Chubb aborde les risques cyber avec une approche flexible et durable

Les assurés peuvent adapter les niveaux de couverture de leur assurance cyber pour les Evénements Systémiques, les Incidents Rançongiciels et les carences de mise à jour de logiciel.

Evénements systémiques

Le monde devient chaque année plus numérisé et interconnecté. Des milliers ou des millions d'entreprises utilisent et s'appuient sur des mêmes logiciels, des mêmes plates-formes de communication et des mêmes technologies. 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 parts de co-assurances spécifiques pour de tels "Evénements Systémiques".

Typologies d'Evénements Systémiques inclus dans la couverture

Vulnérabilités Systémiques Fournisseur

Il s'agit d'attaques permettant aux acteurs malveillants de pénétrer dans les systèmes par le biais de logiciels de confiance. Elles sont en fait un cheval de Troie.

Exemples réels > Solorigate (2020), NotPetya (2017)

Vulnérabilités Systémiques Zero Day

Ces attaques arrivent par certaines vulnérabilités logicielles connues des cybercriminels mais pas encore de tous. Ces vulnérabilités sont facilement exploitables, potentiellement critiques et souvent, ne bénéficient d'aucune protection.

Exemple réel > Hafnium (2021)

Vulnérabilités Systémiques Connues

Ces attaques arrivent par l'exploitation de vulnérabilités logicielles connues critiques n'ayant pas été corrigées. Elles sont considérées comme critiques car faciles à exploiter, peuvent être déployées à distance avec des privilèges d'accès limités et peuvent avoir un impact négatif significatif.

Autres Evénements 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 critique pour la société, et certaines grandes entreprises du cloud sont si largement utilisées qu'une panne généralisée aurait des répercussions sur les activités de milliers voire de millions d'entreprises.

L'avenant relatif aux Evénements Systémiques ajoute des règles d'indemnisation concises et adaptées, incluant notamment :

- Les Frais de Réponse à un Incident n'épuisent pas les limites de l'Evénement Systémique tant que l'incident n'est pas défini comme un Evénement Systémique.
- Les assurés peuvent choisir de ne pas partager certains éléments d'investigation permettant de qualifier l'incident (Evénement Circonscrit vs Evénement Systémique) lorsqu'il est mutuellement convenu qu'un incident est un Evénement 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 :
  - Evénement Circonscrit (par exemple un événement individuel bénéficiant de conditions « habituelles »)
  - Evénement Systémique (Par exemple un événement systémique bénéficiant de dispositions spécifiques telles que la limite, la franchise et la part de co-assurance)

Incidents Rançongiciels

Les attaques par rançongiciels ont progressé de façon spectaculaire, tant en fréquence qu'en intensité. Les conséquences en matière 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'expertise informatique, des pertes d'exploitation, des frais de reconstitution des données et, potentiellement, des frais de défense et conséquences pécuniaires de réclamation de tiers.

Les dispositions spécifiques liées aux Incidents Rançongiciels permettent d'adapter les limites de couverture, la franchise et la part de co-assurance pour les pertes subies à la suite d'un Incident 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. Cependant, certaines organisations peuvent ne pas appliquer les correctifs immédiatement. Il existe parfois des raisons légitimes pour lesquelles les mises à jour logicielles doivent être testées avant d'être déployées, et des problèmes de compatibilité, de capacité ou de simple logistique peuvent également empêcher une organisation avec une bonne gestion de sa sécurité informatique 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 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 [1].

[1]NIST Security Vulnerability Trends in 2020: An Analysis (2021). Accessed at https://www.redscan.com/media/Redscan__NIST-Vulnerability-Analysis-2020__v1.0.pdf.

Les dispositions spécifiques concernant les Carence de Mise à Jour offrent une couverture après l'expiration du délai de 45 jours via un partage des risques entre l'assuré et l'assureur.

L'assuré supportera progressivement une part d'autant plus importante du sinistre que la vulnérabilité n'est toujours pas corrigée après 46, 90, 180 et 365 jours.

Pour plus d'information

Rendez-vous sur notre site web www.chubb.com/fr/cyber ou contactez votre souscripteur cyber.

Chubb. Insured.℠