Le risque cyber dans la digitalisation de l'entreprise

La digitalisation de l'entreprise présente de nombreux avantages : compétitivité, agilité, amélioration des conditions de travail, flexibilité et tant d'autres. Néanmoins, elle expose l'entreprise à plus de vulnérabilités et à un accroissement de sa responsabilité.

Par **Amira Bounedjoum,** *avocate-counsel protection des données, digital & cybersécurité et* **Sophie Nayrolles,** *avocate associée*

La multiplication des canaux de communication et des flux de données dans le cadre de la digitalisation d'une entreprise en font une cible privilégiée des cyberprédateurs.

Une cyberattaque peut avoir des effets désastreux sur une entreprise pouvant aller jusqu'à mettre fin à son activité. La société CLESTRA, fabricant de cloisons du Bas-Rhin, a été placée le 1er août 2022 en redressement judiciaire, notamment du fait d'une cyberattaque en avril qui lui a coûté entre 2 et 3 millions d'euros.

L'anticipation et la préparation de mesures préventives s'avèrent donc essentielles et ce d'autant, qu'être la cible d'une cyberattaque est également de nature à engager la responsabilité de l'entreprise.

En effet si l'on peut se sentir « victime », rappelons que la réglementation française et européenne impose des obligations fortes de sécurité informatique aux entreprises sans distinction de taille ou de chiffre d'affaires.

Le RGPD impose même une obligation de notifier (spontanément et dans un délai de 72 heures) à l'autorité de contrôle, la CNIL, toute violation de données c'est-à-dire tout incident ayant pour effet de compromettre l'intégrité, la disponibilité ou la confidentialité de données personnelles.

Autrement dit, faire l'objet d'une cyberattaque expose l'entreprise non seulement à un risque financier et d'image mais également à un risque juridique puisque si la CNIL constate que le niveau de sécurité n'était pas suffisant, elle peut alors prononcer une sanction.

« Une cyberattaque peut avoir des effets désastreux sur une entreprise. »

La réglementation prévoit des sanctions pouvant atteindre 10 millions d'euros ou 2 % du chiffre d'affaires total de l'entreprise. En pratique, elles sont moins élevées mais dissuasives. À titre d'exemple, MARIOTT s'est vu infligée une amende de 20 millions d'euros en 2020 en raison d'une attaque informatique et la société SLIMPAY (établissement qui propose notamment des solutions de paiement) a écopé d'une amende de 180 000 €. La société DEDALUS BIOLOGIE (éditeur de logiciels) s'est quant à elle vue infliger une amende d'1,5 million d'euros en raison d'une fuite de données en avril 2022.

Face à ce phénomène, la CNIL a orienté en 2021 ses actions de contrôles autour de trois thématiques prioritaires, dont la cybersécurité des sites web.

Dans le cadre de 300 procédures de contrôle que la CNIL a menées, elle a fréquemment remarqué des manquements relatifs à des politiques de mot de passe non conformes, des transmissions de données non chiffré, des données librement accessibles par modification d'URL, l'absence de verrouillage automatique de cession de poste de travail etc...

Afin de se prémunir, il devient ainsi vital d'adopter une stratégie de cybersécurité performante, tant technique que juridique.

SIMON ASSOCIÉS

Cabinet Simon Associés
38 rue Pitot - 34000 Montpellier

contactmontpellier@simonassocies.com