s'engage à respecter la vie privée lors des traitements des données personnelles», Atlanta a annoncé officiellement le 10 décembre une charte pour la protection des données personnelles.

Un document qui matérialise les engagements de la compagnie envers ses clients et décrit les modalités suivant lesquelles la compagnie collecte et utilise les données personnelles de ses clients.
Affichée en interne, chez tous les agents et dans son site web, cette charte est en parfaite conformité avec la loi n°09-08 relative à la protection des personnes physiques à l'égard du traitement des données à caractère personnel.

La publication de cette charte intervient suite à une large mise à niveau de l'ensemble des standards et procédures de la compagnie qui, par ailleurs, a reçu de la part de la Commission nationale de contrôle de protection des données à caractère personnel (CNDP) l'autorisation de traitement des données concernant les process opérationnels.

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

Source : http://www.aujourdhui.ma/une/actualite/atlanta-une-charte-pour-proteger-les-donnees-personnelles-115014#.VIyAT9KG92o
Par ALM

Ce que révèlent les milliers de documents confidentiels volés à Sony Pictures

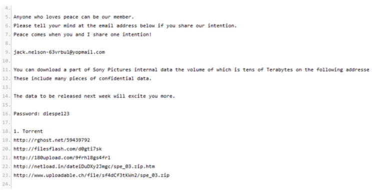
Ce que révèlent les milliers de documents confidentiels volés à Sony Pictures

Des centaines de gigaoctets de fichiers ont déjà été diffusés par des pirates. Une situation catastrophique pour le géant du divertissement hollywoodien.

Imaginez que toutes les données – ou presque – qui transitent sur votre ordinateur de travail, stockées sur les disques durs et serveurs de votre entreprise, soient compilées et rendues accessibles à tous. Voilà la situation devant laquelle se retrouvent actuellement les employés et la direction de Sony Pictures Entertainment, après l'attaque informatique de grande ampleur subie le 24 novembre. Depuis, des milliers de gigaoctets de fichiers confidentiels du géant du divertissement hollywoodien, producteur et diffuseur de nombreux films, sont dispersés sur le Web.

Un mécanisme bien rodé

Les pirates, réfugiés derrière l'acronyme #GOP (pour Guardian of Peace), avaient au départ évoqué onze terabytes de documents (11 000 gigaoctets) subtilisés lors de leur attaque. Ils parlent maintenant de « dizaines de térabytes » de données – une centaine, disent les médias américains. Qu'un tel volume de données ait effectivement été volé semble de plus en plus probable.
Les documents internes de Sony Pictures publiés (fichiers Excel, Word, Powerpoint, PDF, etc.) se comptent déjà par centaines de milliers et en dizaine de gigaoctets, selon un décompte fiable établi par l'entreprise spécialisée en sécurité informatique Risk Based Security.
Le processus de diffusion est toujours le même. Des liens permettant de télécharger des fichiers RAR ou ZIP volumineux, par des sites de téléchargement direct ou grâce à des fichiers torrent, apparaissent sur l'éditeur de texte en ligne Pastebin, qui assure un certain anonymat à leurs auteurs. Les hackers envoient ensuite le lien du document Pastebin par e-mails à leurs contacts, soit n'importe qui ayant signifié son intérêt pour les documents Sony Pictures en écrivant aux adresses anonymes et temporaires que les membre de GOP diffusent régulièrement (journalistes, sympathisants des hackers, entreprises de sécurité informatique, enquêteurs, concurrents…).



```
4.
5.  Anyone who loves peace can be our member.
6.  Please tell your mind at the email address below if you share our intention.
7.  Peace comes when you and I share one intention!
8.
9.  jack.nelson-63vrbu1@yopmail.com
10.
11. You can download a part of Sony Pictures internal data the volume of which is tens of Terabytes on the following addresse
12. These include many pieces of confidential data.
13.
14. The data to be released next week will excite you more.
15.
16. Password: diespe123
17.
18. 1. Torrent
19. http://rghost.net/59439792
20. http://filesflash.com/d0gti7sk
21. http://180upload.com/9frhl8gs4frl
22. http://netload.in/dateiDuDXy2Jmgc/spe_03.zip.htm
23. http://www.uploadable.ch/file/sf4dCf3tKWn2/spe_03.zip
24.
```

Extrait d'un message donnant accès aux fichiers volés à Sony Pictures Entertainment. | Pastebin

Les données sont ensuite accessibles pendant quelques heures, avant la désactivation des liens de téléchargement par les hébergeurs et la suppression du document Pastebin – vraisemblablement sur requête des autorités ou de représentants légaux de Sony. Entre le 24 novembre et le 10 décembre, six « livraisons » de ce type ont eu lieu. Les pirates, maniant le sens du teasing, en promettent à chaque fois davantage : « les données que nous publierons la semaine prochaine vous exciteront encore plus », annonçait par exemple un document Pastebin publié le 5 décembre.

