RISQUE CYBER
L'assurance introuvable

Generali ne couvre plus les rançons en cas de cyberattaque.

ADOBE STOCK

La capacité des assureurs à couvrir le risque de cyberattaques est remise en cause. Un casse-tête pour la profession et les entreprises visées.

PAR MORGANE RÉMY

+ EMAIL *redaction@agefi.fr*

Le 2 février dernier, Generali s'est inscrit dans les pas d'Axa. Les deux assureurs ne couvriront plus les rançons demandées pour déchiffrer des données préalablement encryptées à l'occasion d'une cyberattaque. Chez tous les assureurs, les services juridiques peaufinent leurs clauses d'exclusion pour éviter de s'exposer à un risque systémique. En effet, les applications sont développées par briques de code communes à de nombreux logiciels. Si une brique est vulnérable, comme ce fut le cas avec Log4J en début d'année, des millions de sites internet et d'intranets peuvent être compromis simultanément. « *Cette structuration tue le principe même de mutualisation* », analyse François Nédey, membre du comité exécutif d'Allianz France. Outre ce risque majeur, les primes, estimées grossièrement à 200 millions en France, ne couvrent pas le coût des sinistres en 2021. Les assureurs en sont déjà de leur poche.

Il est loin l'engouement de 2016-2017, quand les compagnies faisaient du risque cyber une piste majeure de développement dans un contexte très concurrentiel.

« *A ce moment-là, nous pouvions négocier des couvertures de 25 millions pour 100.000 euros de prime*, rappelle Timothée Crespe, responsable Aon Tech chez le courtier éponyme en France. *Aujourd'hui, c'est plutôt un coût d'un million pour 10 millions de couverture.* » Et encore faut-il avoir les moyens de se les offrir. « *Pour les assurés, négocier des capacités à quelques millions par ligne, à des coûts très élevés, pose clairement question*, alerte Sandra Magny, responsable des relations marché chez Marsh. *Et cette question est : touchons-nous les limites de l'assurabilité ?* »

Pour autant les assureurs, en repli stratégique, se refusent de quitter totalement le terrain. Allianz France se positionne par exemple sur le cyber mais de manière très mesurée. « *Cela pèse faiblement dans notre portefeuille client*, reconnaît François Nédey. *De l'ordre de 1 %. Pour autant, nous travaillons tout de même sur ces assurances, qui sont utiles à nos clients.* » Ce témoignage est très représentatif de la place. Les assureurs ne souhaitent pas complètement sortir du jeu. Pour rester présents et se protéger, les prix flambent. Les majorations des primes vont de 50 % à 200 %. Enfin, les capacités, c'est-à-dire la somme maximale remboursée en cas de sinistre, ont encore été divisées par deux en 2022, après une réduction similaire en 2021. « *Chez HDI, nous ne sommes pas différents des autres acteurs du marché ; nous réduisons la capacité du fait de l'augmentation constante du risque et des cyberattaques, et de l'insuffisance des primes du marché pour y faire face*, témoigne Frédérique Voreux, directrice commerciale & souscription ETI - RC & dommage pour l'assureur du groupe Talanx, spécialisé dans les risques d'entreprises. *Nous réduisons la voilure pour limiter notre exposition mais ce n'est pas pour autant que nous arrêtons la branche ! Et pour cela, nous supportons nous-même une grande partie de rétention car le coût de la réassurance est décourageant.* »

MÉCANIQUE GRIPPÉE

Les réassureurs, pour leur part, proposent désormais des programmes spécifiques au cyber avec, eux-mêmes, des capacités limitées. « *Jusqu'à il y a trois ou quatre ans, le cyber pouvait passer dans les polices des dommages classiques des réassureurs*, explique Christophe Gaudron, directeur général de Guy Carpenter, société de réassurance du groupe Marsh. *Désormais, les sinistres cyber font l'objet d'exclusion dans ces lignes généralistes et les programmes spécifiques sont plus coûteux pour les assureurs.* » Pour ces acteurs, qui récupèrent le risque de nombreux assureurs, l'aspect systémique inquiète particulièrement. « *Des attaques peuvent toucher des millions d'entreprises en même temps, comme avec Petya Not Petya ou Wanna Cry*, poursuit Christophe Gaudron. *Cela peut compromettre la solvabilité même d'un assureur et d'un réassureur si les précautions ne sont pas à la hauteur de l'enjeu !* » Une situation qui rappelle celle des pertes d'exploitation en temps de pandémie.

