

# Assurances cybercrime: ce qu'il faut savoir

Des offres spécifiquement destinées aux PME et aux indépendants ont fait leur apparition il y a quelques années. Elles ne remplacent cependant en aucun cas les bonnes pratiques de sécurité et peuvent receler des pièges.

PIERRE CORMON

L'attitude des entreprises face aux risques informatiques a évolué. «Cela fait des années que nous sensibilisons nos clients à ce sujet, mais depuis les récentes attaques contre des communes, les demandes de couverture contre la cybercriminalité ont nettement augmenté», raconte Pascal-Henri Vuilleumier, directeur du courtier CGA Conseils.

Or, plusieurs compagnies offrent des polices spécifiquement destinées aux PME et indépendants. L'essentiel en quelques points.

## ❑ Les PME et les indépendants ont-ils intérêt s'assurer?

«Nous le proposons systématiquement à nos clients, en option, mais il est important de comprendre qu'une assurance ne remplace pas une bonne politique de sécurité informatique», répond Steven Meyer, CEO et cofondateur de l'entreprise de sécurité informatique ZENDATA. «C'est un peu comme pour une bijouterie. Elle peut s'assurer contre le vol, mais il est encore plus important d'avoir un garde et un local sécurisé.»

D'autant plus que si les assurances prennent en charge un certain nombre de dommages (lire question suivante), d'autres ne sont ni chiffrables, ni assurables, comme la perte de confiance des clients et les dégâts d'image.

## ❑ Que peuvent couvrir ces assurances?

«Une police globale doit prendre en charge trois types de dommages», répond Sophie Di Meglio, Directrice des risques spéciaux du courtier Swiss Risk & Care. Il s'agit de:

⇒ la gestion de la crise (hotline ouverte sans interruption pouvant orienter vers des spécialistes des technologies de l'information, des juristes et des experts en gestion de crise);

⇒ la prise en charge des dommages (par exemple la perte de revenus due à l'interruption d'exploitation ou la reconstruction des données perdues);

⇒ la responsabilité civile (par exemple les éventuels litiges avec des tiers au sujet des données volées).

A noter que les polices contiennent généralement une franchise, un délai de carence (pour la perte de revenus) et une somme assurée maximale, au-delà de laquelle on n'est plus couvert.

## ❑ Toutes les polices couvrent-elles ces trois types de dommages?

Non. Certaines compagnies proposent des garanties sous forme d'extension d'un contrat d'assurance chose ou responsabilité civile, qui ne couvrent qu'une partie d'entre eux. «Quoiqu'il en soit, il est important de veiller à ce que les garanties de base soient souscrites, ou, si ce n'est pas le cas, d'être conscient que l'on n'a souscrit qu'une partie

de ces garanties», avertit Sophie Di Meglio.

## ❑ Les éventuelles rançons sont-elles couvertes?

«Elles l'étaient au plein de la garantie, mais ce n'est plus la tendance aujourd'hui», répond Sophie Di Meglio. «La situation varie d'une compagnie à l'autre. Certaines l'excluent totalement, d'autres la garantissent partiellement à hauteur d'une sous-limite (par exemple 25% de la somme d'assurance)». Dans tous les cas, le paiement d'une rançon n'intervient qu'en dernier recours, lorsqu'on a épuisé les autres possibilités.

## ❑ Certaines branches d'activités sont-elles exclues?

La politique varie d'assureur en assureur, mais les compagnies rechignent généralement à accepter les entreprises actives dans les services financiers, les jeux en ligne, l'e-commerce, les infrastructures critiques, l'armement et les équipements militaires, les télécommunications, la santé, les cryptomonnaies, l'industrie du sexe, etc. Elles sont en effet très exposées aux attaques et les dommages peuvent s'avérer considérables. Passer par un intermédiaire peut cependant faciliter les choses. «Nous parvenons à convaincre des assureurs d'accepter des entreprises de secteurs dont ils se méfient, car ils nous connaissent et savent que nous aidons nos clients à se protéger au mieux», explique Steven Meyer.

