Le nomadisme ravive la question de la confidentialité des données

	Le nomadisme ravive la question de la confidentialité des données

Au-delà des abus de la NSA révélés par Edward Snowden, les écoutes sont une réalité dans de multiples lieux publics. Il est urgent de considérer le smartphone comme une extension du système d'information de l'entreprise.

Dans le monde du business, tout le monde est aujourd'hui habitué à respecter des règles de sécurité à l'intérieur des murs de l'entreprise. Quelle entreprise ne songerait pas à sécuriser ses accès avec un vigile, en distribuant des cartes d'accès à ses salariés ? C'est la même chose pour son informatique où un minimum est d'installer des firewalls pour empêcher l'accès aux informations internes de l'entreprise à tous.
Tout le monde l'admet et tout chef d'entreprise, même dans une PME, même un particulier, est conscient du risque d'intrusion à partir du moment où un ordinateur est connecté à Internet. Ce risque, pourtant parfaitement compris dans le monde « sédentaire », est encore totalement ignoré en situation de mobilité. Or aujourd'hui, les managers, les cadres, les commerciaux sont de plus en plus nomades et ce besoin de confidentialité des données doit être étendu d'urgence aux terminaux mobiles.

Au changement des usages doivent répondre de nouvelles règles de confidentialité
C'est une évidence, les salariés passent désormais une énorme part de leur temps non plus assis derrière un bureau, mais à l'extérieur. 70% des cadres français ont adopté un mode de travail décentralisé[1].
Plusieurs raisons expliquent cela, notamment les outils de mobilité qui sont de plus en plus performants. Les capacités des applications mobiles vont désormais bien au-delà de ce que l'on peut réaliser sur un PC. Un autre élément fondamental et auquel personne ne peut rien, c'est le phénomène du BYOD (Bring Your Own Device). Les forteresses sont en train de tomber. Jusqu'à peu, un DSI pouvait encore imposer un modèle de smartphone à l'ensemble du personnel et un autre modèle haut de gamme pour la direction. Aujourd'hui, un tel dirigisme est totalement hors de propos. Tout le monde veut apporter son propre device dans son environnement professionnel. Tout le monde veut pouvoir se connecter au système d'information avec son smartphone, sa phablet ou la tablette de son choix.
La barrière entre outils professionnels et outils personnels a désormais totalement disparue.

Des salariés plus libres, mais mieux armés face aux enjeux de la confidentialité
Face à ce mouvement qui semble inéluctable, certains vont continuer à imposer à leurs employés des mesures drastiques et continuer à leur imposer le téléphone de l'entreprise. D'autres, comme McKinsey récemment, choisissent d'ouvrir une conciergerie mobile et de donner des conseils à leurs salariés pour les aider à connecter leurs propres devices à l'entreprise. L'approche qui semble la plus intelligente reste encore de fixer des règles du jeu simples aux employés puis les aider à les appliquer.

Il faut absolument leur donner les moyens de protéger les données qui doivent rester confidentielles. Or on sait que les soucis liés à la confidentialité des données sont bien réels. On connait aujourd'hui les écoutes mises en place par la NSA. Que les Etats-Unis écoutent mes conversations téléphoniques n'a pas tellement d'importance si cela nous permet de prendre l'avion en toute sécurité. Néanmoins, il y a aujourd'hui de nombreux abus en matière d'écoutes. Quand vous êtes un exportateur, que vous vous déplacez dans le monde entier, on sait très bien que les accès Wifi de certains aéroports sont systématiquement écoutés. C'est vrai en Asie, dans le Maghreb et les révélations d'Edward Snowden ont montré que c'était aussi le cas de l'aéroport international de Toronto[2].
Quand vous vous connectez au Wi-Fi invité chez un client, un fournisseur, vous prenez aussi le risque de voir vos données interceptées. Tout récemment, un malware nommé Darkhotel a été détecté par les experts en sécurité informatique. Celui-ci venait s'installer sur les ordinateurs portables des hommes d'affaires habitués à fréquenter des hôtels de luxe afin de siphonner leurs mots de passe et leurs données confidentielles. Darkhotel a ainsi été signalé au Japon, à Taiwan, en Chine, en Russie et en Corée du sud. La nouvelle édition 2014 de l'étude Trustwave Global Security Report montre que le secteur hôtelier est tout particulièrement visé par les pirates informatiques. Il représente 11 % de l'ensemble des fuites de données recensées dans le monde, un taux en forte progression [3]. C'est bien plus que le monde de la finance par exemple.

