Le Medef demande aux patrons de signaler la radicalisation des salariés

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 dinformation 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 ?

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 couteux 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 !

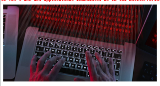
Réagissez à cet article
Source : http://www.infodsi.com/articles/157575/proteger-mieux-donnees-clients-cyberattaques-bernard-girbal-vice-president-emea-chez-hexis-cyber-solutions.html

---

Cyber-terrorisme : un recrutement en 4 phases

Cyber-terrorisme : un recrutement en 4 phases

BLOQUÉS
Ce fut l'une des applications immédiates de la loi antiterroriste de novembre 2014 : plusieurs sites internet accusés « de faire l'apologie du terrorisme » ont été bloqués depuis la mi-mars 2015 par le gouvernement français : plus aucun internaute ne pouvait y avoir accès.



Cette mesure visait à tenter de contrer la radicalisation islamiste express qui se déroule depuis plusieurs mois via Internet, à destination notamment des jeunes dont le nombre de candidats au départ vers la Syrie aurait augmenté de 116% depuis janvier 2014.
Les attentats perpétrés à Paris le 13 novembre tout comme ceux de janvier 2015 l'ont révélé crûment : quelques semaines, voire quelques jours, passés à surfer sur les plateformes et réseaux sociaux comme Youtube ou Facebook ou sur les autres forums d'activistes suffisent à former de petits bataillons d'apprentis djihadistes prêts à adopter les idéaux de groupes terroristes comme Daesh ou encore Jabhat al-Nosra, filiale d'Al Qaida.

Une cyber-propagande en plusieurs actes
Ils sont ainsi des centaines voire des milliers de jeunes, à se faire « hameçonner » dans leur chambre via internet… « Le passage par la mosquée n'est pas une obligation. Certains jeunes partent du jour au lendemain sans avoir jamais eu de réel contact avec l'islam », explique Dounia Bouzar, anthropologue et présidente du CPDSI (Centre de Prévention des Dévives Sectaires liées à l'Islam), en première ligne dans la lutte contre la radicalisation islamique en France.
Dans un rapport de novembre 2014, le CPDSI révèlait déjà que cet endoctrinement concerne à 80 % des familles de référence athée, issues non de milieux défavorisés mais plutôt des classes moyennes et supérieures. Surtout, il touche essentiellement des jeunes, âgés pour la plupart de 15 à 25 ans, dont certains sont partis en Syrie ou projetaient de le faire.
Ce recrutement pour des causes aussi extrêmes est le fruit d'une propagande redoutablement efficace qui se déroule en plusieurs actes.
Cela peut commencer, selon le rapport du CPDSI, par des vidéos découvertes au hasard de recherches sur internet. Y sont développés les thèmes du complot des plus forts contre les plus faibles, de contestation de la société de consommation avec son lot supposé de mensonges et de scandales : complots des firmes pharmaceutiques, scandales sanitaires comme celui de la vache folle, publicités mensongères etc… Une sorte de : « On nous cache tout, on nous dit rien, dans ce monde pourri ! » Et ces vidéos font mouche ! « Les adolescents ne supportent pas l'injustice » indique Bruno Falissard, Directeur de l'unité INSERM U669 (santé mentale de l'adolescent)ALGORITHMES.

Dès lors, l'engrenage est en marche.
Par le jeu d'algorithmes de recommandation – ce procédé technique permettant de filtrer automatiquement un corpus d'informations en fonction des centres d'intérêt d'un internaute – Youtube propose de nouvelles vidéos du même genre à regarder. Celles-ci suggèrent « l'existence de sociétés secrètes qui manipulent l'humanité » souligne le rapport. Pour preuve, de supposés symboles cachés par ces forces maléfiques, un peu partout dans le monde qui nous entoure : ainsi, par exemple, la lecture de la marque Coca Cola dans un miroir révèlerait, avec un peu d'imagination, l'inscription « No Mecque » en arabe.
De clic en clic, l'adolescent glisse vers des contenus évoquant de plus en plus l'islam présenté comme le seul recours contre ce Mal. « Ces vidéos ont pour but de prolonger et parachever la phase d'endoctrinement. C'est là qu'elles commencent par mettre en exergue des images de nature encensant la beauté de la création d'Allah » précise le rapport du CPDSI. Le jeune internaute entre alors de plain pied dans la phase de radicalisation dans laquelle les recruteurs induisent chez lui un questionnement spirituel quasi absent jusque-là.
Avant d'être exposé à une troisième salve de vidéos mêlant cette fois des prêches menaçants « sur les risques d'aller en enfer », « sur les bienfaits de la conversion à l'islam » etc… Des productions qui l'appellent à se « réveiller » et à « agir ».

