ALLIANZ GLOBAL CORPORATE & SPECIALTY

Communiqué de presse : Les attaques par rançongiciel restent le premier risque cyber, mais de nouvelles menaces font leur apparition

- **Rapport d'Allianz Global Corporate & Specialty sur les risques cyber : l'augmentation du coût des attaques par rançongiciel touche les entreprises de toutes tailles.**
- **La sophistication et la fréquence des cas de compromission d'e-mails sont également en hausse.**
- **Les tendances émergentes en matière de risques portent sur les attaques financées par les États, le paysage de la responsabilité civile, la pénurie de professionnels de la cyber-sécurité et l'analyse de la cyber-gouvernance selon les critères ESG.**
- **Une meilleure connaissance des risques cyber contribue à la création d'un marché durable de l'assurance cyber.**

Munich, le 26 octobre 2022. Les attaques par rançongiciel restent le premier risque cyber pour les entreprises dans le monde. Toutefois, les incidents liés à la compromission de la messagerie d'entreprise sont en hausse et continueront d'augmenter, à l'ère du *deep fake*. Parallèlement, la guerre en Ukraine et la montée des tensions politiques constituent une préoccupation majeure. Selon un nouveau rapport d'Allianz Global Corporate & Specialty (AGCS), le conflit pourrait s'étendre au cyberespace et être à l'origine d'attaques ciblées contre des entreprises, des infrastructures ou des chaînes d'approvisionnement.

Le rapport annuel d'AGCS sur le panorama des risques cyber met également en évidence les nouvelles menaces soulevées par la dépendance croissante aux services cloud, l'évolution du paysage de la responsabilité civile, avec une hausse des indemnités et des pénalités, ainsi que l'impact de la pénurie de professionnels de la cyber-sécurité. Compte tenu de ces vulnérabilités potentielles, la cyber-résilience des entreprises est aujourd'hui analysée par un nombre inédit d'acteurs, y compris par les investisseurs internationaux. Selon le rapport, elle constitue dorénavant la première préoccupation au regard des critères environnementaux, sociaux et de gouvernance (ESG) de nombreuses entreprises.

« Face au panorama des risques cyber, mieux vaut ne pas se reposer sur ses lauriers. Les attaques par rançongiciel et les campagnes de phishing n'ont jamais été aussi fréquentes. Et à cela s'ajoute la perspective d'une guerre hybride, souligne **Scott Sayce, directeur mondial cyber chez AGCS et directeur mondial du Centre de compétences cyber**. La plupart des entreprises ne pourront échapper à une cyber-menace. Cependant, il est clair que les organisations ayant une bonne maturité cyber sont mieux armées pour faire face aux incidents. Même lorsqu'elles sont atteintes, leurs pertes sont généralement moins importantes, grâce à leurs dispositifs de détection et d'intervention éprouvés.

Malgré d'importantes avancées constatées, l'expérience montre que de nombreuses entreprises doivent encore renforcer leurs contrôles, notamment en ce qui concerne les formations à la sécurité informatique, la segmentation des réseaux dans les environnements critiques, les plans d'intervention d'urgence en cas d'incident cyber et la gouvernance de la sécurité. En tant qu'assureurs cyber, nous souhaitons aller au-delà du simple transfert de risques, en permettant à nos clients de s'adapter à l'évolution du panorama des risques et en relevant leurs niveaux de protection. »

Dans le monde, la fréquence des attaques par rançongiciel reste élevée, de même que les coûts des sinistres. Un record de 623 millions d'attaques a été enregistré en 2021, soit deux fois plus qu'en 2020. Bien que la fréquence à l'échelle mondiale ait baissé de 23 % au premier semestre 2022, le coût total dépasse à ce jour celui de toute l'année 2017, 2018 ou 2019, période pendant laquelle l'Europe avait connu une multiplication de ces incidents. On estime que les attaques par rançongiciel causeront 30 milliards de dollars de pertes aux entreprises d'ici 2023. Selon le rapport, le montant des sinistres de ce type déclarés à AGCS et aux autres assureurs représente largement plus de la moitié du montant des sinistres cyber survenus en 2020 et 2021.

Les doubles et triples extorsions sont aujourd'hui la norme

« Le coût des attaques par rançongiciel a augmenté, les délinquants ciblant des entreprises plus importantes, des infrastructures essentielles et des chaînes d'approvisionnement. Les pirates informatiques ont adapté leurs tactiques pour extorquer plus d'argent, indique Scott Sayce. Les doubles et triples extorsions sont devenues la norme : outre le chiffrement des systèmes, le vol de données sensibles est de plus en plus souvent utilisé comme levier pour exiger une rançon aux partenaires commerciaux, aux fournisseurs ou aux clients de l'entreprise visée. » Compte tenu de leur gravité, ces attaques devraient rester un risque majeur, alimenté par la sophistication croissante des gangs et la hausse de l'inflation, qui se traduit par l'augmentation des coûts liés aux spécialistes de la sécurité informatique et de la cyber-défense.

