

Les assureurs cherchent encore la parade face aux cyberattaques

En 2020, les cyberattaques ont explosé. Pour autant, petites et moyennes entreprises sont peu couvertes contre ce risque par les compagnies d'assurance aux politiques de garantie devenues parfois obsolètes dans un monde tout numérique.

Temps de lecture : minute

4 juin 2021

La généralisation du télétravail et l'explosion des usages numériques ont offert un formidable terrain de jeu aux hackers. Les attaques informatiques contre les institutions et les entreprises ont bondi en 2020. Pour y faire face, la France a prévu 1 milliard d'euros pour aider à la création de 20 000 emplois en dans le secteur. Un phénomène qui attire investisseurs et créateurs d'entreprises, à l'image de l'ancien PDG de Qwant, Eric Leandri, avec Altrnativ.

Pourtant, peu d'entreprises sont assurées face à un risque de cyberattaques en constante évolution alors que les conséquences potentiellement gigantesques. En effet, les compagnies d'assurance peinent à trouver la martingale pour couvrir convenablement le risque cyber au moment où les attaques informatiques se multiplient.

Le marché est secoué par l'explosion du volume des données informatiques et l'augmentation des attaques, notamment celles aux rançongiciels, lancées par des pirates qui bloquent les données d'une victime et la somment de payer une rançon pour recouvrer l'usage de ses systèmes. En témoigne la récente mésaventure du groupe brésilien JBS, qui a découvert dimanche que plusieurs serveurs sur lesquels est basé son système informatique en Amérique du Nord et en Australie étaient

visés par des hackers.

En France, le Parquet de Paris a enregistré 397 saisines pour des affaires de rançongiciels en 2020 et voit déjà celles-ci doubler en 2021. *"Dans une économie qui se digitalise à marche forcée, (...) les entreprises et les collectivités publiques n'ont pas pris la mesure du danger alors que les pirates gagnent en expertise"* et s'attaquent à *"toutes les activités"*, relève une étude publiée la semaine passée par l'Association pour le management des risques et des assurances de l'entreprise (Amrae). En France, si la plupart des grandes entreprises ont souscrit une assurance contre les risques cyber, les entreprises de taille intermédiaire (ETI), les PME et les collectivités publiques sont en revanche peu protégées, constate l'étude.

217 millions d'euros d'indemnisations en 2021

Du côté des sinistres, le montant des indemnisations versées par les assureurs a été multiplié par trois en France entre 2019 et 2020, passant de 73 millions d'euros à 217 millions, selon les chiffres de l'Amrae, qui précise toutefois que cette inflation n'est due qu'à quatre sinistres de haute intensité qui ont coûté entre 10 et 40 millions d'euros chacun. Pour les assureurs, *"la définition d'un risque cyber, c'est tout dommage à une donnée causé par une donnée. C'est une vieille garantie qui est depuis longtemps dans nos contrats et qui est liée aux dysfonctionnements informatiques"*, rappelle François Nédey, membre du comité exécutif d'Allianz France.



À lire aussi

Covid-19 : Comment CybelAngel a neutralisé une escroquerie visant un fabricant de vaccins

Mais aujourd'hui "*les données sont partout, les systèmes interconnectés et la criminalité plus organisée (...). On se retrouve face à un phénomène de plus forte amplitude, avec des impacts plus importants, qui peuvent potentiellement toucher tout un secteur, voire tout un pays*" , ajoute-t-il. Le cyber a été longtemps couvert par les assurances standard. La multiplication des menaces contraint toutefois les compagnies à examiner plus en détail leurs couvertures et donc à revoir leurs tarifs à la hausse pour couvrir une plus large variété de risques.

En outre, "*la forte volatilité des sinistres rend le risque difficile à tarifer pour les assureurs, qui réduisent en conséquence leurs garanties*" , souligne l'agence Moody's. Certaines compagnies n'acceptent d'ailleurs de couvrir ces risques qu'à condition que les entreprises appliquent au préalable un certain nombre de mesures de sécurité et de prévention.

Risque encore mal perçu

Difficile toutefois de convaincre certains chefs d'entreprises, tentés de ne voir dans ces mesures que des investissements à fonds perdus et disproportionnés au regard d'une menace encore souvent taboue : l'ampleur, le coût réel et le niveau d'indemnisation de ces sinistres sont rarement rendus publics. Les assureurs eux-mêmes se livrent parfois à *"un jeu trouble"*, a récemment tancé le directeur de l'Agence nationale pour la sécurité des systèmes d'information Guillaume Poupard. Une entreprise peut préférer payer *"plusieurs millions d'euros pour la rançon"*, plutôt que *"plusieurs dizaines de millions d'euros"* de préjudice provoquées par la perte des données, incitant ainsi les pirates à attaquer davantage, a expliqué l'expert. *"Avec un taux de couverture des entreprises et un volume de primes encore trop limités, les assureurs ne parviennent pas à trouver les conditions de la mutualisation indispensable au règlement des sinistres de forte intensité"*, résume l'Amrae.

"Le marché de l'assurance cyber ne se consolidera que si le nombre d'assurés augmente suffisamment (...). Mais l'équation est difficile: comment attirer davantage d'assurés quand les taux de cotisations et le niveau des franchises augmentent alors même que les limites diminuent et que les garanties s'amenuisent?", s'interroge encore l'Amrae.