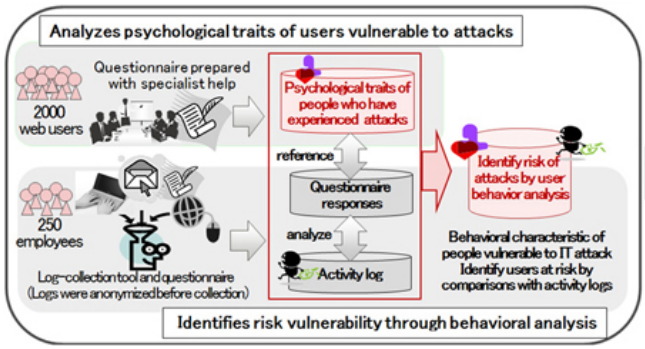
Faire le tri entre ce qui est confidentiel et ce qui ne l'est pas
Lorsqu'on fait du business, que l'on doit échanger des données sensibles avec le siège, c'est un paramètre dont il faut absolument tenir compte. Une grande partie de nos conversations personnelles peuvent être écoutées, mais à certains moments, certaines doivent être absolument confidentielles. Quand vous allez négocier un contrat en Asie, connecter son ordinateur dans sa chambre d'hôtel pour travailler sur sa présentation PowerPoint ou sur le contrat, c'est prendre le risque qu'il soit intercepté et, pourquoi pas, revendu à votre concurrent avant même que vous ayez eu le temps de conclure l'affaire. C'est à ce moment qu'il faut absolument disposer des moyens techniques performants qui vont permettre d'assurer la confidentialité de cet échange. On doit pouvoir transposer les règles de sécurité et de confidentialité qui ont été mise dans l'entreprise auprès de tous les employés en situation de mobilité. Le smartphone est aujourd'hui, qu'on le veuille ou non, une extension du système d'information de l'entreprise et il faut pouvoir en assurer la confidentialité comme tel.

———-
[1] Etude Apec Janvier 2014 / http://www.fedoffice.fr/nomadisme-au-travail-les-salaries-se-decentralisent
[2] Canadian spy agency gleaned passengers' data from airport's Wi-Fi: CBC, The Star, 30 janvier 2014
[3] 2014 Trustwave Global Security Report / http://www2.trustwave.com/rs/trustwave/images/Trustwave_GSR_ExecutiveSummary_4page_Final_Digital.pdf

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

Source : http://www.journaldunet.com/solutions/expert/59720/le-nomadisme-ravive-la-question-de-la-confidentialite-des-donnees.shtml
Par Richard Marry

Une solution pour identifier des utilisateurs vulnérables aux cyber-attaques ?



Une solution pour identifier des utilisateurs vulnérables aux cyber-attaques ?

La société Fujitsu a annoncé avoir développé une technologie permettant d'identifier les utilisateurs vulnérables aux cyber-attaques, ayant des comportements potentiellement « à risque » donc vulnérables aux cyber-attaques. La solution est basée sur l'analyse des activités des utilisateurs sur leur ordinateur.

Cette technologie permettrait de créer des mesures de sécurité plus adaptées, comme l'affichage de messages individualisés d'alertes aux utilisateurs qui cliquent souvent sur les liens ou e-mails suspicieux, ou augmenter le niveau de menace lié aux e-mails envoyés entre départements d'une même entreprise par des utilisateurs propices à être infectés par des virus.
Jusqu'ici, un des problèmes des logiciels de sécurité est de ne pas pouvoir contrôler l'erreur humaine, comme la propension d'un utilisateur à cliquer sur les liens malveillants dans des e-mails, ou sur des sites infectés. Cette technologie permettrait d'y remédier.
Afin de développer cette solution, Fujitsu a utilisé un questionnaire en ligne, réalisé avec des experts en psychologie sociale, afin d'identifier les traits psychologiques des personnes vulnérables à trois types d'attaques : les infections par un virus, les arnaques et les fuites d'information. La société s'est également intéressée aux activités des utilisateurs pour les e-mails, l'accès internet ainsi qu'aux actions de la souris et du clavier.
Cette technologie a été présentée en détail lors du 32ème Symposium sur la Cryptographie et Sécurité de l'Information qui se tient depuis le 20 Janvier dans la ville de Kita-Kyushu.
http://www.bulletins-electroniques.com/actualites/77686.htm
http://ajw.asahi.com/article/business/AJ201501190057
http://www.fujitsu.com/global/about/resources/news/press-releases/2015/0119-01.html

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

Source :
http://www.infohightech.com/une-solution-pour-identifier-des-utilisateurs-vulnerables-aux-cyber-attaques/

Les services DDoS à la demande des pirates de Sony, Lizard Squad, piratés

	Les services DDoS à la demande des pirates de Sony, Lizard Squad, piratés

L’adage veut que les cordonniers soient toujours les plus mal chaussés. Le piratage de LizardStresser, le service de DDoS à la demande de Lizard Squad, tend à confirmer cette règle : le fichier contenant les identifiants et mots de passe des membres n’était même pas chiffré.