Un chantage pécuniaire ?

Les textes diffusés par les hackers qui accompagnent la publication de ces fichiers n'en disent en revanche que peu sur les motivations réelles justifiant cette fuite massive et organisée. La piste de la Corée du Nord, qui agirait en représailles au film The Interview parodiant le régime de Kim Jong-un, est accréditée par des similarités constatées entre l'attaque du 24 novembre et celle subie par la Corée du Sud en 2013. Mais l'un des cadres du FBI, officiellement chargé de l'enquête, a confié le 9 décembre qu'il n'était pour l'instant pas possible d'en attribuer la responsabilité à Pyongyang.
Dans un document publié le même jour, les membres proclamés des GOP demandent bien à Sony d'« arrêter immédiatement de diffuser un film sur le terrorisme qui peut mettre fin à la paix régionale et causer une guerre », sans nommer le film en question, et reprenant une rhétorique déjà servie auparavant à The Verge. Mais ils signalent également avoir « formulé une demande claire à l'équipe dirigeante de Sony », encore une fois sans préciser laquelle :

« Ils ont refusé de l'accepter. On dirait que vous pensez que tout se passera bien, si vous trouvez les attaquants et ne réagissez pas à notre demande. Nous vous avertissons à nouveau. Répondez à ce que nous vous demandons si vous voulez nous échapper. »

De quoi donner du crédit à l'hypothèse d'une tentative d'extorsion de fonds de la part des hackers de « Guardian of Peace ». Ce motif a d'ailleurs été clairement exposé dans un e-mail envoyé aux dirigeants de Sony Pictures quelques jours avant l'attaque : « Nous avons de quoi causer beaucoup de tort à Sony Pictures. (…) Nous voulons une compensation monétaire. Payez, ou Sony Pictures sera frappé dans son ensemble. »

La diffusion au compte-gouttes des documents confidentiels constituerait, dans ce contexte, un moyen de pression supplémentaire pour obtenir cette « compensation », de nature à alimenter un feuilleton médiatique dévastateur pour Sony Pictures. Les médias du monde entier ont ainsi repris :

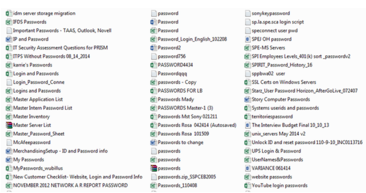
Les données privées de célébrités

Des adresses postales, des numéros de téléphone, des adresses électroniques, ou encore le numéro de sécurité sociale de Sylvester Stallone, contenus dans les documents liés aux films et séries de Sony Pictures ont été rendus publics. Parmi ces informations, on trouve les pseudonymes utilisés par Tom Hanks, Natalie Portman ou encore Ice Cube pour conserver un peu de tranquillité (lors d'une réservation d'hôtel par exemple).
Ont également été publiés une cote de popularité des acteurs pays par pays, ou encore les sommes d'argent perçues par Seth Rogen et James Franco pour le film The Interview. Le premier aurait reçu 8,4 millions de dollars pour avoir coréalisé et interprété l'un des rôles principaux, le second 6,5 millions : des divulgations auxquelles ils ont réagi avec humour.

L'affiche de « The Interview ». | Sony Pictures

Les données privées des salariés et partenaires de Sony Pictures

Numéros de téléphone, CV, photos d'identité, montants de salaires, demandes d'augmentation, e-mails, planning de vacances, factures médicales… Autant d'éléments propres à la vie interne d'une structure qui emploie près de 7 000 personnes aux Etats-Unis, et qui a collaboré avec de très nombreuses personnes ces dernières années – stagiaires, prestataires ou partenaires directs au sein d'entreprises rachetées par Sony, comme Columbia Pictures. Ces détails apparaissent notamment dans un dossier intitulé « Ressources humaines », et se trouvent aussi dans des documents de travail liés aux tournages de films et de séries Sony.
Encore plus grave, de très nombreux mots de passe utilisés par les employés pour se connecter à tous types de services (propres à Sony Pictures, mais aussi ailleurs sur Internet) font partie des publications. Comme le note cruellement Gizmodo, ils étaient stockés sur les disques durs de Sony Pictures dans des fichiers Word et Excel sans protection, et dans un dossier appelé « Mot de passe ».



