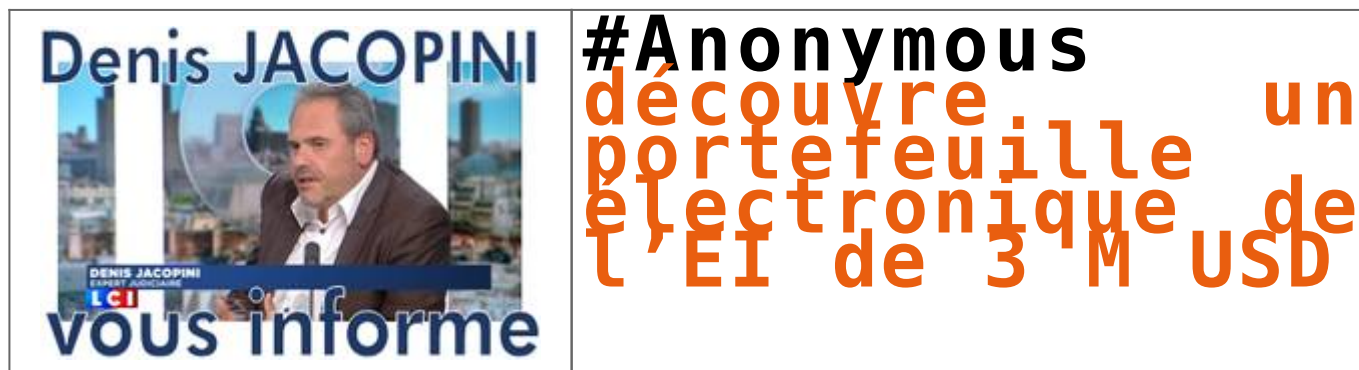


Anonymous découvre un portefeuille électronique de l'EI de 3 M USD



Le groupe hacktiviste Anonymous déclare avoir découvert un portefeuille électronique du groupe terroriste Etat islamique dans le système Bitcoin.

Le groupe de hackers Anonymous tient ses promesses. Suite aux attentats de Paris, les hackivistes ont déclaré une « guerre sans merci » à l'Etat islamique (EI). Bien que tournés en ridicule par des gens qui affirmaient que leurs actions n'avaient aucun de poids comparé au sang réel qui était versé par les terroristes, ils sont rapidement passés à l'action. Ayant annoncé avoir piraté plus de 5.000 comptes de propagande liés à l'Etat islamique sur Twitter, ils déclarent maintenant avoir découvert un portefeuille électronique de l'EI de 3 millions de dollars en bitcoins, un système de paiement sur Internet.

Les Anonymous piratent plus de 5.000 profils de l'EI sur Twitter

« L'Etat islamique utilise de la crypto-monnaie pour financer ses opérations en cours et nous avons réussi à découvrir plusieurs adresses Bitcoin qu'il utilise », ont déclaré les Anonymous dans un commentaire pour NewsBTC. L'une des plus importantes fonctions de la monnaie cryptographique est qu'elle ne peut être censurée à la demande d'un tiers. On ne sait jamais ce qui sera ensuite à l'ordre du jour. Les activistes pour les droits des animaux, les défenseurs de l'environnement ou d'autres groupes dont les comptes peuvent être bloqués optent tous pour le Bitcoin, car il s'agit d'un service libre. Ainsi, le Bitcoin encourage à la fois des objectifs objectivement honorables mais peut aussi servir des intérêts qui le sont un peu moins, comme ceux de l'EI par exemple.

C'est pourquoi il constitue l'un des leviers numériques privilégiés par l'EI pour aider « ses amis » de Syrie, d'Irak, du Liban et de partout dans le monde.

Anonymous déclare (pour de bon) la guerre à l'EI

Pourtant, l'espoir n'est pas perdu. Le groupe hacktiviste Anonymous assure avoir réussi à bloquer la plupart des comptes de l'EI en Bitcoin qui avaient été dissimulés sur un type de bases de données appelé « deep Web ». Plus tôt, les hacktivistes s'étaient fixés pour mission d'anéantir la propagande terroriste ainsi que les réseaux de recrutement de l'EI sur Internet. Dans une vidéo publiée sur YouTube, un porte-parole de l'organisation virtuelle s'était engagé à « lancer la plus grande opération de tous les temps » contre l'EI.