Petit retour en arrière. Nous sommes fin décembre, à quelques heures de Noël, et le groupe de pirates connu sous le nom de Lizard Squad se rappelle au bon souvenir de tout le monde en mettant le PlayStation Network et le Xbox Live hors ligne. Les conséquences s’étendent sur plusieurs jours et le collectif peut se réjouir : il a livré une démonstration très visible de la force de frappe de son réseau basé sur des routeurs piratés. Son service LizardStresser, qui propose de lancer des attaques DDoS à la demande, enregistre alors de nombreuses inscriptions.
Mais cette période faste n’a été que de courte durée. En effet, outre plusieurs arrestations, notamment outre-Manche, un autre pirate ou groupe de pirates s’en est pris au site hébergeant le service LizardStresser. Le service en lui-même est a priori intact, mais sa base de données incluant notamment les pseudonymes et mots de passe des membres est maintenant dans la nature. Or, de manière assez curieuse, Lizard Squad n’a pas jugé nécessaire de se protéger contre le piratage : ses fichiers sont stockés en clair.

Ceux-ci ayant rapidement été publiés, tout le monde a pu voir que les affaires marchaient plutôt bien. Au moment du piratage, LizardStresser comptait la bagatelle de 14 241 membres. Beaucoup, toutefois, n’étaient que des curieux. Comme le pointe KrebsonSecurity, ils n’étaient « que » quelques centaines à avoir alimenté leur compte dans le but de financer une attaque. En tout, Lizard Squad aurait perçu un peu plus de 11 000 $, versés en bitcoins.
Bien sûr, le collectif de pirates n’a que modérément apprécié de voir de ses précieuses données étalées sur la toile. Une copie des documents, en particulier, était disponible sur Mega. Le groupe ne s’est donc pas démonté et a formulé une requête au titre de la loi DMCA, qui protège le droit d’auteur en imposant aux hébergeurs de retirer les contenus publiés illégalement. Comble de l’absurde, celle-ci a été acceptée. De nombreuses copies, néanmoins, demeurent disponibles sur d’autres sites.

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

Source : http://www.lesnumeriques.com/lizard-squad-service-ddos-a-demande-pirate-n38817.html

Forum international de la Cybercriminalité: Bernard Cazeneuve débloque 108 millions d’euros pour aider les enquêteursNicolas Messayaz / Sipa Olivier Aballain

Forum international de la Cybercriminalité: Bernard Cazeneuve débloque 108 millions d’euros pour aider les enquêteurs

Denis JACOPINI, expert judiciaire en informatique diplômé en Cybercriminalité, était présent ce mardi au 7eme Forum International de lutte contre la Cybercriminalité.

Le repérage et la traque des réseaux jihadistes sur internet sont au programme de Bernard Cazeneuve ce mardi: le ministre de l’Intérieur a ouvert à Lille le 7e Forum international de lutte contre la Cybercriminalité (FIC).
Le rendez-vous tombe à pic, puisque Manuel Valls lui-même a rappelé le 19 janvier sur i-Télé que «ce n’est pas dans les mosquées que ces recrutements [de djihadistes] s’organisent, c’est le plus souvent sur internet».
Après une rencontre avec le ministre de l’Intérieur allemand, Bernard Cazeneuve a prononcé un discours vers 10h au cours duquel il a annoncé le déblocage de 108 millions d’euros sur 3 ans pour développer les moyens des services de l’État pour l’enquête en matière de criminalité sur internet

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

Source : http://www.20minutes.fr/lille/1521015-20150120-direct-bernard-cazeneuve-forum-international-cybercriminalite
Par Olivier Abalain

Le Forum International de la Cybersécurité FIC 2015 en vidéo

Le Forum International de la Cybersécurité FIC 2015 en vidéo

« Nous sommes tous les vecteurs de cyberattaques » pour le fondateur du Forum de la cybercriminalité »

Le ministre de l'Intérieur Bernard Cazeneuve a inauguré mardi matin le Forum international de cybersécurité à Lille. Le général Marc Watin-Augouard, fondateur du Forum FIC et directeur du CREOGN, a expliqué que « nous sommes tous les vecteurs de cyberattaques, soit directes, soit par rebonds. »

Source vidéo : « Nous sommes tous les vecteurs de cyberattaques » pour le fondateur du Forum de la cybercriminalité

La cybersécurité au Grand Palais

Orange, cybersécurité et cyberdéfense

Le plateau TV pendant le Forum International de la Cybersécurité 2015 – FIC 2015
Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://videos.tf1.fr/infos/2015/nous-sommes-tous-les-vecteurs-de-cyberattaques-pour-le-fondateur-8549855.html

Les pertes de données d’entreprise ont augmenté de 400 % depuis 2012

Les pertes de données d’entreprise ont augmenté de 400 % depuis 2012

Selon une étude menée dans une vingtaine de pays, les interruptions d’activité dues à la perte de données coûtent environ 1,5 milliard d’euros par an aux entreprises.

