GESTION DES RISQUES

Ce que peut coûter une cyberattaque à l'entreprise

90 % des entreprises françaises auraient été victimes d'une cyberattaque en 2020, avec des dommages parfois importants sur leur activité, leur situation financière ou encore leur réputation. Certaines bonnes pratiques permettent pourtant d'améliorer la résilience contre le risque cyber.

Airbus, Fleury-Michon, Eurofins, Altran… : la liste des entreprises victimes d'une cyberattaque en 2020 n'en finit pas de s'allonger. 90 % des entreprises françaises en auraient fait les frais, selon une étude d'IBM. L'Agence nationale de sécurité des systèmes d'information (ANSSI) recensait au 30 septembre 2020 plus de 1 100 attaques aux rançongiciels, les plus fréquents de ces actes malveillants. Dans la continuité d'une trajectoire initiée en 2019, le nombre d'entreprises, victimes d'une cyberattaque, a été multiplié par quatre en un an. La digitalisation des entreprises et l'essor du cloud computing font exploser la cybercriminalité. Et la crise sanitaire liée à la pandémie de Covid-19 accélère encore le phénomène : entre janvier et avril 2020, les attaques de rançongiciels ont augmenté de 25 %. En multipliant les points d'entrée dans les systèmes informatiques, la généralisation du télétravail, souvent effectuée dans la précipitation, accroît la vulnérabilité des entreprises. « Le développement des objets connectés, de l'intelligence artificielle, de l'informatique quantique, tout comme le déploiement à venir de la 5G, sont des leviers de développement pour les entreprises. Mais ils représentent aussi un facteur de risque supplémentaire. Nous constatons une progression en nombre, en intensité et en préjudice des cyberattaques qui affectent des entreprises de toutes tailles et de tous secteurs », avertit Jean-Philippe Pagès, directeur Industrie & Services chez Bessé, conseil et courtier indépendant en assurance à Nantes.

RISQUE ACCRU DE DÉFAILLANCE

Face à ce risque grandissant, les entreprises françaises apparaissent peu armées. 80 % d'entre elles n'ont pas de plan de remédiation efficace et 86 % n'ont pas souscrit de contrat d'assurance contre le risque cyber, d'après l'enquête Clusif 2020. Les dommages causés par les cyberattaques sont pourtant multiples : interruption d'activité, pertes financières, poursuites juridiques, voire ruptures de contrat, en cas de fuite de données, impact sur l'image et la réputation de l'entreprise… 38 % des entreprises concernées disent ainsi avoir subi une perte de productivité, 33 % des pertes de données clients et 32 % des pertes de données salariés. À terme, les cyberattaques peuvent même mettre en jeu la pérennité de l'entreprise. Selon une étude publiée en novembre 2020 par Bessé, le choc économique provoqué par une cyberattaque est tel qu'il augmente de 80 % le risque de défaillance de l'entreprise dans les trois mois qui suivent. L'augmentation de 55 % du nombre de jours de retard de paiement six mois après tend à corroborer l'impact de ces actes malveillants sur la stabilité économique de l'entreprise. Sa valeur patrimoniale peut également subir une dépréciation de l'ordre de 8 à 10 % après l'annonce d'une cyberattaque. Les chefs d'entreprise prennent peu à peu conscience de la menace. 41 % d'entre eux considèrent le risque cyber comme le premier risque couru par leur entreprise, en raison de la menace critique qu'il fait peser sur la continuité de ses activités et sa réputation, selon le Baromètre des risques Allianz 2019.
Paradoxalement, les stratégies mises en place par les entreprises pour s'en protéger ne sont pas à la hauteur. Trop rares sont encore celles à mettre en place une politique

© DR

© DR

Lutter contre les cyberattaques nécessite la mobilisation de l'ensemble des personnels de l'entreprise.

de cyberrésilience. La cybersécurité est trop souvent vue comme une affaire technique.

ORGANISER LA RÉSILIENCE

Mais dans la majorité des cas, les facteurs humains, culturels et organisationnels sont prépondérants. « Organiser la résilience, c'est se donner les moyens d'affronter la crise et de rebondir le plus rapidement possible », analyse Jean-Philippe Pagès. Cette organisation passe par l'élaboration d'un plan préparant l'entreprise à résister au choc, avant que celui-ci ne se produise. Ce plan doit impliquer l'ensemble des salariés dans l'application des procédures et être porté par la direction pour mobiliser tous les secteurs et strates de l'entreprise. Il suppose d'identifier les risques et de leur apporter une couverture technique, dans l'objectif de préserver la continuité ou de faciliter la reprise de l'activité de l'entreprise. « Il faut impérativement tester la robustesse de ce plan, en simulant une crise, y compris dans sa dimension médiatique, qui peut revêtir une importance, parfois disproportionnée par rapport à la gravité du fait et nuire durablement à l'image de l'entreprise. Bien sûr, il faut circonscrire le malware, réorganiser les systèmes informatiques, etc. Mais, la communication envers toutes les parties prenantes de l'entreprise (salariés, clients, fournisseurs) est tout aussi stratégique. Il ne faut surtout pas être dans le déni ou le mensonge, mais veiller à communiquer pour préserver le capital confiance de l'entreprise et sa réputation », conseille Laurent Porta, associé Vae Solis, spécialisé dans la communication de crise et la prévention des risques. La couverture du risque cyber par l'assurance constitue également un élément de réponse, à intégrer dans une stratégie globale pour contrer une menace qui n'est plus émergente, mais avérée.

Caroline Scribe

> **« Il ne faut surtout pas être dans le déni ou le mensonge, mais veiller à communiquer pour préserver le capital confiance de l'entreprise et sa réputation. »**
>
> **Laurent Porta,** associé Vae Solis

PIERRE BESSÉ, PRÉSIDENT DU COURTIER EN ASSURANCE BESSÉ

« Un risque systémique, sournois et ravageur »

Votre groupe a réalisé trois études en trois ans sur le risque cyber. Pourquoi ?
Depuis plusieurs années, nous investissons fortement sur les enjeux cyber car, selon moi, le risque cyber est stratégique et vital pour les entreprises. Inhérent à la digitalisation, il est aggravé par la généralisation du télétravail. Depuis le début de la crise sanitaire, nous assistons, en effet, à une multiplication des cyberattaques, à l'image de celle qui a paralysé l'activité de l'armateur CMA CGM ou des Mutuelles du Mans pendant plusieurs jours ou encore coûté 50 millions d'euros de dommages au groupe informatique Sopra Steria. Je considère le risque cyber comme plus grave que le Covid-19. Jamais auparavant, nous n'avions été exposés à un tel risque, systémique, sournois et ravageur.

Comment s'en protéger ?
De la même manière que nous n'étions pas prêts à faire face à une pandémie, la grande majorité des entreprises n'est pas armée contre la menace cyber. La résilience est compliquée à organiser. Elle suppose de croire en la réalité d'un risque difficile à appréhender, car multiforme et difficilement quantifiable. Les sinistres se mesurent en termes financiers, techniques, d'image, de dommages causés à des tiers… Ils peuvent dépasser 100 millions d'euros. Pour les entreprises, la question, aujourd'hui, n'est plus de savoir si elles vont être exposées à ce risque, mais quand. Dans cette perspective, il leur appartient de mettre en place un certain nombre de bonnes pratiques. L'assurance constitue un élément de réponse. Mais le défi de la cybersécurité ne pourra être relevé que grâce au développement de dispositifs combinant l'intervention des pouvoirs publics, renforcés par les assureurs privés, qui ne disposent pas des capacités financières pour couvrir, seuls, ce risque.

© GUILLAUME GRASSET