PAS DE BOUÉE DE SAUVETAGE PUBLIQUE

Bercy, conscient de l'enjeu de l'assurance contre le risque de cyberattaques, avait lancé une consultation sur le sujet en septembre 2021. Ses résultats se font encore attendre… sans trop d'espoir du côté des acteurs de la place, qui évoquent déjà un coup d'épée dans l'eau. Le principe d'une prise en charge par l'Etat du risque systémique, avec une faille touchant un ensemble de logiciels par exemple, est actuellement discuté. *« Nous pourrions imaginer, pour faire face à un sinistre systémique aux conséquences catastrophiques, une collecte obligatoire et universelle d'une portion de la prime sur les assurances de dommages et de responsabilité, comme cela se pratique pour les catastrophes naturelles sur les assurances habitation,* explique Mickaël Robart, directeur du département risques financiers et responsable des solutions de cyber assurance chez chez Diot-Siaci. *Après tout, si une attaque touche notre système d'eau potable par exemple, tous les citoyens sont concernés.* » Beaucoup de professionnels restent pour l'heure sceptiques. « *A ce stade, les propositions de partenariat public-privé ne sont pas viables* », tranche François Nédey,membre du comité exécutif d'Allianz France. *« Il n'y a pas de solution à espérer de ce côté-là »*, abonde Timothée Crespe, responsable Aon Tech chezAon.

ADOBE STOCK

« NOUS NE SAVONS PAS CE QUI SE PASSE EN RESPONSABILITÉ CIVILE SI UNE ENTREPRISE, PAR ERREUR, FAVORISE UNE INTRUSION DE PIRATES CHEZ UN TIERS »

—FRANÇOIS NÉDEY, membre du comité exécutif d'Allianz France

A cela s'ajoute l'incertitude et la difficulté à modéliser le risque, en constante mutation, les pirates et leur « modèle économique » étant très évolutifs. « *Nous manquons également de recul en jurisprudence*, ajoute François Nédey. *Nous ne savons pas ce qui se passe en responsabilité civile si une entreprise ou même un particulier, par une mauvaise hygiène cyber ou une erreur de sa part, favorise une intrusion de pirates chez un tiers.* » Si un fournisseur est compromis et favorise une attaque par rebond, pourra-t-il être tenu responsable ? Et son assureur, obligé de payer les dégâts ? A ce jour, impossible de le savoir. Philippe Klein, directeur de la souscription et du développement chez HDI, résume bien la situation : « *Nous avons un recul très sensible sur notre rentabilité, l'intensité du risque cyber s'accroît fortement et l'inadéquation des taux ne nous offre plus de marges suffisantes sur les placements de nos primes… tout cela grippe la mécanique.* »

UNE COUVERTURE EN PATCHWORK

Du côté des assurés, cela se ressent. La première gageure est de trouver l'assureur qui acceptera d'aller en première ligne, c'est-à-dire d'être le payeur exposé en cas de sinistre. Seules deux compagnies acceptent de jouer franchement ce rôle : AIG et Chubb. Et dans une moindre mesure Beazley. Le plus souvent en deuxième ou troisième ligne arrivent Axa XL, Zurich, Allianz, HDI Global... Les entreprises exemplaires en termes d'hygiène cyber auront peut-être une chance

Les assureurs imposent leurs normes

d'être couvertes, avec une technique digne du patchwork, en y mettant le prix et en assemblant différentes assurances… y compris en interne. « *Pour les entreprises, il s'agit d'une marche forcée pour arriver à une plus forte maturité de leur cybersécurité*, explique Mickaël Robart, directeur du département risques financiers et responsable des solutions de cyber assurance chez le courtier Diot-Siaci. *Ce qui a mis vingt ans en dommages, avec la généralisation des extincteurs automatiques à eau pour lutter contre les incendies, doit se faire désormais en deux ou trois ans dans le cyber !* » En clair, les assureurs imposent leurs normes et sauront le rappeler en cas de sinistre. « *Ils n'hésiteront pas à invoquer tout défaut de mise en œuvre des contrôles de cybersécurité préconisés pour refuser l'indemnisation d'un incident ou résilier le contrat* », annonce William Culbert, directeur Emea Sud de BeyondTrust, solution de sécurité informatique.