64 % des entreprises ont subi une perte de données ou une interruption d’activité en 2014. Un chiffre important qui en cache un autre : le nombre de données perdues a augmenté de 400 % depuis 2012 !
Selon une étude (1) réalisée auprès de 3 300 décideurs informatiques dans 24 pays (dont la France), ces interruptions d’activité non planifiées ont provoqué une perte de chiffre d’affaires (36 % des entreprises interrogées) et des retards dans le développement des produits (34 % des entreprises interrogées). Au total, les interruptions d’activité dues aux pertes de données coûtent plus d’1,7 milliard de dollars (environ 1,5 milliard d’euros) aux entreprises chaque année. « Cette étude souligne l’énorme impact budgétaire des interruptions d’activité non planifiées et de la perte de données dans les entreprises où qu’elles se trouvent » explique Chritian Hiller président EMC France.

Big data, mobilité et cloud hybride
A l’heure où les entreprises songent à externaliser leurs données dans les nuages, les décideurs informatiques reconnaissent les failles de leur stratégie : 51 % des entreprises interrogées ne disposent d’aucun plan de reprise après sinistre. Seules 6 % ont prévu un plan en environnement big data, mobilité et cloud hybride. Une très forte majorité des sondés (62 %) estime que ces trois environnements (big data, mobilité et cloud hybride) sont « difficiles » à protéger.
L’étude Vanson Bourne souligne enfin que c’est en Chine que l’on compte le plus grand nombre d’entreprises impliquées dans la protection de leurs données.
(1) Etude menée par le cabinet Vanson Bourne pour le compte de l’entreprise EMC.

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

Source : http://www.archimag.com/veille-documentation/2015/01/07/pertes-donn%C3%A9es-entreprise-augment%C3%A9-400-depuis-2012-0
Par Bruno Texier

1.300 cyberattaques « au nom d’organisations islamistes » radicales, annonce Bernard Cazeneuve

1,300 cyberattaques « au nom d’organisations islamistes » radicales, annonce Bernard Cazeneuve

Lors d’une visite à la sous-direction de lutte contre la cybercriminalité de la police judiciaire (PJ) française à Nanterre (Hauts-de-Seine), Bernard Cazeneuve a annoncé lundi que « plus de 1.300 attaques ont été revendiquées par des équipes (de) hackers se revendiquant d’organisations islamistes » radicales. Le ministre de l’Intérieur a également indiqué que plus de 25.000 sites français avaient été piratés.

La plateforme gouvernementale nationale Pharos, où sont signalés en France les contenus illicites liés à Internet, « a traité plus de 25.000 signalements de contenus illicites sur le net », a en effet déclaré Bernard Cazeneuve, évoquant des « cyberattaques malveillantes » sur des sites institutionnels et privés. Des « contact privilégiés » ont été noués avec Facebook, Dailymotion ou Google et des « demandes de retraits en ligne » ont eu lieu par exemple de sites ou vidéos « liés aux attaques terroristes ».

Des propositions mercredi

« La puissance publique doit prendre des initiatives et affirmer sa puissance pour protéger les internautes » face aux « menaces », a réaffirmé le locataire de la place Beauvau, « dans le respect des libertés publiques ».

Mercredi, à l’issue du Conseil des ministres, des mesures antiterroristes seront présentées par le gouvernement dont certaines visant Internet, a réaffirmé Bernard Cazeneuve. La semaine dernière, Manuel Valls lui avait demandé des propositions « dans les huit jours » concernant le contrôle d’Internet. « Elles devront concerner (…) les réseaux sociaux, plus que jamais utilisés pour l’embrigadement, la mise en contact et l’acquisition de techniques permettant de passer à l’acte », précisait alors le Premier ministre.

D’ici là, Bernard Cazeneuve se rend mardi à Lille pour le Forum international « sur la cybersécurité » en compagnie de son homologue allemand, Thomas de Maizière.

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

Source : http://www.lejdd.fr/Medias/Internet/1-300-cyberattaques-au-nom-d-organisations-islamistes-radicales-annonce-Bernard-Cazeneuve-713734

Mots de passe : « 123456 » toujours le plus utilisé

Mots de passe : « 123456 » toujours le plus utilisé

Les années passent et la situation reste la même : les internautes continuent à créer des mots de passe basiques et simples à deviner. Et pourtant, toutes les conditions sont réunies pour une prise de conscience avec la multiplication des fuites de données et leur médiatisation. Sans parler des discours martelés par les experts, eux-aussi de plus en plus diffusés sur les médias dits traditionnels.

