Les entreprises doivent se préparer à une nouvelle génération de cyber-risques | Le Net Expert Informatique

ALes entreprises doivent se préparer à une nouvelle génération de cyber-risques

Les entreprises doivent se préparer à une nouvelle génération de cyber-risques qui progressent rapidement, passant de menaces avérées de violations de données, problèmes de confidentialité et atteintes à la réputation, à l'interruption d'activité et même à des pertes potentielles catastrophiques, en passant par des dommages opérationnels.

Dans un nouveau rapport — A Guide to Cyber Risk : Managing The Impact of Increasing Interconnectivity —, l'assureur spécialisé Allianz Global Corporate & Specialty (AGCS) observe les dernières tendances en matière de cyber-risques et les dangers émergents au niveau mondial. Le cyber-risque est l'une des principales menaces auxquelles font face les entreprises et connaît une croissance rapide. La cybercriminalité à elle seule coûte approximativement 445 milliards de $ par an à l'économie mondiale et les 10 plus grandes économies représentent plus de la moitié de ce montant (3 milliards de $ pour la France).
« Il y a à peine 15 ans, les cyber-attaques étaient assez rudimentaires et généralement l'œuvre de hacktivistes, mais avec l'accroissement de l'interconnectivité, de la mondialisation et de la commercialisation de la cybercriminalité, la fréquence et la gravité des cyber-attaques ont pris une ampleur considérable », déclare Chris Fischer Hirs, PDG d'AGCS. « La cyber-assurance ne remplace pas une sécurité informatique solide, mais elle crée une seconde ligne de défense qui limite les incidents. AGCS observe une augmentation de la demande pour ces services, et nous nous engageons à collaborer avec nos clients afin de mieux comprendre l'exposition croissante aux cyber-risques et d'y faire face. »

Des réglementations plus strictes et de nouveaux cyber-dangers

Une prise de conscience croissante des expositions aux cyber-risques ainsi qu'une adaptation de la réglementation vont propulser la croissance future de la cyber-assurance. Avec moins de 10 % des entreprises qui achètent actuellement des cyber-polices spécifiques, AGCS prévoit une augmentation des primes de cyber-assurance à l'échelle mondiale de 2 milliards de $ par an aujourd'hui à plus de 20 milliards de $ au cours de la prochaine décennie, soit un taux de croissance annuel de plus de 20 %.
« Aux États-Unis, la croissance a déjà commencé, portée par des règles relatives à la protection des données qui attirent l'attention sur le problème. Dans le reste du monde, de nouvelles dispositions législatives et des niveaux de responsabilité plus élevés seront des moteurs de croissance », affirme Nigel Pearson, responsable mondial de la cyber-assurance chez AGCS. « La tendance générale tend à opter pour une protection des données plus strictes et elle est soutenue par la menace d'amendes importantes en cas d'infraction. » Hong Kong, Singapour et l'Australie, par exemple, travaillent sur de nouvelles lois ou en appliquent déjà. Même si l'Union européenne ne parvient pas à se mettre d'accord sur ses règles paneuropéennes de protection des données, on peut s'attendre à des directives plus strictes à l'échelle de chaque pays.
Auparavant, l'attention se focalisait largement sur la menace de violation de données d'entreprise et d'atteinte à la vie privée, mais la nouvelle génération de cyber-risques est plus complexe : les menaces futures porteront sur le vol de propriété intellectuelle, la cyber-extorsion et l'impact de l'interruption d'activité après une cyber-attaque, ou sur une défaillance opérationnelle ou technique — un risque qui est souvent sous-estimé. « La prise de conscience des risques d'interruption d'activité et de l'assurance relative aux cyber-risques et à la technologie ne cesse de croître. Dans les cinq à dix prochaines années, l'interruption d'activité sera perçue comme un risque majeur et un élément principal du paysage des cyber-assurances », déclare Georgi Pachov, expert cyber dans l'équipe de souscription mondiale Dommages aux Biens d'AGCS. Dans le contexte des cyber-risques et des risques informatiques, la couverture interruption d'activité peut être très étendue, incluant les systèmes informatiques d'entreprise, mais aussi les systèmes de contrôle industriel (SCI) utilisés par des entreprises du secteur de l'énergie, ou encore les robots utilisés dans la production.