Les petites et moyennes entreprises, qui ne disposent pas souvent des contrôles et des moyens pour investir dans la cyber-sécurité, sont de plus en plus ciblées par les pirates, alors que les grandes entreprises investissent davantage dans leur sécurité. Les gangs utilisent également un large éventail de techniques de harcèlement, adaptent leurs demandes de rançon à leurs victimes et utilisent des experts en négociation pour maximiser leurs rendements.

Les escroqueries sont de plus en plus sophistiquées

Les attaques par compromission de la messagerie d'entreprise continuent d'augmenter. Elles profitent de la croissance du numérique, de la disponibilité des données, de la transition vers le distanciel, du développement de la visioconférence et des technologies d'hypertrucage (*deep fake*). Selon le FBI, elles ont rapporté 43 milliards de dollars dans le monde entre 2016 et 2021, avec une hausse de 65 % entre juillet 2019 et décembre 2021. De plus en plus sophistiquées et ciblées, elles sont aujourd'hui utilisées par les délinquants sur les plateformes de réunion virtuelle pour induire les salariés à transférer des fonds ou à partager des informations sensibles. Elles sont aussi de plus en plus souvent facilitées par l'intelligence artificielle, qui permet de reproduire la voix ou l'image d'un dirigeant d'entreprise. L'année dernière, un employé de banque des Émirats arabes unis a effectué un virement de 35 millions de dollars, après avoir été trompé par la voix clonée de son responsable.

La menace d'une cyber-guerre

La guerre en Ukraine et les tensions géopolitiques constituent un facteur majeur, qui bouleverse le panorama des risques cyber. Elles augmentent le risque d'espionnage, de sabotage et de destruction sur les entreprises liées à la Russie ou à l'Ukraine, ainsi qu'aux pays alliés et voisins. Les cyber-attaques financées par les États pourraient cibler des infrastructures essentielles, des chaînes d'approvisionnement ou de grandes sociétés. « Pour l'instant, la guerre entre la Russie et l'Ukraine n'a pas entraîné une augmentation significative des demandes d'indemnisation au titre de l'assurance cyber, mais elle laisse entrevoir une hausse du risque lié aux États », signale Scott Sayce. Bien que les actes de guerre soient généralement exclus des produits d'assurance classiques, le risque d'une guerre hybride a encouragé le marché de l'assurance à intensifier ses travaux pour intégrer la question de la guerre et des cyber-attaques financées par les États dans les conditions d'assurance et fournir des garanties claires aux assurés.

Dans le rapport intitulé ***Cyber: The changing threat landscape***, les experts d'AGCS abordent également les tendances suivantes :

- **Vulnérabilité des chaînes d'approvisionnement :** les attaques contre les chaînes d'approvisionnement, qu'il s'agisse d'infrastructures essentielles, comme le réseau d'oléoducs Colonial Pipeline, ou de services cloud, représentent aujourd'hui un risque important. Les groupes de pirates informatiques utilisent de plus en plus la menace de perturbations graves pour faire pression sur les entreprises, notamment celles du secteur manufacturier, plus vulnérables.
- **Externalisation et cloud computing :** les entreprises continuent de transférer leurs services et le stockage de leurs données dans le cloud, malgré les préoccupations croissantes concernant la sécurité et le cumul des risques. La dépendance à un petit nombre de fournisseurs de services cloud ou de cyber-sécurité crée de grandes concentrations de risques autour de quelques points de défaillance. Et il est souvent faux de croire que le prestataire de services d'externalisation ou de cloud assumera l'entière responsabilité en cas d'incident.
- **Assurance responsabilité civile :** couvrant les amendes et les pénalités, elle devient de plus en plus nécessaire, compte tenu des avancées technologiques, du nombre croissant d'informations recueillies par les entreprises et du

durcissement de la réglementation sur la confidentialité des données. Presque tous les incidents cyber, y compris les attaques par rançongiciel à double extorsion, peuvent donner lieu à des litiges et à des réclamations de dommages et intérêts par les parties concernées.

- **Pénurie de professionnels :** elle entrave les efforts visant à renforcer la cyber-sécurité. Malgré la sensibilisation des conseils d'administration, le nombre de postes vacants en cyber-sécurité a augmenté de 350 % dans le monde au cours des huit dernières années, pour atteindre 3,5 millions selon les estimations. Cela signifie que de nombreuses entreprises ont des difficultés pour embaucher, ce qui réduit leur capacité à améliorer leur cyber-sécurité.
- **Cyber-sécurité et respect des critères ESG.** Aujourd'hui, la cyber-résilience des entreprises est examinée par un nombre beaucoup plus important de parties prenantes que dans le passé. Les questions de cyber-sécurité sont de plus en plus souvent intégrées dans les cadres d'analyse des risques ESG, qui étudient les pratiques des fournisseurs de données pour évaluer leur niveau de préparation à la cyber-criminalité. Il n'a jamais été aussi important de vérifier que les procédures et les mesures de cyber-sécurité sont prises en compte par le conseil d'administration et que les dispositifs de surveillance des risques sont mis en place.