Les mots de passes de Sony Pictures. | Risk Biaised Security

De quoi pousser d'anciens employés à réfléchir à une plainte collective, arguant du manque flagrant de sécurité du réseau de l'entreprise. « Il y a des raisons de penser qu'il y a eu une grosse négligence de la part de [Sony Pictures]. Nous nous inquiétons tous concernant notre vie privée, et nos familles », a déclaré l'un d'entre eux à Fox News, après avoir vu diffuser son passeport, son visa, son numéro de sécurité sociale et ses contrats passés avec l'entreprise.
Des avocats californiens incitent également les salariés actuels à se lancer dans de telles procédures. Particulièrement exposés, ils se sont vus en plus directement menacés dans un e-mail leur étant adressé. « Tout le monde panique, et personne ne sait quoi faire », a témoigné l'un d'eux sur le site Fusion, décrivant une hostilité grandissante au sein de Sony Pictures à l'encontre du service informatique. Le FBI, chargé de l'enquête, devrait faire le point devant les employés sur le comportement à adopter face à cette situation le 12 décembre.
Les dirigeants de Sony Pictures ne sont pas épargnés. L'un des premiers documents diffusés par le site d'information Fusion dresse le détail des rémunérations des 17 salariés les mieux payés, à commencer par le dirigeant Michael Lynton (3 millions de dollars par an) – une seule femme dans ce palmarès. Parmi les fichiers publiés figurent des sauvegardes de plusieurs mois de conversations par courriels (professionnels et personnels) issues des messageries Outlook de cadres de l'entreprise : Amy Pascal, vice-présidente de Sony Pictures, Steve Mosko, à la tête de Sony Television, ou encore Leah Weill, conseiller juridique en chef.

Des révélations sur les films et les séries Sony

Dans son ensemble, cette masse de données fourmille d'informations sur la manière dont Sony Pictures gère son catalogue, ses productions et ses projets. Finances de l'entreprise, projets marketing, bilans comptables liés aux séries diffusées à la télévision américaine, rétrospectives annuelles, bases de contacts, documents préparatoires pour des négociations… Ces milliers de fichiers bruts s'accompagnent de visées stratégiques, comme en témoignent les points de vue exprimés par des employés (s'énervant par exemple contre l'omniprésence d'Adam Sandler à l'écran).
Dans ces documents se nichent ainsi, fatalement, des informations propres aux films et aux séries télévisées estampillées Sony. On y apprend par exemple comment les dirigeants de Sony Pictures ont fait modifier la fin du film The Interview (attention spoiler !), et négocié avec Marvel, qui souhaitait que Spiderman apparaisse dans le prochain Captain America. Plus problématique, des scripts inédits d'épisodes de séries, et même de films devant sortir en 2015, ont été repérés.
Plusieurs médias, comme le Wall Street Journal, ont également extrait diverses phrases chocs des e-mails échangés ces dernières années par la vice-présidente Amy Pascal avec le tout-Hollywood (réalisateurs, agents, stars, etc.). On y trouve quelques commentaires désobligeants sur des acteurs : Angelina Jolie et son « ego devastateur » en prennent pour leur grade. Ou encore, une chronique détaillée des négociations et conversations, parfois brutes de décoffrage, entourant le biopic sur Steve Jobs sur lequel Sony travaille depuis trois ans (notamment sur les choix de casting du scénariste Aaron Sorkin, qui avait songé à Tom Cruise pour incarner le fondateur d'Apple).

En savoir plus sur http://www.lemonde.fr/pixels/article/2014/12/11/ce-que-revelent-les-milliers-de-documents-confidentiels-voles-a-sony-pictures_4537271_4408996.html#Ox8W3PwS6l8JJu0T.99
Par Michaël Szadkowski journaliste à Pixels

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

Source : http://www.lemonde.fr/pixels/article/2014/12/11/ce-que-revelent-les-milliers-de-documents-confidentiels-voles-a-sony-pictures_4537271_4408996.html
par Par Michaël Szadkowski

Droit à l’oubli pour les entreprises, plus qu’une idée…

	Droit à l’oubli pour les entreprises, plus qu’une idée…

Au nom du principe de la protection de la vie privée, une directive européenne confère aux ressortissants des pays membres des droits face aux responsables des traitements de leurs données personnelles.

