LE MOT DE LA SEMAINE

Cyber risque

1192

www.lexisnexis.fr

Les enjeux du Cyber risque


Valérie Lafarge Sarkozy, avocat De Gaulle Fleurance et Associés, expert du Club des juristes

Georgie Courtois, avocat De Gaulle Fleurance et Associés

Pas un jour ne passe sans qu'une attaque cyber ne fasse la une de l'actualité Hi-Tech. Ainsi, la société OVH, leader dans l'hébergement sur internet, vient d'annoncer avoir été victime d'une attaque DDOS (attaque en déni de services) visant à rendre ses services inaccessibles. Au même moment, Yahoo! révélait l'attaque, datant de 2014, ayant permis à des hackers d'obtenir des informations concernant 500 millions de comptes d'utilisateurs au sein de ses bases de données.

Alors que des études estiment que le nombre moyen de jours durant lesquels les hackers sont présents sur le réseau de leur cible s'élève à 205 jours, la prise de conscience de ce risque cyber au sein des entreprises, tant qu'elles n'en sont pas victimes, est encore trop faible.

Cette sous-estimation du risque conduit à une absence d'anticipation et à une aggravation du préjudice lorsque l'attaque survient. Europol, l'agence européenne de police, vient d'avertir que le "ransomware", attaque par laquelle un hacker bloque l'accès à un ordinateur ou un ensemble de fichiers en les cryptant et ne les rend à nouveau accessible que contre paiement d'une rançon, est maintenant la première menace en termes de cybercriminalité en Europe. Étant précisé que la question de la légalité et de l'assurabilité de la rançon n'est pas tranchée. Les cyber attaques peuvent également être utilisées pour obtenir des informations détaillées sur les modes de fonctionnement d'entreprises dument identifiées en vue de réaliser ultérieurement et à leur détriment des infractions de droit commun, telle que l'escroquerie au Président maintenant dument identifiée mais toujours d'actualité.

La législation française est pourtant en avance sur ces problématiques de risques en matière de sécurité. La loi informatique et liberté de 1978, qui fait figure d'exemple au niveau européen, impose notamment des obligations de sécurité dans le traitement des données personnelles, tandis que la loi n° 2013 -1168 du 18 décembre 2013 relative à la programmation militaire (LPM) pour les années 2014 à 2019 prescrit des obligations de sécurisation des systèmes d'information des Opérateurs d'Importance Vitale, dont l'indisponibilité risquerait de diminuer d'une façon importante la sécurité ou la capacité de survie de la Nation.

Au niveau européen, le mouvement s'accélère et impose désormais une prise de conscience rapide des enjeux en matière de risque cyber, notamment au regard des sanctions encourues. Ainsi, le règlement général sur la protection de données (RGPD), adoptée en avril 2016 et d'application directe dès mai 2018, imposera aux responsables du traitement de ces données de nouvelle obligations, dont la notification aux autorités nationales (la CNIL en France) des failles de sécurité ayant porté atteintes à des données personnelles, la sanction pouvant atteindre 4 % du chiffre d'affaires mondial de l'entreprise qui ne respectera pas ces obligations. Parallèlement, la directive « Network and Information Security » approuvée le 6 juillet 2016 par le Parlement européen devrait être transposée début 2018 et imposera notamment aux fournisseurs de services numériques tels que les services de Cloud Computing, les moteurs de recherche et les plateformes de e-commerce de prendre des mesures pour assurer la sécurité de leurs infrastructures et pour notifier les incidents majeurs aux autorités nationales, comme l'Agence nationale de la sécurité des systèmes d'information en France.

Devant l'ensemble de ces menaces, la question de l'assurance du risque cyber conduit les assureurs à proposer des produits de plus en plus adaptés tout en s'interrogeant sur les limites d'assurabilité de ce risque aux contours encore assez flou.

En résumé la technicité et la nature protéiforme des atteintes, l'évolution permanente des attaques toujours plus innovantes pesant sur les entreprises et les citoyens, la mise en œuvre de l'harmonisation des législations entre les États européens, la préservation des libertés individuelles, l'assurabilité de ces risques ou encore l'acculturation ne sont qu'une partie des multiples problématiques à résoudre pour prévenir et combattre les cyber risques, trop souvent sous-estimés alors que leurs impacts financiers, opérationnels et réputationnels sont rarement anodins. ■