«Se protéger contre les risques de cyberattaques est essentiel pour toute entreprise»

Puisque les risques en termes de cyberattaques seront de plus en plus conséquents à l'avenir, les assurances en cybersécurité constituent une priorité pour les entreprises.

Joël Ramos

Directeur technique, Economiste d'entreprise HES,
Brevets fédéraux en assurances sociales et en conseil financier

Aujourd'hui, l'importance de la cybercriminalité dans le secteur de l'assurance est croissante. Les entreprises sont de plus en plus dépendantes de leurs systèmes informatiques et de leurs infrastructures numériques. Cette véritable montée en puissance technologique expose chaque entreprise au véritable danger que constitue la cybercriminalité.

Aucune entreprise n'est à l'abri d'une attaque car cette menace vise les multinationales comme les PME. Conclure une assurance cybersécurité constitue alors une véritable plus-value pour toute entreprise. Ceci permet de se protéger contre les demandes de rançon, les attaques virales générales, le vol ou la fuite d'informations.

C'est ce que souligne Joël Ramos, directeur technique de Argos Group qui aide ses clients à définir les risques et à se protéger convenablement. Avec une augmentation considérable des cyberattaques et une évolution permanente des nouvelles technologies, la cyberassurance permet de transférer son risque et de s'entourer d'experts afin d'affronter les problèmes financiers, juridiques et réputationnels liés aux cyberattaques et aux fraudes.

Comment une société comme Argos Group se protège-t-elle des cyberattaques?

De manière générale, Argos Group a mis en place différentes procédures en termes de sécurité. Tout d'abord, l'entreprise procède régulièrement à une analyse complète pour s'assurer que la protection anti-virus est suffisante. Ensuite, l'employé contrôle que les supports externes de données introduits dans l'ordinateur soient exempts de toute contamination. En cas de découverte d'un virus, le poste de travail infecté ne doit plus être utilisé. Toutes les identités sont uniques, personnelles et ne peuvent pas être partagées avec d'autres employés. Nous utilisons également l'authentification double via le système de MFA (reconnaissance par multi-facteurs). Concernant la messagerie électronique, le collaborateur doit s'assurer de la source des fichiers attachés. C'est pour toutes ces raisons qu'il est primordial de sensibiliser les employés et de les former aux risques et à la manière de réagir.

Quel a été l'impact du coronavirus en termes de cybersécurité?

Son impact a été très fort et l'instabilité créée par cette pandémie a favorisé les actions des cybercriminels. De nombreuses entreprises n'étaient pas prêtes à réaliser du télétravail. Par exemple, nous avons remarqué une augmentation du nombre d'attaques de phishing par mail. La Covid-19 nous a rappelé qu'un virus représente un problème concret et que l'invisible et l'intouchable ont des effets destructeurs plus conséquents des incidents tangibles.

Quel rôle joue Argos Group en matière de cybersécurité par rapport à ses clients?

La devise de Argos Group est «prévoir pour préserver». Ainsi, nous jouons un rôle de Risk Manager auprès de nos clients. Au sens large, la gestion des risques se définit comme la maîtrise consciente des dangers. Son but est de déceler les risques qui peuvent empêcher la réalisation d'un objectif. Avec nos clients, nous identifions les risques et définissons la protection la plus adaptée contre ces derniers. Le client peut alors décider de renoncer à son objectif premier parce que le risque est trop élevé. Il peut réduire les risques et limiter les dommages, opter pour une assurance et choisir la couverture adaptée ou décider de prendre personnellement en charge le risque.

Que couvre cette cyberassurance?

La cyberassurance offre trois garanties importantes. Il y a d'abord une responsabilité civile et une protection juridique contre les dommages à des tiers. En effet, si des clients portent plainte pour atteinte au respect de la vie privée et aux droits de la personnalité ou pour transmission d'un virus à un tiers, l'entreprise assurée bénéficiera d'une protection juridique lors de la procédure administrative ainsi que d'un remboursement sur les préjudices de fortune consécutifs à la violation de la sécurité des informations.

Deuxièmement, elle propose une assistance complète en cas de gestion de crise: elle est là dès la phase qui suit la cyberattaque par l'intervention d'experts et la prise en charge des frais associés.

Enfin, elle inclut une couverture pour les propres dommages, à savoir l'élimination des malicieux ainsi que la reconstitution et/ou récupération des données électroniques et des logiciels. Elle offre une couverture en cas de perte de produit d'exploitation dû à une cyberattaque ou dans le cas d'une cyberextorsion.

En plus de ces garanties, la cyberassurance offre une palette d'autres modules liés notamment aux escroqueries de cartes de crédit ou aux achats en ligne. Il est donc recommandé de se rapprocher d'experts comme Argos Group pour être guidé au mieux.

Comment voyez-vous l'avenir de l'assurance en cybersécurité?

Je pense qu'elle sera de plus en plus nécessaire. Aujourd'hui, nous sommes toujours plus digitalisés. Pourtant, nous avons toujours un train de retard par rapport aux cybercriminels. Les risques sont nombreux et ils le seront davantage à l'avenir. Dans ce contexte, l'assurance en cybersécurité a toute sa légitimité. Se protéger contre les risques de cyberattaques est essentiel pour toute entreprise et même pour les ménages privés.

TEXTE **ANDREA TARANTINI**

ARGOS | GROUP