Réagissez à cet article

Source

<http://fr.sputniknews.com/international/20151121/1019708957/anonymous-portfeuilles-ei-hactivistes-hackers.html>

Le Medef demande aux patrons de signaler la radicalisation des salariés



Le vice-président du Medef, Geoffroy Roux de Bézieux, pense que, comme tout citoyen, les chefs d'entreprise doivent dénoncer les dérives radicalistes au sein de leur entreprise.

«quelqu'un a un comportement radicaliste, le devoir du chef d'entreprise, comme tout citoyen, c'est de signaler à la police ce comportement», estime le vice-président du Medef, Geoffroy Roux de Bézieux, tout en soulignant que ces cas restaient exceptionnels.

Certaines entreprises, notamment la RATP ou encore Air France, la SNCF, La Poste, font face à des incidents liés à une pratique rigoriste de l'Islam: refus d'obéir à des femmes, refus de conduire un bus si une femme l'a au préalable conduit, salariés qui s'arrêtent de travailler pour prier, etc.

Pour lutter contre ces aberrations, le Medef pense que les entreprises ont un rôle à jouer. Pour cela «nous avons recommandé à nos adhérents d'être vigilants sur des dérives radicalistes dans les entreprises», déclare le vice-président du Medef.

La laïcité s'applique dans les lieux publics mais aussi aux fonctionnaires. Le patronat souhaite-t-il aller plus loin jusqu'à imposer ce principe dans l'entreprise? «Nous sommes encore sous le coup de l'émotion et donc pas en mesure d'affirmer quoi que ce soit sur le sujet, mais, en tout cas, c'est une question qui est posée», déclare Geoffroy Roux de Bézieux, prudent.

Valorisation des réservistes

Parmi les autres travaux lancés, la sécurité des entreprises et des salariés. D'ailleurs, les sites industriels ont renforcé leur sécurité depuis l'attaque de Charlie Hebdo. L'Union des industries chimiques a demandé mardi au ministère de l'Environnement le retrait de toutes les informations relatives aux productions et aux stocks (lieu par exemple) des usines du secteur qui sont publiées sur des sites Internet.

Parmi les 1200 sites Seveso (qui représentent des risques associés à certaines activités industrielles dangereuses), la moitié appartient au secteur de la chimie.

Une autre piste de réflexion: la valorisation et gestion des salariés qui font partie de la réserve opérationnelle que ce soit à travers l'armée ou les sapeurs-pompiers volontaires. L'idée du Medef est de simplifier leur mobilisation et de valoriser l'expérience qu'ils apportent aux entreprises.

D'ailleurs, depuis les attentats de vendredi, les centres d'information et de recrutement des armées font le plein aussi bien sur le web que dans leurs centres d'accueil répartis sur toute la France.

Interrogé par Ouest-France après les attentats de vendredi dernier, le général de brigade Thierry Marchand, à la sous-direction du recrutement de l'armée de terre, annonçait plus de 1000 appels par jour.

Enfin, l'organisation patronale a exprimé son souhait de travailler avec le gouvernement et tous les acteurs concernés pour atténuer l'impact économique des événements dans le secteur du commerce et du tourisme malgré les nécessaires mesures de sécurité.



Réagissez à cet article

Source

<http://www.lefigaro.fr/societes/2015/11/20/20005-20151120ARTFIG00188-le-medef-demande-aux-patrons-de-signaler-la-radicalisation-des-salaries.php>

Comment protéger au mieux les données clients des cyberattaques ?



Les derniers piratages des données bancaires de plus de 1,3 millions de clients Orange, les 83 millions de données de clients volées à la banque américaine JP Morgan Chase ou les menaces d'hackers de divulguer l'identité de 36 millions d'utilisateurs du site de rencontres canadien Ashley Madison... Tous ces épisodes démontrent que les cyber-attaques menacent aujourd'hui fortement la liberté individuelle et les données personnelles.