Dis-moi comment te référence Google, je te dirai qui tu es… ou pas. Car parfois, la révélation est rude, humiliante, voire dégradante, de celle que l'on voudrait effacer. Mais Internet possède malheureusement une très bonne mémoire, vive et éternelle. Pourtant, le 13 mai 2014, la Cour de justice de l'Union européenne (CJUE) a joué les hypnotiseurs : « Oubliez ! Je le veux », a-t-elle dit en substance aux moteurs de recherche. Une décision historique – ont estimé les commentateurs –, instaurant un « droit à l'oubli ». Mais est-ce vraiment sûr ? A y regarder de près la décision n'a qu'une portée limitée. Entre le moteur de recherche et l'internaute, désormais, c'est un peu « je t'oublie, moi non plus ». Parce que ce « droit à l'oubli » existe depuis… 1995.
C'est au nom du principe de la protection de la vie privée qu'une directive européenne confère aux ressortissants des pays membres des droits face aux responsables des traitements de leurs données personnelles. La Cour de justice a souligné ce point au début de son arrêt, plaçant sa décision sous le signe de la sauvegarde des droits fondamentaux. « La CJUE a décidé que l'exploitant du moteur de recherche est tenu de supprimer, sur demande, les liens vers des pages Web, à condition que la démarche de l'internaute soit justifiée. L'arrêt n'instaure pas cependant un "droit à l'effacement des données", mais un "droit à la désindexation" : les liens perdurent, notamment à partir du site américain Google.com, accessible à un internaute européen », explique Olivier Cousi, avocat et associé du cabinet Gide, expert en droit de la propriété intellectuelle.

Zones grises
En outre, si la protection des données est encore imparfaite pour les particuliers, elle est inexistante pour l'entreprise. En effet, la protection comme l'entend l'arrêt de la CJUE ne concerne que les personnes physiques. Alors comment l'entreprise peut-elle gérer son e-réputation ? Quelle démarche pour contrer l'information fausse ou malveillante la concernant ? Autre sujet : cette absence d'intimité, renforcée en France par l'absence de secret des affaires, donne peu d'armes à l'entreprise pour contrer la diffusion de données confidentielles – procès-verbaux de conseil d'administration, chiffre d'affaires… C'est une des zones grises du droit à l'information qui protège également, c'est le bon côté de la médaille, d'une entreprise qui voudrait réécrire son histoire. Pour le reste, il faudra utiliser le bon vieux droit de la presse (diffamation) ou dénoncer la concurrence déloyale pour essayer de se défendre.
Un espoir quand même, un projet de règlement européen, qui doit être adopté « au plus tard en 2015 » par la France et l'Allemagne devrait venir réformer la directive de 1995. Il recommanderait un réel effacement des données et pourrait étendre la protection des données personnelles à certaines informations concernant les entreprises.

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

Source : http://www.lesechos.fr/enjeux/les-plus-denjeux/idees/0203967538313-pas-encore-de-droit-a-loubli-pour-lentreprise-1074046.php par Valérie de Senneville

---

La WPC participe au débat : le Big Data débouchera-t-il sur un Big Brother ?

La WPC participe au débat : le Big Data débouchera-t-il sur un Big Brother ?

Parallèlement aux grands dossiers à caractère géopolitique, la World Policy Conference, dont les travaux de sa septième édition viennent de s'achever à Séoul, a planché sur un problème lié à un autre genre d'actualité : l'émergence du Big Data et ses conséquences économiques et politiques.

La situation actuelle au Moyen-Orient ainsi que la place grandissante qu'occupe l'Asie dans le nouvel ordre mondial – dossiers liés à l'actualité internationale – ont été au centre de la 7e édition de la World Policy Conference (WPC) qui s'est tenue du 8 au 10 décembre à Séoul (voir L'Orient-Le Jour des 8, 9 et 10 décembre). Mais parallèlement, et dans le but d'élargir le débat et d'étendre les échanges de connaissances à un champ plus large que la sphère purement politique, les congressistes réunis dans la capitale coréenne ont planché dans le même temps sur des thèmes à caractère sociétal en rapport avec le changement climatique, l'énergie, l'environnement, les défis que pose le phénomène de Big Data, sans compter les rapports agroalimentaires entre l'Asie et l'Afrique. Autant de sujets liés aussi à l'actualité, mais une actualité d'un autre genre. Celle qui concerne les populations dans le détail de leur vie quotidienne et qui influe sur leur niveau de vie.