Face à un environnement de risques plus complexe et à une augmentation des sinistres cyber, le secteur de l'assurance a adopté un processus de souscription plus rigoureux, afin de mieux évaluer les profils de risque cyber de ses clients et d'encourager les entreprises à améliorer leur sécurité et leurs contrôles de gestion des risques.

« La bonne nouvelle, c'est que nous assistons à des discussions sur la qualité du risque cyber très différentes par rapport aux années précédentes, note Scott Sayce. Nous obtenons des renseignements plus précis et nous apprécions que les clients fassent un effort supplémentaire pour nous fournir des données exhaustives. Cela nous permet aussi de leur apporter une plus grande valeur ajoutée et de leur offrir des informations et des conseils utiles. Nous leur indiquons, par exemple, quels contrôles sont les plus efficaces ou comment améliorer leur gestion des risques et leurs mesures d'intervention. Ainsi, pour nos clients, les événements cyber devraient être plus rares ou moins importants. De notre côté, les déclarations de sinistres devraient moins nombreuses. Cette collaboration contribuera également à créer un marché durable de l'assurance cyber, offrant non seulement des couvertures classiques, mais intégrant aussi les risques cyber dans les programmes des captives et autres types de transfert alternatif des risques. »

Contact presse :
Florence Claret / Tel : 01 58 85 88 63 / florence.claret@allianz.com

À propos d'Allianz Global Corporate & Specialty

Allianz Global Corporate & Specialty (AGCS) est un leader mondial en assurance des grands risques industriels et l'une des principales entités du groupe Allianz. AGCS fournit aide à la gestion des risques, solutions d'assurance des dommages et transfert alternatif des risques pour un large éventail de risques commerciaux, industriels et spéciaux avec dix branches dédiées.

Nos clients sont aussi divers que les activités économiques, allant des sociétés du classement Fortune Global 500 aux petites entreprises et aux particuliers. Parmi eux figurent non seulement les plus grandes enseignes du monde, des institutions financières, des entreprises technologiques, des compagnies aériennes et maritimes internationales, mais aussi des parcs éoliens flottants ou des sociétés de production hollywoodiennes. Tous se sont tournés vers AGCS pour obtenir des solutions intelligentes face aux risques les plus importants et les plus complexes, dans un environnement dynamique et international. Ils font confiance à un groupe d'assurance fort d'une longue expérience en matière d'indemnisation. AGCS travaille en permanence à construire les meilleures solutions pour ses clients grâce à son équipe mondiale comptant quelque 4 250 collaborateurs de plus de 83 nationalités dans 31 pays. Elle est l'une des plus importantes entités d'assurance des dommages du groupe Allianz, elle bénéficie de notations financières élevées et stables, ainsi que d'un réseau actif dans plus de 200 pays et territoires. En 2021, AGCS a enregistré un volume mondial de primes brutes de 9,5 milliards d'€. Pour en savoir plus, rendez-vous sur www.agcs.allianz.com ou suivez-nous sur Twitter @AGCS_Insurance et LinkedIn.

Mise en garde concernant les déclarations prospectives

Le présent document contient des déclarations prospectives, telles que des prévisions ou des anticipations, qui sont fondées sur les opinions et les hypothèses actuelles de la direction, et qui sont soumises à des incertitudes et à des risques connus et inconnus. Les résultats, les performances ou les événements réels peuvent différer sensiblement de ceux qui y sont évoqués, implicitement ou explicitement. Des écarts peuvent survenir en raison d'une évolution de certains facteurs, notamment des suivants : (i) la situation économique et concurrentielle générale dans les principaux métiers et marchés d'Allianz ; (ii) le comportement des marchés financiers (en particulier, la volatilité, la liquidité et les événements de crédit) ; (iii) une publicité négative, des mesures réglementaires ou des litiges concernant le groupe Allianz, d'autres entreprises connues ou le secteur des services financiers en général ; (iv) la fréquence et la gravité des sinistres assurés, y compris ceux résultant de catastrophes naturelles, et l'évolution des charges des sinistres ; (v) les niveaux et les tendances de mortalité et de comorbidité ; (vi) les taux de conservation ; (vii) l'ampleur des défaillances de crédit ; (viii) les taux d'intérêt ; (ix) les taux de change, en particulier le taux de change EUR/USD ; (x) l'évolution des lois et règlements, y compris en matière fiscale ; (xi) l'impact des acquisitions, compte tenu des questions

d'intégration et des mesures de réorganisation associées ; et (xii) les conditions générales de concurrence qui s'appliquent, dans chaque cas, au niveau local, régional, national et/ou international. Nombre de ces évolutions peuvent être accentuées en cas d'activités terroristes.

Absence d'obligation de mise à jour

Allianz n'assume aucune obligation de mise à jour des informations ou des déclarations prospectives contenues dans les présentes, à l'exception des informations que nous sommes légalement tenus de publier.

Note sur la confidentialité

Allianz SE est soucieuse de la protection de vos données personnelles. Pour en savoir plus, consultez notre déclaration sur la confidentialité.

Mentions légales

Pour plus d'informations sur l'entreprise, cliquez ici.