Elles viennent également rappeler qu'aucune entreprise, même bien protégée, n'est aujourd'hui en mesure de garantir à 100% la sécurité des données qu'elle manipule. Face à ce constat, les entreprises doivent changer la façon dont elles peuvent rapidement détecter et répondre en utilisant de nouvelles solutions plus précises, plus actionnables pour les équipes de sécurité.

C'est un véritable enjeu pour les entreprises d'assurer à leurs clients la protection la plus fiable possible.

Voici 4 conseils aux entreprises pour protéger au mieux les données sensibles de leurs clients et les actions à mettre en place lors d'une attaque :

- Toute organisation chargée de la gestion des données personnelles très sensibles de leurs clients doit prendre ses responsabilités très au sérieux et protéger ainsi les données contre les accès non autorisés indésirables. Cela impliquerait de multiples niveaux de contrôles de sécurité au niveau de l'IT, peut-être en commençant par le cryptage des données personnelles alors qu'elles sont actives et en cours d'utilisation. Cette approche peut être efficace à la protection des données hautement sensibles, même si le réseau dans lequel elles résident est compromis. Cela peut paraître coûteux à mettre en œuvre mais c'est une méthode de protection efficace.

- Il est capital d'avoir des processus et procédures internes qui garantissent l'accès physique aux centres de stockage de données sécurisées y compris de CLOUD. Les comptes d'utilisateurs inutilisés devraient être supprimés rapidement et les restrictions d'accès gérés de façon stricte pour s'assurer que tous les employés n'aient pas accès aux données de n'importe quel autre utilisateur.

- Nous pouvons également parler d'une nouvelle génération, solide dans son approche, permettant d'atténuer les menaces (en constante évolution) d'attaques malveillantes des réseaux d'entreprise provenant de l'extérieur. Les organisations "pirates" peuvent percevoir cela comme une énorme opportunité financière à voler les données personnelles détenues par quelque organisme que ce soit. Le fait d'avoir des défenses périmétriques fortes mises en place comme un pare-feu, des anti-virus sur toutes les stations de travail, d'une solution de filtrage d'e-mail, ou encore d'une solution IPS / IDS et un SIEM offrant la possibilité de surveiller les événements de toutes ces technologies en un seul endroit, ne restent malheureusement pas les plus fiables et beaucoup de sociétés ayant mis en place ces solutions ont quand même été attaquées, des brèches ont été exploitées car toutes ces solutions ne permettent pas d'arrêter tous les logiciels malveillants persistants qui vont compromettre un réseau en offrant la possibilité de se déplacer librement afin de trouver des données ciblées à voler.

- Là où les entreprises doivent se focaliser (en plus d'autres options internes déjà mentionnées), c'est de déployer une solution de détection des menaces plus intégrée qui peut extraire des informations à partir de plusieurs points dans le réseau, d'analyser ce qui se passe en temps réel (sur les stations de travail et sur le réseau) et défendre activement les réseaux d'entreprise avec la possibilité d'automatiser les réponses défensives générées en temps réel et 24 heures sur 24. Il y a encore à ce jour une réticence au niveau des comités exécutifs des entreprises de reconnaître la nécessité d'avoir un budget propre à la « Cyber Sécurité » mais qui permettrait de continuer à investir sur les dernières générations de solutions qui sont adaptées aux nouvelles menaces. Jusqu'à ce que cela change ; les cyber attaques vont continuer, les hackers utilisant des outils automatisés de pointe. Et nous continuerons de découvrir de nouvelles attaques de grandes ampleurs, quasiment tous les jours !



Réagissez à cet article

Source

<http://www.infodsi.com/articles/157575/protger-mieux-donnees-clients-cyberattaques-bernard-girbal-vice-president-emea-chez-hexis-cyber-solutions.html>

Cyber-terrorisme : un recrutement en 4 phases



Le ministère de la Défense récuse l'avoir organisé en urgence, mais ce colloque tombe à pic. Les 2 et 3 novembre 2015, le nouveau site de Balard, «l'Hexagone», accueille une série de conférences sur le thème «Droit et Opex» (opérations extérieures, la guerre donc), autour de deux thèmes clés : la judiciarisation croissante des conflits et l'adaptation du droit aux nouvelles menaces, aux «zones grises».