Mais rien y fait : Mme Michu continue à protéger son client mail par le mot de passe ‘123456’. C’est le constat du traditionnel palmarès (Amérique du Nord et Europe de l’Ouest) des mots de passe les plus utilisés établi par Splashdata. En seconde place, on trouve le très complexe ‘password’. Les deux lauréats occupent les deux premières positions depuis maintenant trois ans, devant le plus compliqué à trouver… ‘12345’ ou encore ‘12345678’.
Onoubliera pas non plus le célèbre ‘qwerty’ ou ‘azerty’ pour les français qui rendent hilares les pirates de la planète. Petites nouveautés dans le Top 20, la présence de noms de superhéros comme superman ou batman, très utilisés par les fans de comics mais dont la protection est quasiment aussi nulle que les autres.

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

Source : http://www.zdnet.fr/actualites/mots-de-passe-123456-toujours-le-plus-utilise-39813303.htm

---

Faut-il craindre une cyberguerre ?

Faut-il craindre une cyberguerre ?

Leurs PC sont leurs armes et leur guerre se mène en ligne. Après les attentats à Paris, des cyberattaques ont été menées contre des sites internet français, par des hackers affirmant agir au nom du groupe Etat islamique (EI). Dans le même temps, des « hacktivistes » se revendiquent d'Anonymous ont piraté des sites et comptes sur les réseaux sociaux des organisations islamistes et de leurs membres.

Mais c'est loin d'être terminé. Des comptes YouTube et Twitter appartenant au commandement militaire américain au Moyen-Orient (Centcom) ont également été visés, et une attaque d'envergure est annoncée pour jeudi 15 janvier. Sommes-nous à l'aube d'une cyberguerre ? Non, toujours pas, répond Gérôme Billois, expert en sécurité informatique au cabinet Solucom et administrateur du Club de la sécurité de l'information français (Clusif).

Francetv info : Peut-on parler de cyberguerre lorsque l'on évoque les attaques informatiques menées par des hackers qui se revendiquent du jihad ?
Gérôme Billois : Non, on n'y est pas du tout. Ce serait exagéré de parler de « guerre ». Aujourd'hui, nous parlons d'actes qui n'ont pas d'effets dans le monde réel. Il n'y a pas d'explosions, pas d'interruption de services essentiels comme l'énergie ou les transports. Il n'y a pas non plus de pertes humaines. On reste dans le monde virtuel.

Alors comment pourrait-on appeler cela ?
Il n'existe pas vraiment de mot pour déterminer ces actes. Après l'attaque contre la société Sony Pictures, qui a subi une destruction massive de son système d'information et le vol d'une importante quantité de données, Barack Obama parlé de cybervandalisme. Le terme semble assez juste. Ce qui se passe aujourd'hui, c'est comme si des activistes entraient dans des centaines de boutiques pour y coller leurs affiches et repartir. Les propriétaires de ces magasins n'avaient pas bien fermé la porte en partant et en revenant le lendemain matin, ils trouvent des affiches qui font la publicité de l'Etat islamique.

Pour vous, ces actions restent plutôt d'ordre symbolique ?
Extrêmement symbolique, puisqu'il s'agit d'une lutte entre deux idéologies. Avec d'un côté l'#opFrance (pour « Opération France », lancée par des cyberjihadistes), annoncée pour le 15 janvier, qui vise à tenir l'image de la France en attaquant un grand nombre de structures dans l'Hexagone, et de l'autre l'#opCharlieHebdo, qui vise à dénoncer et rendre indisponibles des sites jihadistes.

Qui se trouve derrière cette contre-attaque ? Certains revendiquent leur appartenance aux Anonymous…
On ne peut pas dire qu'il s'agit « des » Anonymous. Ce sont, en fait, des groupes très divers. Il faut d'ailleurs savoir que certains des groupes qui attaquent la France aujourd'hui ont pu participer à des opérations des Anonymous, ou s'en revendiquer. Il y a des acteurs en commun, qui œuvraient auparavant dans une même direction et se divisent aujourd'hui sur ce cas particulier. La logique de « l'hacktivisme » au sens large c'est : « Il se passe un événement, je me positionne par rapport à celui-ci et à chaque nouvel événement je redéfinis ma doctrine ».

Quelle est la force de frappe des cyberjihadistes aujourd'hui ?
Aujourd'hui, ils mènent des attaques de faible intensité. Sur une échelle de 1 à 10, ils atteignent 5, au maximum. Ces piratas utilisent des vulnérabilités connues depuis longtemps ainsi que des outils disponibles facilement sur internet. De plus, ils s'attaquent à des sites peu sécurisés et pas mis à jour. Il existe tout de même un risque à moyen terme. Ces groupes de pirates, petit à petit, vont apprendre, se développer, et augmenter ainsi leurs capacités d'attaque pour viser des services plus importants. On sait que l'EI dispose d'importants moyens financiers. Il n'aura, de toutes façons, pas de problème de matériel : avec un simple PC, vous pouvez lancer des attaques.