La connectivité engendre le risque

L'interconnectivité accrue des appareils que nous utilisons au quotidien et la dépendance croissante à la technologie et aux données en temps réel au niveau personnel comme à l'échelle de l'entreprise, connue sous le nom d'« Internet des objets », créent d'autres vulnérabilités. Certaines estimations suggèrent qu'un billion d'appareils pourraient être connectés d'ici 2020 et 50 milliards de machines pourraient échanger des données quotidiennement. Les SCI sont un autre sujet de préoccupation étant donné que nombre de ces systèmes qui sont toujours utilisés aujourd'hui ont été conçus avant que la cyber-sécurité devienne un problème prioritaire. Une attaque contre un SCI pourrait donner lieu à des dommages matériels comme un incendie ou une explosion, ainsi qu'à une interruption d'activité.

Evénements catastrophiques

Alors que des violations de données très importantes ont déjà eu lieu, la perspective d'une perte catastrophique est devenue plus probable, mais il est difficile de prédire ce qu'elle impliquera exactement. Les scénarios comprennent une attaque réussie contre l'infrastructure de base d'Internet, une violation grave des données ou une panne de réseau chez un fournisseur de cloud, alors qu'une cyber-attaque impartante impliquant une entreprise d'énergie ou de services publics pourrait se traduire par une interruption significative des services, des dommages matériels ou même des pertes humaines à l'avenir.

Couverture autonome

D'après Allianz, la portée de la cyber-assurance doit également évoluer en vue de fournir une couverture plus étendue et plus approfondie, prenant en charge l'interruption d'activité et comblant les lacunes entre la couverture traditionnelle et les cyber-polices. Alors que les exclusions des cyber-risques dans les polices IARD vont vraisemblablement devenir monnaie courante, la cyber-assurance autonome va continuer d'évoluer pour devenir la source principale de couverture complète. On observe un intérêt croissant dans les secteurs des télécommunications, de la distribution, de l'énergie, des services publics et du transport, ainsi que de la part des institutions financières.

La formation — en termes de compréhension de l'exposition de l'entreprise comme de connaissances en souscription — doit s'améliorer pour permettre aux assureurs de répondre à une demande croissante. De plus, comme pour tout autre risque émergent, les assureurs doivent en outre faire face à des défis concernant la tarification, les libellés des polices non testés, la modélisation et l'accumulation des risques.

Réponse aux cyber-risques

Le rapport d'AGCS expose les démarches que les entreprises peuvent entreprendre pour couvrir les cyber-risques. L'assurance ne peut être qu'une partie de la solution, avec une approche globale de la gestion des risques en guise de fondement de la cyberdéfense. « Le fait de contracter une cyber-assurance ne signifie pas que vous pouvez ignorer la sécurité informatique. Les aspects technologiques, opérationnels et assurantiels de la gestion des risques vont de pair », explique Jens Krickhahn, expert Cyber & Fidelity chez AGCS Central & Eastern Europe. La gestion des cyber-risques est trop complexe pour être l'apanage d'un seul individu ou département, de sorte qu'AGCS recommande la constitution d'un groupe de réflexion pour combattre les risques, au sein duquel différentes parties prenantes dans toute l'entreprise collaboreraient pour partager leurs connaissances.

De cette manière, différentes perspectives sont remises en question et d'autres scénarios sont pris en considération : ceux-ci peuvent par exemple inclure le risque découlant des développements de l'entreprise comme les fusions et acquisitions, ou de l'utilisation de services externalisés ou d'un cloud. De plus, la contribution intersociétés est essentielle pour identifier les actifs clés en matière de risque et, surtout, pour développer et tester des plans d'action solides en cas de crise.

Denis JACOPINI est Expert Judiciaire en Informatique, consultant, formateur et chargé de cours.
Nos domaines de compétence :
• **Expertises et avis techniques** en concurrence déloyale, litige commercial, piratages, arnaques Internet… ;
• **Consultant** en sécurité informatique, cybercriminalité et mises en conformité et déclarations à la CNIL ;
• **Formateur et chargé de cours** en sécurité informatique, cybercriminalité et déclarations à la CNIL.
Contactez-nous

Source : http://www.globalsecuritymag.fr/Allianz-Global-Corporate-Specialty,20150909,55621.html