A l'instar des bombardements français en Syrie dont la légalité a soulevé de nombreuses questions.

Ces bombardements se sont accompagnés d'actions d'un nouveau genre. Selon Le Monde, «une opération informatique du cybercommandement de l'état-major» a permis de «remonter jusqu'au groupe» visé.

Soit une nouvelle application de la doctrine française en matière de «lutte informatique offensive», dans un cadre légal encore flottant.

Pourquoi la question se pose aujourd'hui ?

«La France dispose de capacités offensives [en matière informatique]», a tonné le ministre de la défense, Jean-Yves Le Drian, fin septembre, lors d'un autre colloque, consacré au «combat numérique».

Le message était clair : la France ne se contente pas de se défendre, elle attaque.

La décision n'est pas nouvelle. Le livre blanc de la Défense de 2008 poussait déjà à l'acquisition de moyens d'attaque, un souhait réitéré cinq ans plus tard à dans le nouveau livre blanc.

En 2013, l'exécutif plaidait ainsi pour «un effort marqué» en matière de cyberdéfense militaire : «Les engagements de coercition seront conduits de façon coordonnée dans les cinq milieux (terre, air, mer, espace extra-atmosphérique et cyberspace).»

Un nouveau champ de bataille est né.

« La guerre de demain devra combiner le cyber avec les autres formes de combat », écrit Le Drian dans le numéro de novembre de la Revue Défense Nationale.

«Pour nos forces armées, le premier enjeu est désormais d'intégrer le combat numérique, de le combiner avec les autres formes de combat.» L'attaque est ainsi devenue une priorité en France, mais pas seulement.

La prise de conscience de 2008 est provoquée par une série d'événements : les cyberattaques contre l'Estonie au printemps 2007 lors d'un différend diplomatique avec Moscou, un scénario similaire un après lors de la guerre entre la Géorgie et la Russie, la découverte en 2010 du virus Stuxnet développé pour saboter certaines installations nucléaires iraniennes...

Les Etats-Unis adaptent rapidement leur doctrine. En 2011, le Pentagone annonce se réserver la possibilité de répondre par des moyens conventionnels à une cyberattaque. Cette année, le Pentagone a revendiqué ouvertement mener des cyberattaques dans la nouvelle mouture de sa «cyber stratégie».

Le droit international peut-il s'appliquer ?

La militarisation croissante du cyberspace a mené à une première vague de travaux visant à encadrer ce nouveau recours à la force. Une réflexion a ainsi été lancée par des experts au sein de l'Otan après les attaques contre l'Estonie, pour aboutir, en 2013, au Manuel de Tallinn. Le texte reconnaît que le droit international s'applique aux conflits dans le cyberspace et le décline en 95 règles.

Une opération cyber est ainsi «une agression armée lorsque l'emploi de la force atteint un seuil élevé en termes de degré, de niveau d'intensité et selon les effets engendrés : pertes en vies humaines, blessures aux personnes ou des dommages aux biens.»

La définition est cruciale, puisqu'elle conditionne l'invocation de la légitime défense, donc le recours licite à la force. D'autres principes sont aussi déclinés à propos des cibles, de l'intensité des attaques...

Existe-t-il un consensus entre les Etats ?

Le Manuel n'est que le fruit d'un travail otanien, non contraignant. Une autre démarche, sous l'égide des Nations Unis, a donné des résultats cet été. Un groupe d'experts gouvernementaux a rédigé un rapport visant à prévenir une escalade en cas d'incident. «Il faut faire ce travail avant qu'un vrai pépin existe. Est-ce que ce sera respecté ? Au moins, ces normes sont là» défend le Quai d'Orsay.

Toutes les parties l'ont endossé, représentants chinois et russes compris, alors que le consensus n'a pas prévalu tout au long des négociations, loin s'en faut.

Elles n'ont abouti que deux minutes avant la fin de la dernière rencontre, le 26 juin 2015, peu avant 18h. Les discussions bloquaient sur l'application concrète du droit international au cyberspace. «Les Chinois ne voulaient pas que le droit international humanitaire s'applique, explique le Quai d'Orsay, leur argument phare était : si on codifie les conflits armés dans le cyberspace, alors on les encourage.»

