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