L'AGEFI

Cyber

Le délai de déclaration d'une cyberattaque devient la clé de l'indemnisation

Un futur amendement dans le projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité veut modifier le délai de dépôt de plainte de 72 heures en cas d'incident cyber.

Publié le 8 janvier 2026 à 16:52

Marie-Amélie Fenoll Camille George

Écouter l'article 03:47 min

- Fotolia

Le risque cyber court encore et toujours. Comme il devient protéiforme et plus sophistiqué, se pose la question épineuse de sa couverture assurantielle. Plusieurs amendements ont été déposés dans le cadre du

projet de loi relatif à la résilience des infrastructures critiques et au renforcement de la cybersécurité concernant la couverture assurantielle des risques cyber.

Après plusieurs reports dus à l'instabilité politique de ces derniers mois, le projet de loi devrait revenir en lecture à l'Assemblée nationale en février. Une occasion pour les risk managers des entreprises, par la voix de leur association, l'Amrae, d'amender certains aspects de la déclaration d'incident cyber, à savoir le délai de dépôt de plainte en cas d'attaque.

Délai de 72h

Actuellement, le code des assurances ainsi que la loi d'orientation et de programmation du ministère de l'intérieur (LOPMI) contraignent les entreprises à déposer plainte au commissariat dans les 72h qui suivent l'attaque cyber. Un délai particulièrement court qui ne laisse pas aux entreprises le temps d'analyser les répercussions de l'attaque sur leurs activités, filiales comprises. Or, la garantie cyber et l'indemnisation potentielle qui en découle dépendent de ce dépôt de plainte. Il y a donc un risque de perte de garantie si le dépôt de plainte est hors délai. *« Une particularité française qui incite parfois à s'assurer hors de France pour ne pas avoir cette contrainte »,* souligne l'Amrae.

L'amendement, qui est le fruit d'échanges entre l'Amrae, la direction générale du Trésor, le parquet cyber et France Assureurs, vise donc à instaurer un décompte de 72h non pas dès la survenance de l'incident mais au moment de sa notification à l'assureur. *«Ce qui n'a rien à voir en termes d'analyse du risque et d'évaluation des pertes»*, souligne François Baume, président de l'Amrae. *Par ailleurs, aujourd'hui le dépôt de plainte sert uniquement à éviter la déchéance de garantie ce qui n'est pas l'objectif initial. Si le délai est modifié comme proposé, les plaintes pourront être beaucoup plus fournies et documentées, ce qui permettra à la gendarmerie d'en tirer profit pour ses analyses et pour apporter un support adéquat.»*

Sans compter qu'il serait *« plus efficace de limiter ce dépôt de plainte par les entreprises assurées aux attaques qui vont potentiellement entrainer*

une indemnisation et non pas les alertes ou petites attaques qui n'ont pas de conséquence et où la loi actuelle peut amener à saturer les parquets avec des plaintes sans importance qui ne seront pas instruites», précise l'amendement dans sa rédaction. Et de fait, éviter l'engorgement des tribunaux.

A lire aussi: L'évolution rapide du risque cyber oblige les assureurs à revoir leur approche de couverture

Preuve à charge au crédit de l'assureur

Autre point de crispation pour les gestionnaires des risques, la charge de la preuve quant à la nature de l'attaque qui pèse sur l'entreprise et non sur l'assureur. *«Contrairement aux autres pays, il n'y a qu'en France où la preuve à charge incombe à l'entreprise et non à l'assureur. De plus, l'assuré doit démontrer l'absence de lien de causalité entre le sinistre et un fait de guerre étrangère»,* a rappelé François Beaume, président de l'Amrae.

De plus, s'agissant des couvertures de dommages aux biens, les risques de guerre, considérés inassurables, sont légalement exclus de la garantie de l'assureur, sauf convention contraire. Mais de fait, cela ne peut s'appliquer en cas de cyberattaque, juge l'Amrae qui rappelle que *«la loi ne prévoit pas expressément d'exclusion pour le risque d'attaques cyber d'origine étatique (cyberguerre)».* Des exclusions conventionnelles disparates commencent cependant à émerger dans les polices d'assurance, ce qui crée une insécurité juridique à la fois pour les assurés et les assureurs, rapporte l'Amrae.

Ainsi, pour inverser la charge de la preuve vers l'assureur et non l'entreprise assurée, un amendement a été adopté en commission le 10 septembre dernier. Celui-ci a également été rédigé en concertation avec la Direction générale du Trésor, l'Agence nationale de la sécurité des systèmes d'information (ANSSI), l'ACPR, l'Amrae et France Assureurs.

A lire aussi: Le marché de l'assurance cyber aborde une nouvelle phase de croissance

Assurance