Risques de cybersécurité : tout le monde concerné, certains assurés

À la suite des récentes cyberattaques dans divers secteurs d'activité comme des logiciels de gestion d'enregistrements aériens, la criminalité informatique est à nouveau sous le microscope. Quand il y a un risque, un mouvement naturel est de tenter de limiter les dégâts. Au moyen, par exemple d'une assurance. De plus en plus d'entreprises se tournent vers des assureurs pour gérer ce risque de plus en plus fréquent.

Par Pascal Bustamante

Un risque en pleine progression

Le risque d'incidents de cybersécurité s'est considérablement accru, entre autres par la dématérialisation de plus en plus importante des entreprises.

Les criminels, par ailleurs investissent de plus en plus l'espace cyber dans lequel les opportunités d'escroqueries en tous genres se multiplient également.

Enfin, les pouvoirs publics se sont aussi saisis de cette matière en produisant des législations obligeant les acteurs, étatiques et privés, de se munir d'outils pour contrer les cybermenaces. L'Union européenne a pris des initiatives législatives. Parmi elles, la directive européenne NIS2 transposée dans diverses législations nationales. Une directive qui met le doigt sur ces nouveaux risques et qui impose aussi des mesures pour s'en prémunir.

Des dégâts qui peuvent être importants

Tom Van Britsom est expert en assurances cyber et en sécurité chez le courtier en assurances Vanbreda Risk & Benefits. Il nous détaille les activités de son employeur, actif dans l'assurance du risque cyber depuis 2010. Il a depuis lors traité plus de 300 cas d'incidents cyber parmi lesquels on compte aussi bien des hackings (piratages) que du phishing (usurpation d'identité en vue de voler des informations sensibles permettant par exemple le vol) :

"En 2024, pour 72% des assurés, les dommages sont restés limités (inférieurs à 20.000 €). Pour 12%, les montants étaient compris entre 20.000 € et 100.000 €. Pour 12%, ils étaient entre 100.000 € et 1.000.000 €. Enfin, pour 4%, ils dépassaient 1.000.000 €. Ces chiffres concernent uniquement les cas assurés ; nous ne traitons pas ici des pertes non assurées."

Des assurances comportant trois piliers importants

Pour notre spécialiste, une assurance cyber repose en général sur trois piliers.

- Le premier pilier, c'est l'assistance. Celle qui vous aide immédiatement quand vous êtes confronté à un cyber incident pour réactiver les choses le plus vite possible. Par exemple, pour récupérer des données, négocier avec les criminels qui demandent une rançon. […]
- Le deuxième pilier, c'est celui qui concerne tous les dégâts qu'un client s'est infligés lui-même. C'est par exemple la couverture d'une interruption des activités. Prenons une entreprise de production de fromage ou de chocolat et le temps que la production est arrêtée. On va immédiatement calculer les dégâts auxquels elles sont confrontées pendant la période d'inactivité forcée.
- Le troisième pilier ce sont les réclamations tierces : la prise en charge des demandes en responsabilité émises par des clients ou des individus suite à l'incident.

Quels sont les critères de l'assurabilité des entreprises

La variété des entreprises qui peuvent être touchées par la cybercriminalité est telle qu'une approche individualisée de la part de l'assurance est indispensable. Néanmoins, notre expert souligne cinq critères à tenir à l'œil pour évaluer le risque et l'importance de la prime :

- l’authentification multi-facteurs,
- la stratégie et la fréquence des sauvegardes (back-up) et leur rapidité de restauration,
- la sécurité des endpoints (PC, portables, smartphones),
- la gestion des vulnérabilités et le suivi/scan IT,
- ainsi que la formation du personnel.

"Nous constatons que 90% des incidents résultent d’une erreur humaine (clic sur un lien de phishing, mauvaise manipulation, etc.)".

Tous ces aspects vont faire l’objet d’une évaluation qui va, à son tour, donner une idée à l’assureur du risque à couvrir.

Et question prix : "Pour une entreprise réalisant 100 millions de chiffre d’affaires, il est possible de proposer une couverture correcte à partir d’une prime modeste (ex. 10.000 €) : avec ce montant, on peut déjà obtenir une assurance qui couvre la majorité des coûts d’un incident cyber".

Sans compter qu’une réévaluation des procédures de sécurité peut aboutir, après amélioration, à une révision à la baisse du montant des primes.

Personne n’est à l’abri

Croire que les cybercriminels ne vont s’attaquer qu’aux grandes entreprises est - de l’avis de tous les spécialistes - un leurre. Mais toute entreprise disposant d’adresses e-mail pour les collaborateurs fournit ainsi des portes d’entrées potentielles pour les criminels.

« La question n’est pas de savoir si on va être confronté à un risque cyber mais quand on va y être confronté. » Ertu Musoglu, Adjoint au responsable du risque cybernétique et de la sécurité chez HeadMind Partners

Pour Ertu Musoglu, adjoint au responsable du risque cybernétique et de la sécurité chez HeadMind Partners, les personnes qui travaillent dans les PME et les indépendants sont moins au fait des bonnes pratiques générales de la cybersécurité.

"Ce sont par exemple les bonnes pratiques, du style avoir un mot de passe qui est particulièrement sécurisé. Donc pas juste le nom ou le prénom ou une date d’anniversaire, ne pas écrire son mot de passe sur un morceau de post-it qu’on colle sous un PC. Vous n’avez pas idée du nombre de gens qui font encore ce genre de choses".

Une sensibilisation du Service Public Fédéral Économie

Le mois d’octobre est devenu aussi celui de la cybersécurité. À cette occasion, le Service Public Fédéral Économie s’est lancé dans une campagne de sensibilisation à destination des entreprises et plus particulièrement des PME. Il a confié à HeadMind Partners l’organisation d’ateliers de formation et des modules gratuits permettant aux employés de la fonction publique d’explorer les règles de base de la cybersécurité.

Pour Ertu Musoglu, il s’agit avant tout d’un travail de sensibilisation mais aussi de diagnostic correct : "Ce sont des ateliers où on fait participer les gens activement et où on leur donne des notions de cybersécurité. Comment fait-on face à un ransomware (logiciel de demande de rançon, ndlr) ? Comment avoir des bonnes pratiques de cybersécurité ? Et on a également des programmes qui, par l’intermédiaire de notre site web cyber4sme.be, permettent de faire un état des lieux de la situation en termes de protection IT de la société."

Pour les PME et même les autoentrepreneurs, la démarche peut aller plus loin. Notamment sur la recherche de solutions une fois que d’éventuelles failles auront été découvertes : "On a un chatbot dédié sur notre site qui va poser toute une série de questions et on va pouvoir faire un état des lieux du niveau de sécurité de l’entreprise, de la PME ou de l’indépendant qui répond. Alors à cela aussi, on ajoute un service supplémentaire, c’est qu’on propose un entretien d’une heure avec un de nos

consultants pour aller plus loin que l’état des lieux et peut-être amener des solutions et une capacité d’amélioration de la situation."

La cybersécurité est donc une question qui se pose à tous. De la plus petite entité à la plus grande. Avec la numérisation de toutes les interactions sociales que nous avons vécues et que nous continuons à vivre, toutes les facettes de l’activité humaine ont à présent leur pendant numérique. C’est vrai pour les affaires, c’est aussi vrai pour la criminalité.

Source : rtbf
Date : 2 octobre 2025