LE FIGARO
Pays : FR
Périodicité : Quotidien
OJD : 305701

Date : Du 10 au 11 juillet 2021
Page de l'article : p.3
Journaliste : INGRID VERGARA

MÉDIAS et TECH

La vague de cyberattaques pose un défi à l'assurance

Bercy souhaite faire émerger d'ici à 2022 une offre à la hauteur des risques économiques.

INGRID VERGARA @Vergara_I

CYBERSÉCURITÉ Une semaine après l'attaque au rançongiciel dont il a été à la fois la victime et l'instrument, l'éditeur de logiciels américain Kaseya peine toujours à redémarrer ses serveurs et à retrouver une activité normale. Tous comme le millier d'entreprises et d'institutions dont les systèmes informatiques ont été infectés par ricochet. L'ampleur de l'attaque n'est toujours pas connue à ce jour, la dernière estimation varie entre 800 et 2 000 victimes, dont de nombreuses petites entreprises.

La France a été peu touchée par cette attaque en particulier. Mais elle sait qu'elle n'est pas à l'abri d'une opération similaire, ni de l'inflation des attaques au rançongiciel. Cette semaine, la direction générale du Trésor a mis en place un groupe de travail réunissant assureurs, chercheurs et experts cyber pour construire d'ici l'an prochain une offre d'assurances cyber *« adaptée aux besoins de l'économie et aux enjeux de résilience »*. Pour Bercy, c'est un des moyens de mieux protéger le tissu économique de ce risque *« en croissance exponentielle »*.

Ce marché peine à se développer. Selon une étude de l'Association pour le management des risques et des assurances de l'entreprise (Amrae), seuls 8 % des ETI et PME françaises ont souscrit une assurance cyber contre 87 % des grandes entreprises. Depuis un an, les assureurs ont aussi durci les conditions d'accès car financièrement ils ne s'y retrouvent pas. *« Le marché de l'assurance a vécu une année 2020 catastrophique. Les assureurs ont eu à payer 260 millions d'euros en risques, contre 130 millions euros reçus en primes »*, résume Christophe Madec, expert cyber chez le courtier Bessé. La conséquence ne s'est pas seulement fait ressentir dans le relèvement significatif du prix des contrats et la hausse des franchises. *« Avec la démesure des attaques, les assureurs limitent la couverture mais imposent désormais en amont des niveaux de sécurité qu'elles n'exigeaient pas jusqu'à présent »*, précise Éric Barbry, avocat associé spécialisé en droit des nouvelles technologies au cabinet Racine. Qualité des sauvegardes, politique de gestion des mots de passe, formation des salariés, etc. Cette nouvelle exigence peut avoir un côté vertueux en sensibilisant davantage certaines entreprises, mais peut aussi en décourager certaines. *« L'ETI doit mettre en place des ressources économiques et humaines trop importantes pour ce qu'elle considère comme un investissement non productif »*, ajoute Christophe Madec. Ce sont pourtant ces entreprises qui auront le plus de difficultés à se relever d'une attaque au rançongiciel.

L'épineuse question de la rançon

Pour les assureurs, le risque est compliqué à appréhender, car il a évolué vite. Le problème vient de ce que les primes n'ont pas de fondements techniques, elles ne reposent pas sur des données. *« Nous avons un vrai sujet de quantification. Que peut vraiment coûter un sinistre cyber ? Nous travaillons avec des clients pour évaluer ce que représentent pour eux, par exemple, quinze jours de perturbations »*, explique Cédric Lenoire, analyste financier chez Bessé.

Un des grands débats dans le secteur concerne aussi le paiement de la rançon, et sa prise en charge par l'assureur. Lors d'une audition au Sénat en avril dernier, l'Anssi et le parquet de Paris avaient reproché aux assureurs d'encourager l'augmentation des attaques par ransomware avec cette pratique. En mai, Axa a suspendu cette option proposée jusque-là. Lorsqu'une entreprise se retrouve totalement à l'arrêt après une attaque, ce paiement peut être vu comme l'unique moyen de s'en sortir. Une solution pourtant risquée à plus d'un titre : selon une étude menée pour la société Cybereason dans 7 pays, dont la France, dans 60 % des cas où la rançon a été payée, l'entreprise a été ciblée par une deuxième attaque. ■

> « Avec la démesure des attaques, les assureurs limitent la couverture mais imposent désormais en amont des niveaux de sécurité qu'elles n'exigeaient pas jusqu'à présent »
>
> ÉRIC BARBRY, AVOCAT ASSOCIÉ AU CABINET RACINE