Qu'est-ce qui pourrait rendre ces groupes plus dangereux ?
Pour eux, il s'agit d'abord de gagner en expérience. Mais ils peuvent aussi acheter ce qu'on appelle des « vulnérabilités zero day », c'est-à-dire des connaissances sur une vulnérabilité qui n'est pas encore connue des éditeurs de sécurité. Quand vous possédez cet atout, vous pouvez attaquer un système, même s'il est mis à jour. Pour poursuivre l'analogie des boutiques vandalisées : imaginons que quelqu'un, comme un chercheur, découvre que pour la marque de serrure XYZ il existe un pass universel. Avec cette information, il peut faire deux choses : soit prévenir le fabricant de la serrure pour qu'il corrige son produit, soit vendre cette vulnérabilité à des criminels sur le marché noir.

Les pirates ont donc toujours un temps d'avance sur les systèmes de sécurité…
Oui et non. Une partie des pirates, les plus pointus, certains groupes de cybercriminels, peuvent aller jusqu'à dédier une partie de leurs moyens à faire de la recherche en attaques et trouver ces « vulnérabilités zero day ». Ces groupes-là, oui, peuvent avoir cette capacité. Il peut s'agir soit d'Etats un peu belliqueux, soit de cybercriminels pointus. Mais il n'y en a pas des milliers. Dans le cas qui nous intéresse, les pirates n'ont pas cette avance. Ils utilisent simplement des failles connues, dont certaines ont été rendues publiques depuis 2012. Or, nous sommes en 2015 et les systèmes qu'ils attaquent n'ont pas été corrigés. On parle de petites mairies, d'universités, de PME… Ces structures-là n'ont pas forcément l'expertise ni les moyens pour maintenir leurs systèmes à jour.

D'autres structures, susceptibles de devenir des cibles plus importantes comme les grandes banques françaises par exemple, sont-elles mieux protégées ?
Oui, les systèmes sensibles sont mieux protégés. Les grandes sociétés ont les capacités nécessaires pour investir dans la sécurité. Les banques en ligne, par exemple, réalisent quotidiennement, voire plus encore, des tests de vulnérabilité automatisés, qui mènent les mêmes actions que les pirates. Les résultats de ces tests remontent aux services de sécurité informatique qui peuvent très rapidement effectuer les mises à jour nécessaires. Ce qui n'empêche qu'un site d'une grande banque est tombé, pendant une des attaques. Mais il s'agissait d'un site satellite sur lequel il n'y avait aucune transaction financière.

Là, nous parlons de sites internet. Qu'en est-il des systèmes informatiques internes ?
Ces systèmes-là disposent d'un niveau de sécurité, a priori, plus fort. Ne peuvent y rentrer que des employés ou des collaborateurs connus. Soit parce qu'il existe une protection physique : il faut entrer dans le bâtiment de la société. Soit parce qu'il y a des mots de passe ou des cartes à puce pour accéder à distance aux données. On n'est pas pour autant à l'abri d'une attaque visant le système d'information interne. C'est ce qui est arrivé chez Sony. Le FBI l'a dit : 90% des sociétés américaines seraient tombées si elles avaient été confrontées à la même méthode de piratage. C'est énorme.

Donc la menace existe…
Oui. La vraie question est de savoir si les jihadistes passeraient à ce type d'actions. Leur logique, pour l'instant, est plutôt de faire du bruit, de multiplier les cibles, de casser des milliers de sites, pour pouvoir dire mille fois qu'ils l'ont fait. Une attaque plus poussée, qui ferait plus de mal, aurait peut-être moins de résonance médiatique.

C'est tout de même une menace prise au sérieux, sur laquelle l'Otan se penche sérieusement. Est-ce à cause des menaces de ces jihadistes ?
Pas seulement. On distingue trois grandes « familles d'attaquants » : les « hacktivistes », qui attaquent par idéologie comme les cyberjihadistes, les cybercriminels, qui volent des données pour les monnayer, et enfin les Etats, qui développent des capacités défensives et offensives. Mais on peut craindre des regroupements entre ces groupes. Dans l'exemple de Sony, l'attaque est attribuée à la Corée du Nord, mais on sait qu'elle aurait été appuyée par des groupes d' «hacktivistes ».

Comment les Etats se préparent-ils face à cette menace ?
La cyberdéfense ne se résume pas à créer des murs en attendant que des pirates tentent de les casser. Cela inclut aussi des techniques de contre-attaque, pour pouvoir neutraliser les attaquants. Tous les Etats s'y préparent. Pour ce qui est de mener des attaques, on peut estimer que tous les pays industrialisés ont déjà des moyens et les renforcent au quotidien.

