Chubb aborde les risques cyber croissants avec une approche flexible et durable

Les assurés peuvent adapter les niveaux de couverture de leur assurance cyber pour les événements systémiques, les événements de types rançongiciels et carence de mise à jour de logiciel.

CHUBB®

Événements systémiques

Le monde devient chaque année plus numérisé et interconnecté. Des milliers ou des millions d'entreprises utilisent et s'appuient sur des logiciels, des plateformes de communication et de technologie. Une seule attaque et/ou défaillance de l'une de ces plateformes ou technologies largement utilisées pourrait créer un risque d'agrégation qui dépasse la capacité d'assurance du secteur. Afin d'offrir aux assurés une couverture claire et une stabilité du marché, Chubb prévoit des limites, des franchises et des coassurances précises et spécifiques pour de tels « événements systémiques ».

Types d'événements systémiques inclus dans la couverture :

- *Événements visant la chaîne d'approvisionnement logicielle :*
  Il s'agit d'attaques permettant aux pirates de pénétrer dans les systèmes par le biais de logiciels fiables et certifiés. Elles sont en fait un cheval de Troie.
- *Événements graves « zero-day » :* Ces attaques arrivent par certaines vulnérabilités logicielles connues des cybercriminels mais pas encore de tous. Ces vulnérabilités sont facilement exploitables, potentiellement sévères et souvent, ne bénéficient d'aucune protection.
- *Événements graves exploitant des vulnérabilités connues :*
  Ces attaques arrivent par de graves vulnérabilités logicielles connues n'ayant pas fait l'objet de correctif. Elles sont considérées comme graves car elles sont faciles à exploiter, elles peuvent être déployées à distance avec des privilèges d'accès limités et avoir un impact négatif significatif[1].
- *Autres événements systémiques :*
  Certains types de cyberattaques peuvent être menées simultanément ou automatiquement contre un grand nombre de victimes, provoquant finalement un événement cyber catastrophique. Internet et certains services de télécommunications ont atteint un niveau d'infrastructure sociétale critique, et certaines grandes entreprises infonuagiques sont si largement utilisées qu'une panne généralisée aurait des répercussions sur les activités de milliers voire de millions d'entreprises.

Exemples réels d'événements sytémiques :

- Événements visant la chaîne d'approvisionnement logicielle : Solorigate (2020) et NotPetya (2017)
- Événements graves « zero-day » : Hafnium (2021)
- Événements graves exploitant des vulnérabilités connues : Attaque MSSP (2021)
- Autres événements systémiques :
  Panne de service infonuagique Virginie (2020)

L'avenant relatif aux événements systémiques prévoit des règles d'indemnisation de sinistres concises et adaptées, notamment :

- Les frais de réponse à un incident n'épuisent pas les limites de l'événement systémique tant que l'incident n'est pas déterminé comme un événement systémique, et les frais engagés avant de déterminer la nature de l'incident restent à la charge de l'assureur.
- Les assurés peuvent choisir de ne pas partager certains types de données d'enquête lorsqu'il est mutuellement convenu qu'un incident est un événement systémique.
- Afin de permettre aux assurés de souscrire la couverture qui répond le mieux aux besoins de leur organisation, tous les incidents cybers sont classés dans l'une des catégories suivantes : Événements circonscrits (par exemple un événement dans le cadre des règles habituelles de sinistres) Événements systémiques (par exemple un événement systémique avec des différences structurelles d'ajustement des pertes telles que la limite, la franchise et la coassurance)

Rangonçiels

Les attaques par rançongiciels ont augmenté de façon spectaculaire, tant en fréquence qu'en gravité. Les conséquences en termes de pertes pour les assurés vont bien au-delà de la simple valeur de la rançon. Que la rançon soit payée ou non, les assurés doivent souvent faire face à des frais juridiques, des frais d'enquête, des pertes d'exploitation, des frais de récupération des données numériques et, potentiellement, des frais de responsabilité et de défense juridique. L'avenant Rançongiciel permet de personnaliser les limites de couverture, la franchise et la coassurance pour les pertes subies à la suite d'un rançongiciel.

Carence de mise à jour

Maintenir les logiciels à jour est un aspect important d'une bonne hygiène en matière de risques cyber. De nombreuses pertes peuvent être évitées en appliquant des correctifs aux logiciels vulnérables avant que les cybercriminels n'aient l'occasion de les exploiter. Mais certaines organisations peuvent ne pas appliquer de correctifs immédiatement. Il existe parfois des raisons légitimes pour lesquelles les mises à jour de logiciels doivent être testées avant d'être déployées, et des problèmes de compatibilité, de capacité ou de simple logistique peuvent empêcher même une organisation avec une sécurité de l'information bien gérée, de déployer des correctifs dès le premier jour ou la première semaine suivant leur disponibilité. C'est pourquoi Chubb accorde aux assurés une période de grâce de 45 jours pour corriger les failles de sécurité informatique qui sont publiées en tant que Common Vulnerabilities and Exposures (CVE) dans la base de données nationale sur les vulnérabilités gérée par le National Institute for Standards and Technology (NIST) des États-Unis.

L'avenant Carence de mise à jour offre une couverture après l'expiration du délai de grâce de 45 jours, le partage des risques entre le titulaire de la police et l'assureur passant progressivement au titulaire de la police, qui assume une part de plus en plus importante du risque si la vulnérabilité n'est pas corrigée après 46, 90, 180 et 365 jours.

Nous joindre

Pour en savoir plus sur l'expérience de Chubb en matière de gestion des cyberrisques et son expertise à la fine pointe de ce secteur, visitez le site https://www.chubb.com/ca-fr/business-insurance/cyber-services.html ou envoyez un courriel à votre Souscripteur Cyber chez Chubb.

Chubb. Insured.℠

[1]NIST Security Vulnerability Trends in 2020: An Analysis (2021). Issu de https://www.redscan.com/media/Redscan_NIST-Vulnerability-Analysis-2020_v1.0.pdf.