## ❑ L'assureur examine-t-il la sécurité informatique du client potentiel?

Cela dépend. Pour les gros clients, l'examen peut être assez poussé. «Pour les indépendants et PME, cela varie d'un assureur à l'autre», ajoute Sophie Di Meglio. Certains assureurs ne font même pas remplir de questionnaire à leurs clients, dans le cas d'une extension d'un contrat choses ou responsabilité civile. D'autres font remplir un questionnaire très simple, avec des rubriques telles que le chiffre d'affaires, le secteur d'activité, la somme d'assurance, de franchise et les extensions de garantie souhaitées, sans demander de détails techniques.

D'autres, enfin, demandent de remplir des questionnaires plus techniques. Ils peuvent porter sur la formation et la sensibilisation régulière du personnel, les mesures de protection adoptées, la nature et le volume des données sensibles, la fréquence des sauvegardes et d'actualisation des logiciels, la gestion de l'accès des utilisations aux systèmes, etc. Selon les réponses, l'assureur pourra proposer une offre, demander des améliorations ou refuser tout simplement la couverture – ce dernier cas est cependant minoritaire dans les secteurs jugés peu sensibles.

Une mesure est systématiquement exigée: c'est la mise en place d'une authentification multi-facteur nécessitant deux

ou plusieurs étapes de vérification (par exemple, un mot de passe plus un code envoyé par SMS) pour se connecter à distance sur le système de l'entreprise ou accéder à des données sensibles. Les autres conditions peuvent comprendre des exigences telles que réaliser une sauvegarde par semaine, effectuer systématiquement des mises à jour de sécurité, etc.

Les prestations peuvent être réduites, voire refusées si l'assuré ne s'est pas conformé à ces règles. «Or, certaines assurances imposent des conditions si strictes que l'on sait d'avance que, le jour où un sinistre survient, le client n'aura pas rempli toutes les conditions», prévient Steven Meyer. Mieux vaut donc les examiner attentivement.

## ❑ Serais-je plus facilement accepté si je possède un label du type Cybersafe?

Certaines compagnies peuvent accorder un rabais aux entreprises certifiées avec ce label, spécifiquement destiné aux PME. D'autres incluent des questions relatives aux certifications et normes ISO dans le questionnaire qu'elles font remplir aux clients potentiels, mais ce n'est pas le cas de toutes. La démarche pour obtenir le label permet d'adopter des bonnes pratiques, ce qui augmente les chances d'être accepté par une compagnie d'assurances et réduit le risque d'être victime d'une attaque.

## ❑ Combien peut coûter une couverture?

La prime dépend en général du secteur d'activité, du chiffre d'affaires et des réponses apportées au questionnaire sur les mesures de cybersécurité. «Pour les indépendants et les très petites entreprises, on trouve des polices à partir de deux cents francs par an pour une couverture de cent mille francs», précise Sophie Di Meglio. «Pour une entreprise réalisant de quinze à vingt millions de chiffre d'affaires, les primes que nous voyons aujourd'hui oscillent entre mille cinq cents et six mille cinq cents francs par an, pour une somme assurée d'un million de francs et une franchise se situant entre dix mille et vingt mille francs.»

## ❑ L'augmentation des cas d'intrusion rejait-elle sur les primes?

Oui, très nettement. «Non seulement les primes augmentent, mais les conditions se resserrent, notamment au niveau du ransomware», observe Sophie Di Meglio. «Pour les grands comptes, on a vu des primes augmenter de 150% à 200% en quelques années, alors que les sommes assurées ont été divisées par quatre et des franchises revues fortement à la hausse. Pour les petits clients, l'augmentation est moins sensible, mais tout de même réelle.» ZENDATA pronostique un doublement des primes d'ici à un ou deux ans. ■