Les « like » qui trahissent l'utilisateur
Parallèlement, l'endoctrinement se déroule aussi sur le réseau social Facebook. L'adolescent ne tarde pas à s'inscrire dans un groupe ouvert sur le fameux réseau social par les recruteurs pour l'inciter à combattre le prétendu complot. Il tisse ainsi rapidement des liens avec de nouveaux « amis » qui peu à peu évoquent le « djihad global ».
De manière très fine, le discours tenu sur ce réseau par les recruteurs est adapté à chacun selon son profil. « Par exemple, les filles qui indiquent sur leur profil Facebook leur volonté de s'engager pour des causes humanitaire, pour aider ou soigner les autres, sont repérées et abordées sous cet angle altruiste » raconte Dounia Bouzar. Rappelons à cet égard qu'une étude scientifique britannique a récemment révélé qu'il suffisait de quelques « clics » sur le fameux réseau social pour que celui-ci nous connaisse mieux que nos « vrais » amis et nos proches : ainsi, les psychologues de l'université de Cambridge ont montré qu'une centaine de « like » (les mentions « j'aime » par lesquelles un internaute définit les pages qu'il apprécie) suffit à l'algorithme de Facebook pour « cerner » une personnalité !

MATRAQUAGE.
Loin d'être le fait d'amateurs, le processus de recrutement s'apparente à une vraie démarche commerciale. « Semblable à celle que l'on retrouve dans les sectes. Elle s'adresse à tous » indique Serge Blisko, président de la Mission interministérielle de vigilance et de lutte contre les dérives sectaires (Miviludes). Car il ne faut pas oublier la dimension de séduction déployée par les recruteurs qui se donnent l'apparence d'un entourage chaleureux. Une stratégie d'enfermement également. « L'internaute reçoit de nombreux messages de ses nouveaux « amis » sur Facebook, des dizaines de SMS par jour » explique Magalie*, une analyste de la Miviludes qui souhaite garder l'anonymat.
S'ensuit une phase dite de « déconstruction ». « Le but est alors de l'isoler. Les messages utilisent un néolangage, celui des initiés comportant de plus en plus de termes arabes transcrits phonétiquement. La liste des interdits s'allongent : aliments contenant de la gélatine de porc, parfums à base d'alcool etc. » poursuit Magalie. Dès lors, le matraquage des vidéos de propagande sur le web constitue, lui, la phase de reconstruction. « On réécrit l'histoire et les croyances de la personne » précise Magalie.
Vient enfin une dernière étape, celle du renforcement qui consiste à tout faire pour que l'individu n'échappe pas à cette emprise. Il est surveillé par d'autres, imprégné de réponses automatiques à toutes les critiques que l'on peut lui opposer. « On leur fait croire que la conversion à l'islam est un acte irréversible. Ce qui dans leur esprit ferme toutes les portes de sorties et complique sérieusement toute tentative de retour à la normale » précise Magalie.
Début mars 2015, Manuel Valls déclarait à la presse qu'il y avait 3000 européens aujourd'hui en Syrie et en Irak. « Il pourrait y en avoir 5 000 avant l'été et sans doute 10.000 avant la fin de l'année » s'inquiétait alors le Premier ministre. Un phénomène qui profite aussi de la poussée récente d'un autre réseau social : Twitter.
Une étude du Center for Middle East Policy paru en mars indiquait que Daesh disposait de 46000 comptes Twitter plus ou moins actifs. Mais selon les auteurs de cette étude, le succès du groupe terroriste sur les réseaux sociaux est surtout le fait de 500 à 2000 comptes hyperactifs qui twittent de manière intensive. Quant à la suppression de ces comptes pour contrer la propagande djihadiste, les chercheurs estiment que cela pourrait être contre-productif. Selon eux, si elle créé des obstacles à ceux qui veulent rejoindre Daesh, elle tend aussi à les isoler sur le web et pourrait ainsi accroître la vitesse et l'intensité de leur radicalisation. Ce qui n'est pas le but recherché !

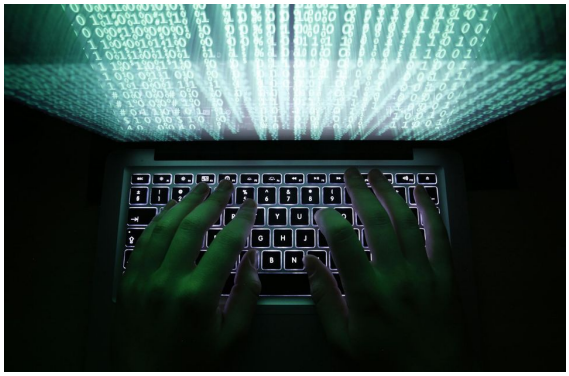
Réagissez à cet article
Source : http://www.sciencesetavenir.fr/high-tech/20150317.OBS4764/cyber-terrorisme-un-recrutement-en-4-phases.html

---

Existe-t-il un droit de la cyberguerre ?

Existe-t-il un droit de la cyberguerre ?

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 cyberespace).»

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 cyberespace 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 cyberespace 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 cyberespace. «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 cyberespace, 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

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

	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

Il sera bientôt possible de détecter le diabète avec un smartphone