Le développement exponentiel de la révolution numérique est à n'en point douter l'un des principaux domaines qui touche de près le citoyen lambda. À l'ouverture de la session consacrée aux conséquences économiques et politiques du Big Data, le modérateur du débat, Nicolas Barré, directeur adjoint du quotidien Les Échos, indiquait, en guise d'entrée en matière, qu'en l'an 2000, un quart des données dans le monde étaient sous forme numérique. Aujourd'hui, cette proportion est quasiment de 100 pour cent. Et dans ce bouleversement vertigineux, l'Asie joue un rôle central. C'est du moins ce qu'affirme Chang Due Whan, président d'un géant médiatique en Corée du Sud, le Mackyung Media Group, qui possède, notamment, un quotidien, qui tire à un million d'exemplaires, ainsi que quinze de chaînes de télévision.

Évoquant les circonstances de cette révolution du XXIe siècle, Chang Due Whan souligne que la plupart des nouvelles inventions dans le domaine numérique viennent d'Asie. Il en déduit que cette zone sera la force motrice du secteur des appareils numériques, tels que les smartphones ou les phablets (combinaison du téléphone et de la tablette). Le développement dans ce domaine est tellement rapide que nombre d'utilisateurs estiment déjà que le PC est devenu obsolète et qu'il est de plus en plus évincé par la nouvelle génération de téléphones portables. Et dans ce cadre, souligne Chang Due Whan, la nouvelle technologie 5G va accroître considérablement le flux d'informations.

C'est précisément sur ce plan qu'intervient le problème du Big Data, en ce sens qu'il représente la capacité d'avoir accès, d'analyser et d'exploiter la quantité gigantesque de données disponibles, ce qui implique la création et l'utilisation efficace des outils permettant l'exploitation des données versées sur le marché un peu partout dans le monde. « Le Big Data est le nouveau pétrole », affirme à cet égard Chang Due Whan.
Le rythme de l'expansion de ce secteur d'activité a été mis en évidence par Luc-François Salvador, président exécutif pour l'Asie-Pacifique du groupe Capgemini, qui affirme que 90 pour cent des données actuelles ont été créées ces deux dernières années, et ce volume de données disponibles double chaque année. Conséquence prévisible : de nouveaux outils sont créés pour analyser et exploiter ces data. À titre d'exemple, Google a mis en place un système de gestion des maladies de manière à prévoir les dates, ou plus précisément les périodes, auxquelles apparaissent les grippes dans une région déterminée. Autre exemple dans ce domaine : au Japon, des chercheurs planchent sur l'analyse des données que l'on peut tirer de la façon de… s'asseoir ! La manière de s'asseoir devient ainsi une sorte de « signature » propre à la personne considérée.

La protection des données
Cette accumulation des données, notamment personnelles, à un rythme exponentiel, ainsi que la capacité grandissante d'analyser et d'exploiter de telles informations posent, à l'évidence, le problème de la protection des données personnelles et les craintes d'un fâcheux impact qui pourrait se manifester au niveau de la liberté de l'individu. Plusieurs intervenants ont évidemment soulevé ce point précis lors du débat. M. Salavador a ainsi relevé que le Big Data permet d'enregistrer des progrès énormes au niveau du traitement de certaines maladies ou aussi dans les projets d'urbanisme, mais dans le même temps, il pose le problème de la protection des données personnelles, ce qui implique la nécessité de concevoir les moyens dont devrait bénéficier le citoyen pour s'assurer une protection adéquate face au Big Data.

Cette question a été soulevée par un expert et consultant américain, Ben Scott, qui a affirmé qu'il se profile à l'horizon, du fait de ce problème, une perte de confiance de la population dans les gouvernements et les pratiques démocratiques, et, surtout, dans les outils informatiques, ce qui risque de pousser les individus à hésiter de trop s'engager dans l'utilisation des nouveaux outils ou applications numériques.