La légitime défense sera retirée du rapport, «elle n'apparaît que dans une référence très indirecte» précise-t-on au ministère des Affaires Etrangères. Sont reconnus «Les principes d'humanité, de nécessité, de proportionnalité et de discrimination [entre les combattants et les non-combattants].» Les experts gouvernementaux se sont surtout accordés sur des «normes de comportements» : absence d'attaque contre les infrastructures critiques ou les «équipes d'intervention d'urgence», coopération entre Etats pour renforcer la sécurité des systèmes essentiels.

Plus surprenant, les Etats «devraient s'attacher à prévenir l'utilisation de fonctionnalités cachées malveillantes». Un engagement pour le moins surprenant de la part de Washington, également coauteur du rapport, alors que les Etats-Unis se sont fait une spécialité d'introduire des «backdoors», des portes dérobées, dans certains produits... «Toutes les questions relatives à l'espionnage sont exclues du périmètre du travail du groupe» justifie le Quai d'Orsay.

Un deuxième Manuel de Tallinn sera publié en janvier 2016. Il ne devrait pas traiter le domaine conflictuel. Au niveau européen, les discussions se concentrent sur la protection des données personnelles. Un thème remonté dans l'agenda politique après une décision récente de la Cour de justice de l'UE et surtout les révélations d'Edward Snowden sur l'ampleur de la surveillance dans les démocraties.



Réagissez à cet article

Source : http://www.liberation.fr/futurs/2015/11/03/existe-t-il-un-droit-de-la-cyberguerre_1410778

Le nombre d'attaques sur Mac a considérablement augmenté en 2015

| | |
|--|---|
|  <p>Denis JACOPINI</p> <p>8 LE JT</p> <p>DENIS JACOPINI PAR TÉLÉPHONE</p> <p>vous informe</p> | <p>Le nombre d'attaques sur Mac a considérablement augmenté en 2015</p> |
|--|---|

Selon l'étude d'un spécialiste de la sécurité, il y a eu plus d'attaques sur Mac en 2015 que durant ces cinq dernières années cumulées.



Jusqu'à présent, il s'agissait d'un archétype assez clair : les PC étaient plus vulnérables aux attaques que les Mac. Les détenteurs des ordinateurs Apple pouvaient alors se targuer de posséder un objet protégé des virus et autres logiciels malveillants.

Mais, selon une étude de Bit9 + CarbonBlack , spécialiste en sécurité informatique, cette idée est désormais mise à mal : « Jusqu'à présent, on a longtemps cru que les Mac faisaient face à beaucoup moins de risques de cyber-attaques que les PC et, jusqu'à très récemment, ce sentiment était plutôt correct. Les utilisateurs de Mac ont été, la plupart du temps, plus à l'abri que les utilisateurs Windows. Mais le vent est en train de tourner », indique la société qui affirme que le nombre de malwares ayant ciblé le système OS X d'Apple a bondi cette année.

En 2015, il y a même eu plus d'attaques sur OS X que durant les cinq dernières années cumulées.

948 malwares en 2015. Entre 2010 et 2014, l'OS d'Apple a été la cible de 180 logiciels malveillants, Bit9 + CarbonBlack indique qu'il y en a eu près de 948 cette année, soit « l'année la plus prolifique de toute l'histoire de l'OS X d'Apple ».

Si les attaques sont plus nombreuses sur le système Apple, c'est aussi parce qu'il y a de plus en plus de personnes qui ont acheté des Macs ces dernières années. Un revers de médaille en quelque sorte : ces engins sont devenus « mainstream » et se sont fortement implantés dans les entreprises.

Par exemple, le marché des OS sur desktop est certes dominé par Windows, mais Apple s'affiche désormais en 3e place parmi les systèmes les plus utilisés, avec 14,46% de parts de marché en 2015, contre 12,46% en 2014.

Si ces logiciels malveillants sont souvent découverts à temps par les entreprises et les chercheurs, il convient malgré tout aux utilisateurs de vérifier s'ils disposent d'un logiciel antivirus à jour, qu'ils soient des aficionados du PC ou du Mac.