Concrètement, en quoi consiste la contre-attaque face à des cyberjihadistes ?
Les moyens de contre-attaque sont quasiment les mêmes que les moyens d'attaque. On peut imaginer attaquer leurs systèmes, les rendre inopérants, capturer les données pour bien comprendre qui ils sont. On peut aussi « boucher leurs tuyaux » pour éviter que les attaques ne passent.
Mais la difficulté, dans ce domaine, est de bien savoir qui se trouve en face de nous. Dans le cas Sony, on lit que l'attaque serait partie d'un hôtel en Thaïlande. A mon avis, elle est passée par là, mais ce n'est pas son point de départ. J'ai déjà vu des attaques menées contre certains de mes clients provenir de serveurs d'écoles maternelles au Vietnam. On se doute bien que ce n'est pas un écolier vietnamien qui l'a lancée, qu'il s'agit simplement de brouiller les pistes. Dans des scénarios plus vicieux, il peut s'agir de faire croire que l'attaque vient d'un endroit en particulier, pour provoquer une contre-attaque sur cette cible. Si l'on n'attribue pas l'attaque au bon responsable, on risque d'infliger des sanctions à un leurre.

Quand vous parlez de « boucher les tuyaux », s'agit-il d'attaques par déni de service, méthode qu'utilisent justement certains hackers ?
Cette méthode-là n'est efficace que temporairement, pour freiner une attaque. Mais les Etats ont la possibilité, à distance, de faire tomber les réseaux, de les couper, plutôt que de les boucher. Je parle bien des Etats, car les entreprises privées n'ont pas le droit de contre-attaquer. La légitime défense n'existe pas dans le cyberespace. En France, le seul cadre légal aujourd'hui, c'est la loi de programmation militaire, qui donne cette capacité à l'Agence nationale de sécurité des systèmes d'information (Anssi) ou, en tout cas, aux services rattachés au Premier ministre.

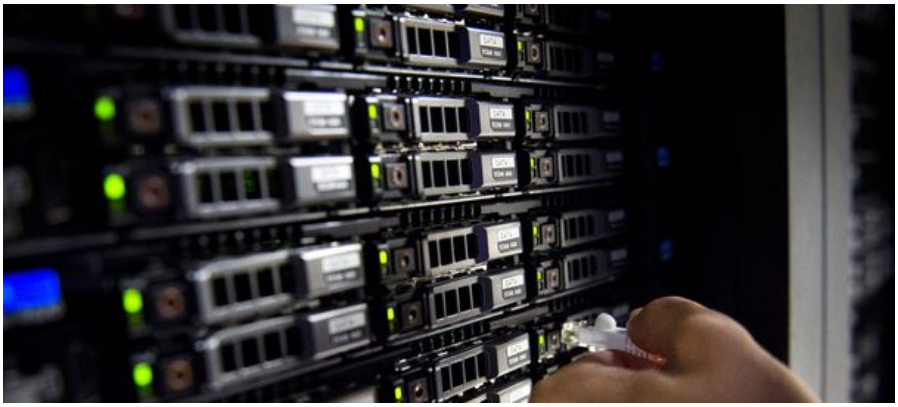
Manuel Valls va annoncer une série de mesures, dont certaines concernent internet. Où placer le curseur, entre la neutralité de net, le verrouillage pour empêcher les cyberjihadistes de nuire et la protection de la vie privée ?
C'est une question idéologique fondamentale, mais on n'y trouvera pas de réponse parfaite. Ce qui est certain, c'est qu'il y a une menace, qui, il faut le préciser, représente une très faible portion des usages d'internet. L'énorme majorité des usages sont très bénéfiques, pour l'économie, la culture, notre quotidien. Le plus important, selon moi, c'est le contrôle des moyens qu'on se donne. Il faut, certes, pouvoir être très réactif, car les attaques peuvent être menées très vite, mais il faut se contrôler pour éviter de tomber dans la surveillance généralisée. Ce contrôle peut être exercé par la justice ou des autorités indépendantes.

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

Source : http://www.francetvinfo.fr/monde/terrorisme-djihadistes/faut-il-craindre-une-cyberguerre_796909.html

---

Trois contrats pour assurer son informatique



Trois contrats pour assurer son informatique

En France, en 2013 les violations de données informatiques ont coûté 6,1 milliards d'euros aux victimes dans le monde professionnel.

Qu'elle soit de production ou de gestion, l'informatique est présente dans chaque entreprise. Il est nécessaire de couvrir non seulement le matériel, mais également les données qu'elle contient. En France, en 2013 les violations de données informatiques ont coûté 6,1 milliards d'euros aux victimes dans le monde professionnel : trois fois plus qu'en 2010 (2,2 milliards d'euros). En 2014, le coût par donnée piratée se chiffrerait à 351 euros contre 98 euros en 2010, selon les estimations de la société de sécurité informatique Symantec.
Aux traditionnels risques de dommages du matériel informatique et de responsabilité civile, s'ajoute depuis peu, la cybercriminalité. Le point sur les trois catégories de contrat que peut souscrire l'entreprise.
A noter : les contrats multirisques de matériels de bureaux peuvent couvrir les dommages informatiques. En revanche, la responsabilité civile comme la criminalité informatique font l'objet de contrats spécifiques, à souscrire séparément.