CAPTIVES

Nécessité faisant loi, les entreprises ont très sensiblement amélioré leur cybersécurité. Certaines ont même développé leur propre programme d'assurance. « *La captive permet vraiment de mobiliser simultanément les ressources financières et les données nécessaires au pilotage des risques*, souligne Brigitte Bouquot, vice-présidente de l'Association pour le management des risques et des assurances de l'entreprise (Amrae). *Elle est le vecteur d'un véritable changement de culture en gestion du risque car la direction de l'entreprise y siège.* »

Mais aussi innovantes et efficaces soient-elles, les captives ne constituent pas l'ensemble de la solution (*lire 'La parole à'*). Les entreprises ne pourront pas assumer seules le risque. « *L'assurance constitue un prérequis pour certaines activités comme l'aérospatial ou l'aérien et pour traiter avec des acteurs anglo-saxons*, rappelle Brigitte Bouquot. *Si le secteur ne trouve pas de solution, cela constituera un frein à notre compétitivité.* » Sans compter que les petites entreprises ne peuvent pas se permettre autre chose que de simples provisions… qui pourront paraître bien maigres en cas d'attaque très structurée. « *Or les PME, plus vulnérables aux cyberattaques, sont souvent une porte d'entrée donnant sur les plus grands groupes, y compris les opérateurs d'importance vitale pour l'économie et la France* », conclut-elle.

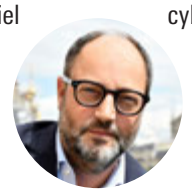
LE COÛT MÉDIAN DIRECT D'UNE CYBERATTAQUE OSCILLAIT ENTRE **7.000** ET **22.000** EUROS SELON LA TAILLE DE L'ENTREPRISE EN 2020, D'APRÈS LE RAPPORT ANNUEL D'HISCOX SUR LES CYBER RISQUES EN EUROPE (MAI 2021).

EN FRANCE, **19 %** DES SOCIÉTÉS CIBLÉES ONT VERSÉ UNE RANÇON.

LA PAROLE À… **OLIVIER WILD,** directeur des risques et des assurances de Veolia et président de l'Amrae*

« *Les polices cyber sont à la fois hors de prix et vidées de leur substance* »

Sentez-vous un retrait des assureurs dans le domaine du cyber ?
Clairement, oui ! Le marché assurantiel est cyclique. Pendant dix à quinze ans, il a été très compétitif. Cela se sentait sur le cyber, avec des assureurs proactifs et innovants. Puis il y a eu un changement brutal en deux ou trois ans seulement. Les assureurs tentent de morceler leurs risques. Ils y vont avec des capacités de 10 à 12 millions d'euros alors que les grands groupes pouvaient obtenir entre 100 et 150 millions auparavant. De plus en plus d'assureurs refusent même d'y aller en première ligne. Les polices cyber sont désormais à la fois hors de prix et vidées de leur substance. A cela s'ajoute un dialogue complexe entre entreprises et assureurs !


CHARLES DE TOIRAC

Que voulez-vous dire par là ?
Globalement et particulièrement en cyber, les dernières campagnes de renouvellement ont été très tendues. Pourtant, les grandes entreprises ont traité ce risque très sérieusement. Au sein de l'Amrae, nous constatons qu'il y a une progression fulgurante en la matière et que les dirigeants, très impliqués sur la question du cyber, ont envie d'échanger sur ce qui a été développé dans le cadre de la gestion du risque. Or les équipes de souscription manquent cruellement d'experts capables de comprendre ce que nous avons mis en place. Et elles sont souvent localisées dans des pays anglo-saxons, qui peinent à comprendre nos spécificités européennes.

L'une des solutions est l'auto-assurance, donc la création d'une captive. Est-ce vraiment la panacée ?
Les *risk managers* de grands groupes, dont je fais partie, ont déjà beaucoup innové avec des captives d'assurance. C'est notre façon de prendre notre part de risques et de le gérer au mieux, en mobilisant l'ensemble de l'entreprise autour de ce projet d'auto-assurance. Mais la gestion du risque est évidemment une chaîne de valeur : prévention, partage mais aussi externalisation de ce risque. C'est avec cet ensemble de solutions que nous serons résilients face à une menace d'une telle ampleur ! Nous avons encore besoin des assureurs. Et nous souhaitons rétablir le dialogue au plus vite.

*Association pour le management des risques et des assurances de l'entreprise.