Réagissez à cet article

Source

<http://www.lesechos.fr/tech-medias/hightech/021447295747-le-nombre-dattaques-sur-mac-a-considerablement-augmente-en-2015-1171406.php>

État d'urgence : perquisition dans le cloud et Internet coupé ?

Denis JACOPINI



État d'urgence :
perquisition dans
le cloud et
Internet coupé ?

Le projet de loi qui veut mettre à jour les règles en cas d'état d'urgence prévoit d'une part d'autoriser la saisie de fichiers informatiques stockés à distance pendant les perquisitions, d'autre part d'interdire aux assignés à résidence de communiquer avec certaines personnes, et peut-être même sur internet...



Le projet de loi relatif « à l'état d'urgence et renforçant l'efficacité de ses dispositions » a été mis en ligne sur le site de l'Assemblée nationale.

Débatu le jeudi 19 novembre, il a pour but de modifier la loi n° 55-385 du 3 avril 1955 sur l'état d'urgence en le rendant notamment plus adapté aux nouvelles technologies.

Le premier exemple de ce qu'on peut y lire est d'ailleurs parlant. « Il permet enfin l'accès aux données informatiques accessibles depuis le lieu perquisitionné, ainsi que la prise de copies », indique d'abord le texte avant de préciser plus loin que durant une perquisition il sera possible d'accéder aux données dans un système ou un équipement (ordinateur, smartphone, etc.) « dès lors que ces données sont accessibles à partir du système initial ou disponibles pour le système initial ».

Il semble donc que cela concerne les systèmes de stockage à distance lorsque les enquêteurs sont sur place.

Les forces de l'ordre pourront également copier « sur tout support (...) les données auxquelles il aura été possible d'accéder dans les conditions prévues par le présent article ».

Plus loin, le texte précise que « cette rédaction vise les données informatiques telles que celles qui sont présentes dans un ordinateur, celles qui sont accessibles depuis un ordinateur (« nuage »), celles qui sont contenues dans un téléphone... ».

L'article 2 proroge également la possibilité « d'ordonner des perquisitions de jour et de nuit », lit-on encore.

Assignation à résidence = plus d'internet ?

Ces mesures vont de pair avec une autre information contenue dans le document, mais qui est encore à l'heure actuelle peu précise. Il s'agit de prescrire à une personne assignée à résidence l'interdiction « de se trouver en relation, directement ou indirectement, avec certaines personnes nommément désignées dont il existe des raisons sérieuses de penser que leur comportement constitue une menace pour la sécurité et l'ordre publics ».

L'utilisation des termes « directement ou indirectement » laisse planer un certain doute quant à ce que cela peut signifier concrètement. Elle pourrait se traduire par l'interdiction d'utiliser des appareils de communication comme les téléphones ou même Internet. Mais cette dernière disposition paraît délicate à mettre en œuvre dans la mesure où Internet est devenu un droit fondamental en France, et est entré dans les Droits de l'Homme reconnus par l'ONU.

En revanche, l'état d'urgence permet quant à lui de déroger à certains Droits de l'Homme.



Réagissez à cet article

Source

<http://www.linformaticien.com/actualites/id/38575/etat-d-urgence-perquisition-dans-le-cloud-et-internet-coupe.aspx> :

Comment faire face aux cyber-attaques sur le plan juridique ?



Les cyber-attaques constituent une menace majeure pour les entreprises : elles sont en constante augmentation et touchent toutes les entreprises, de la firme multinationale à la PME. Elles coûtent également de plus en plus cher aux entreprises touchées, sans même parler des conséquences en matière de réputation et d'image, et donc de perte de confiance de la part de leurs clients.

Les entreprises sont encore peu sensibilisées à cette menace et manquent de réactivité. Or des outils d'information existent, en particulier le guide de l'ANSSI (Agence nationale de la sécurité des systèmes d'information) en accès libre qui offre des informations très utiles sur les moyens à mettre en œuvre pour se protéger.

Au-delà de ce volet technique, des choses très pratiques sont à mettre en œuvre sur le plan juridique pour pouvoir, le moment venu, réagir comme il se doit.