1. Dommages informatiques
Existant sur le marché français depuis une quinzaine d'années, l'assurance de dommages couvre le matériel informatique en cas d'incendie et de vol. L'assureur garantit essentiellement les frais de reconstitution des données et les coûts supplémentaires d'exploitation, en versant un capital à l'entreprise ayant subi un dommage. Traditionnellement, cette garantie faisait l'objet d'un contrat d'assurance « Tous Risques Informatiques ». Mais la tendance consiste à l'inclure dans le contrat « Multirisques Bureaux ».

2. Responsabilité civile
A ce stade, il faut distinguer la responsabilité civile d'exploitation, de la responsabilité professionnelle.
La responsabilité civile d'exploitation joue par exemple lorsqu'une entreprise transmet un virus informatique à un client.
La responsabilité civile professionnelle pour les mises en cause de l'entreprise au titre de ses prestations : conseils ou services. « Couvrant les dommages immatériels causés au cours d'une mission, la responsabilité civile professionnelle intéresse surtout les sociétés d'informatique », précise Benoît Salembier, à la tête du cabinet de courtage Add Value Assurances.

3. Criminalité informatique
Les compagnies d'assurance anglo-saxonnes ont une longueur d'avance sur leurs homologues européens. Les quelques acteurs en pointe sur les nouvelles technologies – Ace Europe, Hiscox, Beazley, Chartis, CNA – proposent un contrat ou garantie réduisant les risques de piratage et d'intrusion dans les systèmes d'information d'une entreprise.
Le contrat « Cybercriminalité » proposé par le courtier Add Value permet à l'entreprise de couvrir sa responsabilité et les dommages subis suite à une attaque informatique. « Les frais de restauration des données perdues constituent un vrai sujet. Les pertes de revenus ou d'exploitation consécutives à cette attaque sont également à prendre en compte. Quand on est une marque importante, il arrive que les hackers demandent une rançon à l'entreprise attaquée pour lui restituer les données », détaille Benoit Salembier.
Deux critères jouent sur le risque de criminalité. D'une part la taille de la base de données d'une entreprise : plus elle est grande, plus elle est exposée aux risques de piratage. D'autre part, la nature des données. Plus elles sont sensibles, plus elles sont exposées à la cybercriminalité. Ainsi par exemple les cabinets d'avocats, les experts comptables et même les journalistes seraient particulièrement visés.

Cybercriminalité : deux exemples de sinistres garantis
Avec le concours d'Add Value Assurances, voici deux cas de criminalité informatique réels avec les garanties que vous pouvez demander à votre assureur.
Exemple n°1. Piratage d'un site internet
Une société X crée un site e-commerce afin de vendre ses produits au grand public. Son succès attise la convoitise de ses concurrents. Des hackers réussissent à pirater son site et à le mettre hors service, ce qui signifie l'arrêt quasi complet de l'activité. En effet cette société commercialise ses produits à 75% sur internet.
L'assureur peut prendre en charge les frais engagés par les consultants mandatés pour identifier la faille de sécurité, et remettre le site web en état, à hauteur du plafond de garantie défini dans le contrat. De même, il indemnise l'entreprise de la perte de chiffre d'affaires sur la période d'arrêt du site internet, à hauteur du plafond de garantie défini dans le contrat.

Exemple n°2. Extorsion de données clients
Des hackers ont détourné une base de données clients d'une agence de voyage comprenant notamment leurs coordonnées bancaires. Ils demandent une rançon de quelques centaines de milliers d'euros euros à la direction pour la récupérer. Après deux semaines de négociation et le paiement de la rançon, l'entreprise piratée récupère sa base de données.
La base de données était assurée. L'assureur mandate ses consultants spécialisés pour accompagner l'assuré et mener à bien les négociations. Il indemnise l'entreprise assurée pour le paiement des honoraires des consultants et de la rançon, dans la limite des plafonds définis dans le contrat.
A noter. Avant de souscrire un contrat informatique, mieux vaut s'adresser à un expert qui déterminera votre exposition aux risques. En fonction de cela, votre intermédiaire d'assurance – courtier ou agent – évaluera le capital à assurer. Bien sûr, il faut être vigilant aux exclusions, c'est-à-dire les cas où l'assurance ne joue pas. Exemple : les dommages dus à une erreur de programmation sont généralement exclus. Et bien examiner les plafonds de garantie et les franchises

En savoir plus sur
http://lentreprise.lexpress.fr/gestion-fiscalite/responsabilites-assurances/trois-contrats-pour-assurer-son-informatique_1641399.html

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

Source :
http://lentreprise.lexpress.fr/gestion-fiscalite/responsabilites-assurances/trois-contrats-pour-assurer-son-informatique_1641399.html
Par Martine Denoune