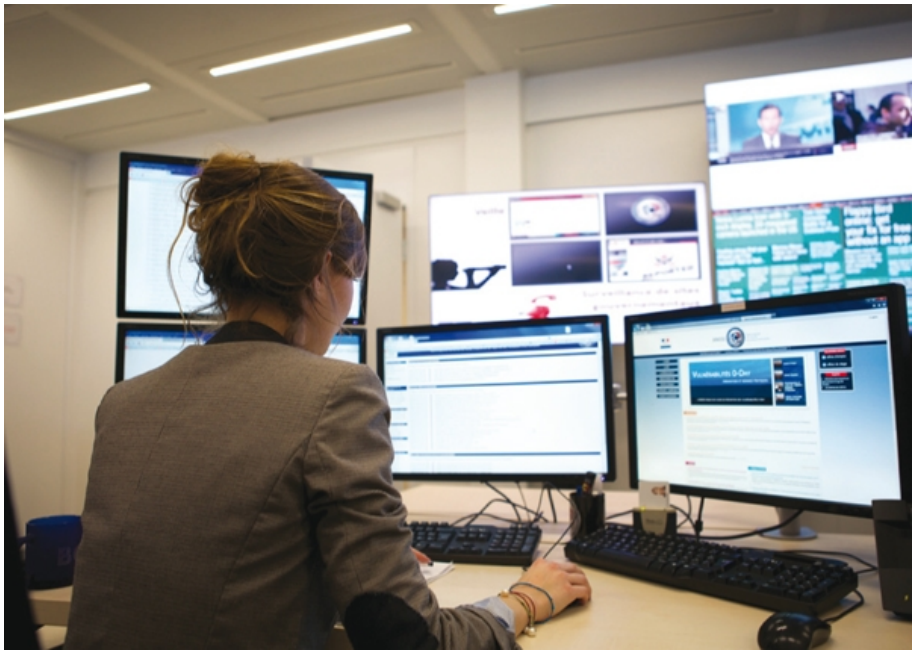
Un professeur universitaire américain, Joseph Nye, a relevé dans ce cadre que la capacité de traitement des données double chaque deux mois, de sorte que les citoyens vivant dans des pays démocratiques finissent par exprimer leurs appréhensions concernant l'exploitation des données personnelles. Certes, certaines personnes soulignent qu'au nom de la sécurité, face aux menaces terroristes, notamment, elles sont disposées à sacrifier de leur liberté ou de leur confidentialité. Cela pose, relève Joseph Nye, le problème de l'absence, au stade actuel, de contre-pouvoirs dans ce domaine.

Le Big Data risque-t-il ainsi de rendre quelque peu réel le danger de l'émergence d'un Big Brother ? Intervenant dans le débat, le député israélien de gauche Meir Sheetrit a apporté une nuance dans la nature du danger qui plane à cet égard, soulignant que le Big Data n'est pas exclusivement contrôlé par les gouvernements, mais il est aussi contrôlé et exploité surtout par les grandes entreprises, d'où la nécessité de protéger également les populations contre certaines grandes entreprises privées. Joseph Nye relèvera à ce propos que c'est dans la mesure où les données sont partagées entre plusieurs entreprises puissantes que le danger se fait plus grand au niveau de la confidentialité et de la liberté de l'individu.
Le débat sur ce plan est donc ouvert à l'échelle planétaire. Les experts et hauts responsables qui planchent sur la question feraient bien de proposer sans trop tarder des mesures concrètes en termes de protection des libertés individuelles avant que la situation dans ce domaine n'échappe à tout contrôle.

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

Source : http://www.lorientlejour.com/article/900564/la-wpc-participe-au-debat-le-big-data-debouchera-t-il-sur-un-big-brother-.html
par Michel TOUMA

Les cyber attaques dans le transport maritime



Les cyber attaques dans le transport maritime

La cyber-défense est classée au rang des priorités par le gouvernement. Un plan d'investissement d'un milliard d'euros sur 5 ans a été dévoilé au début de l'année pour faire face à cette nouvelle menace.