Se préparer en amont en mettant en place une procédure de gestion de crise

Tout d'abord, il faut établir et mettre en œuvre les chartes et procédures de gestion de crise qui permettront à chacun dans l'entreprise de savoir quels sont les risques, comment ils peuvent se manifester et quelle est la réponse attendue de leur part le cas échéant. Cette question est d'ordre juridique dans la mesure où la mise en œuvre de ce type de procédure qui impacte l'organisation d'une entreprise nécessite généralement une concertation avec les institutions représentatives du personnel et au minimum une information.

Il faut se rappeler sur ce point qu'en droit, une information essentielle – telle que l'identification d'un complice au sein de l'entreprise – mais qui a été obtenue par la mise en œuvre de moyens de traçage illégaux car tenus secret, ne pourra constituer une preuve valable et sera donc écartée.

Pour éviter ce type de situation absurde, il faut donc préparer l'entreprise en amont. Doter la cellule de crise de compétences juridiques pendant l'attaque. Pendant la cyber-attaque, il faut évaluer et gérer la situation en mettant en œuvre immédiatement une cellule de crise dotée des compétences nécessaires pour réagir avec la rapidité requise. Elle doit intégrer des décisionnaires aptes à évaluer et à gérer la situation sur les plans technique, opérationnel, juridique, et de la communication, et qui doivent disposer des moyens techniques de lutte contre l'attaquant. Il faut également faire le lien avec les moyens institutionnels, en particulier les autorités judiciaires, et les divers organismes internationaux de coopération dans ces matières. Se doter d'une compétence juridique est indispensable pour pouvoir évaluer dans l'instant si les conditions requises pour prendre une décision sont réunies et anticiper les conséquences prévisibles de celle-ci.

L'entreprise qui fait l'objet d'une attaque va faire face à des conséquences potentiellement considérables sur le plan juridique, en particulier sur le terrain de sa responsabilité. Il faut donc avoir la compétence sous la main, au sein de la cellule de crise.

Répondre sur le plan juridique aux conséquences de l'attaque

Enfin, après l'attaque, la réponse se fera en trois temps. Il faut d'abord poursuivre l'enquête. Celle-ci peut être longue et nécessiter une coordination sur le plan international. Il est essentiel, dans ce cas de figure, de suivre l'enquête au plus près sur les différents terrains d'investigation sur lesquels elle se déroule. L'erreur courante consiste, quand l'attaque touche plusieurs pays, à ne déposer plainte que dans un seul pays et attendre que la justice fasse son travail : au contraire, il est recommandé de déposer des plaintes dans chacun des pays concernés.

Ensuite, il faut engager les poursuites nécessaires : cette phase vise à engager la responsabilité de tous ceux qui ont contribué à la réalisation de la cyber-attaque, que ce soit de manière délibérée ou par leur négligence, en interne ou à l'extérieur. On cherchera dans cette étape à récupérer, lorsque cela est possible, par le biais d'actions en responsabilité, une partie de la perte subie par l'entreprise.

Enfin, il faut défendre l'entreprise face à l'ensemble de ceux qui auront subi un préjudice du fait de la cyber-attaque (salariés, actionnaires, cocontractants, clients, institutions, etc.) et qui viendront lui en demander des comptes : c'est la responsabilité de l'entreprise, et de ses dirigeants, qui va être recherchée au motif que la cyber-attaque leur a causé un préjudice propre et que celle-ci aurait pu être évitée par la mise en œuvre de mesures adaptées, propres à la prévenir.

C'est ce qu'on voit couramment aux Etats-Unis avec les class actions. Pour récapituler, il est très clair que les risques relatifs à une cyber-attaque sont considérables pour les entreprises, mais le risque principal pour les entreprises et leurs dirigeants est bien de ne rien faire.



Réagissez à cet article

Source : <http://www.jdt.fr/tribunes/item/154-comment-faire-face-aux-cyber-attaques-sur-le-plan-juridique>

Il sera bientôt possible de détecter le diabète avec un smartphone

| | |
|---|---|
| <p>Denis JACOPINI</p>  <p>VOUS INFORME</p> | <p>Il sera bientôt possible de détecter le diabète avec un smartphone</p> |
|---|---|