LES CYBERATTAQUES DOUBLENT LE RISQUE DE DÉFAILLANCE POUR LES ENTREPRISES

Source : Les Echos

Le courtier Bessé publie une étude montrant la faible préparation des entreprises françaises aux attaques informatiques. Or la montée du risque s'accélère avec, pour conséquences, des défaillances, des pertes de valorisation et de réputation.

Le télétravail, la porosité des systèmes d'information qui l'accompagne, la 5G, la prolifération des objets connectés, le recours accru à l'intelligence artificielle… autant de failles à la menace cyber, largement sous-évaluée par les entreprises. C'est l'un des constats du cabinet nantais Bessé .

Ce spécialiste du courtage et du conseil en assurances auprès des ETI vient de publier une étude sur l'impact d'une attaque informatique sur la valorisation des entreprises. Il en ressort que, sur le panel observé, le risque de défaillance augmente de 50 % dans les trois mois qui suivent l'annonce de l'incident. Ce risque atteint même 80 % pour les entreprises françaises. Quant à la perte de valorisation des entreprises, « elle peut être estimée de 8 à 10 % après l'annonce », selon l'étude, sans parler du dommage causé à la réputation, « l'actif immatériel le plus précieux dont dispose l'entreprise », note Pierre Bessé, PDG du groupe éponyme.

Quatre-vingts pour cent des entreprises sans plan de réponse

Bessé estime que 76 % des dirigeants d'ETI ont subi au moins une incidence cyber en 2019. Mais la montée du risque s'accélère. Se référant aux données de l'Agence nationale de sécurité des systèmes d'information (Anssi), le cabinet rappelle que le nombre d'attaques de rançongiciels a été multiplié par trois ou quatre en un an, 128 attaques ayant été répertoriées au 30 septembre 2020 contre 54 sur toute l'année 2019.

Une foule d'exemples récents corroborent ce constat. « Ouest-France », Eurofins, Sopra Steria, les Mutuelles du Mans ou l'électronicien Eolane ont récemment déploré des attaques. Ce n'est là sans doute que la partie visible de l'iceberg. Or, selon une étude IBM Ponemon Institute, 80 % des entreprises françaises n'ont pas de plan de réponse aux incidents robustes et, selon le Club de la sécurité de l'information français (Clusif), 86 % d'entre elles n'ont toujours pas souscrit de contrat de cyberassurance. « Jamais un tel péril n'a autant menacé l'économie, il est systémique, diffus et sournois, plus encore que le Covid, soutient Pierre Bessé. Pour les entreprises, la question n'est plus de savoir si elles vont être attaquées mais quand et avec quelle intensité. » Pour l'entrepreneur, la menace est telle qu'elle doit faire l'objet d'une prise en compte amplifiée dans laquelle pouvoirs publics et assureurs joueraient un rôle complémentaire, au même titre que pour les catastrophes climatiques ou les menaces terroristes.

Perte d'image de marque

Les procédures en cas d'agression sont désormais bien identifiées. Guy-Philippe Goldstein, enseignant-chercheur à l'école de guerre économique, rappelle les bonnes pratiques consistant à stopper le logiciel malveillant, isoler le risque , reconstruire le système, notifier l'attaque à la CNIL et, surtout, communiquer auprès des clients, des actionnaires, des salariés pour éviter un effondrement de l'image de marque. « Car le refus d'admettre une attaque n'abuse personne », signale Laurent Porta, du cabinet Vae Solis, spécialiste de la communication de crise et de la prévention des risques.

En amont, il faut prévoir une redondance, s'assurer de la disponibilité d'experts, tester les réponses, modéliser l'éventuel préjudice et « prévoir un transfert du risque résiduel vers l'assureur », préconise naturellement le cabinet Bessé, qui a, parmi ses 460 salariés, une équipe dédiée à la cybermenace. Pour Pierre Bessé, le secteur public dispose d'une longueur d'avance en la matière. Car le cyberrisque peut paralyser des territoires entiers ou des fonctions vitales, comme l'eau, un « cybergeddon » en somme. Les entreprises ont là matière à inspiration.

Emmanuel Guimard