Des cyber-attaques qui inquiètent aussi le monde maritime.
« Le transport et la logistique maritimes sont le prochain terrain de jeux des pirates informatiques » : c'est le BMI, le Bureau Maritime International qui le dit..
L'organisme est spécialisé dans la lutte contre la criminalité envers le commerce maritime, notamment la piraterie et les fraudes commerciales ainsi que dans la protection des équipages. Dans un communiqué publié le 20 août 2014, le BMI a tiré la sonnette d'alarme en appelant l'ensemble de secteur à se protéger contre les cyber-attaques..
Si ces cyber-menaces inquiètent c'est parce qu'aujourd'hui dans un bateau, presque tout est informatisé. Tout est connecté à Internet entre la terre et la mer.
Aujourd'hui il est possible pour un hacker (voire un État) de détourner des informations, de prendre le contrôle d'un navire ou même de son système d'armement..
Au début c'était un jeu, c'est devenu une véritable guerre. Vous avez des menaces de ce type-là qui sont organisées comme des réseaux terroristes.

Trafic de drogue, vol de données, kidnapping
Les spécialistes en cyber-défense ont identifié deux menaces principales, comme l'espionnage et le sabotage.
Un « espion » peut par exemple « voler les données techniques » pour connaître avec précisions le trajet emprunté par un bateau. Cela « permet à un concurrent de voler le marché et de pratiquer des prix plus bas », raconte Dominique Riban, de l'ANSSI (Agence nationale de sécurité des systèmes d'information).
C'est elle qui surveille les sites internet de l'État français. Elle a été créée après la publication du Livre blanc de la Défense en 2008.

Télécharger l'intégralité du Livre blanc de la Défense

« Tout est potentiellement attaquable »
L'angoisse des experts en cyber-défense c'est aussi l'attaque des géants des mers, ces containers géants qui débarquent dans les ports européens.
Le plus gros au monde doit transporter 20 000 containers pour une valeur de deux à quatre milliards de dollars. On y trouve tout un tas de systèmes de cartographie, d'informations. Tous ces systèmes là sont potentiellement attaquables.
Patrick Hebrard est titulaire de la chaire Cyber-défense des systèmes navals à l'Ecole navale. Il s'occupe aussi de cyber-défense chez DCNS. « La passerelle peut ne plus avoir la maitrise de sa propulsion et de sa gouverne », poursuit-il. « Un hacker pourrait complètement bloquer la barre d'un bateau. »
En 2011, l'Agence européenne de cyber-sécurité (ENISA) a publié un premier rapport européen sur la cyber-sécurité maritime. Elle évoquait déjà les menaces qui s'amplifiaient. Elles mettaient en garde sur les conséquences désastreuses de ces cyber-attaques.
La même année, le port d'Anvers (dans lequel des milliers de containers sont débarqués chaque semaine sur les quais) avait été piraté par un cartel de la drogue. Ils avaient réussi à récupérer la marchandise avant que les douanes n'inspectent les containers.

Un yacht (volontairement) piraté et détourné
En 2013, un groupe d'étudiants en école d'ingénieurs a fait une expérience en pleine mer : ils ont piraté un yacht de luxe pour le détourner de son trajet initial, en utilisant le système GPS..
C'était en fait un test organisé avec l'accord des propriétaires du bateau. Naviguant de Monaco à l'île de Rhodes, le yacht a été piraté en pleine mer Ionienne. Grâce à un faux boîtier simulateur GPS, ils ont envoyé des signaux de localisation avec de fausses données, des signaux plus forts que ceux transmis par les satellites. Les « faux signaux » se sont donc substitués aux vrais, en les brouillant. Le yacht a alors viré de bord, en modifiant le pilote automatique.
« Les armateurs prennent de plus en plus en compte ces menaces », explique Eric Banel, secrétaire général d'Armateurs de France. « Les politiques d'entreprises contiennent quasiment toutes un chapitre sur la cyber-criminalité. »
Quand aux constructeurs navals, comme DCNS qui construisent des bateaux pour la Marine nationale notamment, ils développent des moyens pour faire face à cette cyber-criminalité maritime, avec aussi des experts présents à terre pour surveiller les flux qui transitent entre la terre et le bateau.
L'école navale, Telecom Bretagne, DCNS et Thales se sont associés pour créer, avec le soutien de la région Bretagne, une chaire de cyber-défense des systèmes navals. Le but est de mettre en œuvre toutes les techniques pour lutter contre les menaces du cyberespace. Cette chaire universitaire mais aussi industrielle ambitionne de stimuler la cyber-innovation. Des chercheurs qui devront trouver des parades à la vulnérabilité des navires en mer, du porte-container au méthanier en passant par les navires de guerre.

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

Source : http://www.franceinter.fr/emission-le-zoom-de-la-redaction-les-cyber-attaques-dans-le-transport-maritime