PANNE MONDIALE CROWDSTRIKE :

Quels impacts pour l'assurance des entreprises ?

La panne mondiale qui a affecté les entreprises et institutions du monde entier vendredi 19 juillet 2024 souligne notamment :

- le caractère potentiellement systémique du risque cyber,
- la coexistence des garanties de l'évènement malveillant, standard, et de l'événement accidentel, moins standard, dans les polices d'assurance,
- la question de la chaine de responsabilité voire de recours.

Ce que nous savons de cet incident

En l'état actuel des informations dont nous disposons, l'incident informatique majeur est le résultat d'un conflit entre la mise à jour de la solution d'EDR (Endpoint Detection & Response) Falcon de l'éditeur Crowdstrike et l'OS (Operating System) Windows.

Cet incident a eu pour conséquence une panne généralisée des systèmes utilisateurs, générant une impossibilité d'exploiter les Systèmes d'Information (SI).

Solutions proposées par les éditeurs

Windows et Crowdstrike ont très vite communiqué des procédures correctives :

https://www.crowdstrike.com/blog/statement-on-falcon-content-update-for-windows-hosts/

https://support.microsoft.com/en-us/topic/b1c700e0-7317-4e95-aeee-5d67dd35b92f

Nous recommandons, en complément des mesures techniques de remédiation, de rester vigilant, l'EDR (Endpoint detection and response) étant un des outils essentiels de la détection de la menace d'atteinte au SI (Système d'information). Il faut donc éviter autant que possible tout redémarrage en mode dégradé du point de vue de la détection des comportements suspects. Cette situation de « fragilité » pourrait en effet être exploitée par des organisations malveillantes.

Du point de vue de l'assurance

Cyber

L'ANSSI a écarté l'hypothèse d'une cyberattaque ; le fait générateur à retenir est donc l'évènement accidentel et non l'atteinte malveillante.

Pour que les conséquences de cet évènement soient couvertes par votre police d'assurance, il faut avant tout que :

- la durée de l'interruption d'activité dépasse le délai de carence (les polices mentionnent souvent 24h),
- la panne figure parmi les évènements couverts ; certaines polices dénomment clairement cet évènement garanti,
- éventuellement, la panne consécutive à un conflit provoqué par la solution d'un fournisseur et/ou prestataire IT soit prévue,
- la panne consécutive à une « montée de version » ne soit pas exclue.

Aussi sommes-nous à votre disposition pour répondre à vos interrogations et préciser les termes de votre police, ou des différentes polices du marché si vous n'êtes pas assuré.

Responsabilité Civile

Les conséquences de votre interruption d'activité pour vos clients (ou tout autre tiers) pourraient faire l'objet d'une réclamation à votre encontre au titre de votre Responsabilité Civile, en raison de l'impossibilité d'exécuter vos prestations, de la délivrance de vos prestations avec retard ou de la défectuosité constatée de vos produits livrés. Toutefois, dans certains cas un tel incident pourrait constituer un évènement de force majeure exonératoire de votre responsabilité.

Pour apprécier l'applicabilité de votre contrat de Responsabilité Civile dans le contexte Crowdstrike / Microsoft, nous recommandons de veiller en particulier :

- **A la définition de l'« événement cyber » :**
  - Si cet incident entre dans la définition d'événement cyber aux termes de votre contrat RC, il convient de vérifier la couverture des Dommages Immatériels Non Consécutifs "DINC" : généralement exclus, ils peuvent faire l'objet de rachats de garantie en RC Exploitation, RC Produit/Après Livraison et/ou RC Professionnelle,
  - A contrario, si le contrat limite le périmètre de l'«événement cyber» à un événement d'origine malveillante ou une action non autorisée dans le SI (Système Informatique) de l'assuré, l'exclusion relative à l'« événement cyber » , telle que prévue dans les contrats RC, ne trouverait pas application en l'espèce.
- **A l'exclusion du retard de livraison :** cette exclusion est généralement assortie d'un rachat du fait d'un dommage accidentel qui, au titre de cet incident, pourrait trouver application.

Dommages aux biens

Sauf rare extension « pertes d'exploitation ou frais supplémentaires sans dommages matériel », les contrats d'assurance dommages aux biens ne sont pas mobilisables. Au-delà de l'objet des contrats rédigés désormais (depuis la grande remédiation des textes en 2020/2022) de telle sorte que les dommages immatériels doivent être strictement consécutifs à la survenance de dommages matériels, les événements Cyber sont désormais strictement exclus qu'ils s'agissent :

- de phénomènes accidentels (« Cyber Event ») que ce soit champ magnétique, microcoupure, erreur dans les instructions données aux machines (i.e. erreur de programmation),
- de phénomènes malveillants (« Cyber Act »).

Seuls les dommages matériels sont rachetables avec beaucoup de réticences pour racheter d'autres phénomènes que l'incendie ou l'explosion.

Si l'événement est dénommé, les polices « pertes pécuniaires diverses » souscrites via des polices captivées pourraient être répondantes.

Nous vous invitons à prendre contact avec nos spécialistes, experts des risques cyber ou de Responsabilité Civile, qui auront le plaisir de répondre à vos demandes de précisions.

Alexandra Gavarone,
Directrice
Département Risques Financiers

Audrey Bernard,
Directrice
Département Responsabilité Civile, Environnement & Individuelle Accident

Stéphanie Bournoville, Directrice adjointe
Sébastien Hager, Responsable Pôle Cyber
Maxence Le Garrec, Directeur Indemnisation

Xavier Denis, Directeur Production
Philippe Boizon, Directeur Indemnisation

DiotSiaci