Assurances

Cyberattaques: pourquoi s'assurer n'est pas la meilleure solution

Par Astrid Landon le 23.07.2017 à 11h24, mis à jour le 24.07.2017 à 10h11

Les risques de cybercriminalité sont l'une des bêtes noires des entreprises. Les cyberattaques deviennent de plus en plus nombreuses et coûteuses. Face à cette situation, s'assurer n'est pas forcément la meilleure solution.

Les cyberattaques peuvent avoir un coût très important pour les entreprises, notamment en termes d'image.
KIRILL KUDRYAVTSEV / AFP

https://www.challenges.fr/finance-et-marche/assurances/cyberattaques-pourquoi-s-assurer-n-est-pas-la-meilleure-solution_488857

SUR LE MÊME SUJET

- **FedEx annonce un "impact matériel" de la cyberattaque Petya**
- **La facture astronomique que pourrait provoquer la future cyberattaque mondiale**
- **La cyber-attaque venue d'Ukraine était sans doute une diversion**
- **Cyberattaque : comment un virus informatique peut mettre à genoux le monde entier**
- **Cybersécurité: ces 3 priorités que les entreprises devront traiter d'ici 2020**

Les cyberattaques seront de plus en plus coûteuses et de plus en plus nombreuses à l'avenir. Au cours des dernières années, les offres d'assurances anti-cyberattaques, les cyberassurances, ont fleuri dans le monde. Le problème, c'est que les risques de cyberattaques sont pour la plupart difficilement chiffrables car ils peuvent avoir un impact sur de nombreux aspects de la vie d'une entreprise, comme sa réputation ou son image. Dès lors, la problématique assurantielle devient un véritable casse-tête. Car plus le risque est important et plus la police d'assurance sera chère. Va-t-on se diriger vers des assurances qui ne couvriraient que la moitié du risque ? Les risques devenant plus coûteux, cela entraînera-t-il une hausse des prix telle que les entreprises ne pourront plus s'assurer contre les cyberattaques ? L'assurance est-elle vraiment nécessaire lorsqu'une cyberprotection solide est installée en amont ? Plus simplement, la cyberassurance est-elle la meilleure solution à la cyberattaque ?

Un retard à combler par rapport aux Etats-Unis

"Au sein de notre groupe international, le premier produit de cyber-assurance a vu le jour dès 1998 aux Etats-Unis. Il faut cependant attendre septembre 2012 pour que son équivalent naisse en France", rappelle Sophie Parisot, product leader cyber d'AIG en France. En cause, le manque d'attaques en France par rapport au voisin américain. "Les objets connectés qui intéressent les cybercriminels sont arrivés tard en Europe", explique Michael Bittan, associé responsable des activités de gestion des risques cyber chez Deloitte. Le risque étant moins présent sur le vieux continent, les polices d'assurance avaient moins de raisons de se développer.

Et puis, il y a aussi les réglementations européennes. Aux Etats-Unis, le cadre juridique est plus adapté qu'en Europe en ce qui concerne le marché des cyberassurances. La donne est cependant en train de changer. Le 25 mai 2018 entrera en vigueur le règlement européen sur la protection des données (RGPD) qui obligera les professionnels à augmenter leur niveau de cybersécurité.

"En France, la cyberdélinquance est de plus en plus présente. Les technologies d'attaques sont disponibles en ligne ou sur le dark web. L'article 32 du RGPD oblige à mettre en place des systèmes de sécurité pour protéger les données personnelles. Quant à l'article 33, il contraint dorénavant à notifier à la CNIL les failles de sécurité", précise Alain Bensoussan, avocat à la Cour d'appel de Paris spécialisé en droit de l'informatique et des technologies avancées. S'ils ne suivent pas les nouvelles directives, les grands groupes pourront être condamnés à une amende représentant jusqu'à 4% de leur chiffre d'affaires ou 20 millions d'euros.

"La discrétion, un élément de défense"

La plupart des entreprises touchées par des cyberattaques ne communiquent pas sur le sujet. Elles craignent la double peine, avec le coût qu'une telle information pourrait avoir sur leur image et leur réputation. Joint par *Challenges*, le groupe Auchan, cible récemment d'une cyberattaque contre ses hypermarchés en Ukraine, refuse de s'exprimer et affirme que "la discrétion est aussi un élément de défense".

Aujourd'hui, les assurances proposent pour la plupart un volet de prestations qui accompagnent la compensation financière. "C'est là qu'est désormais la valeur ajoutée comme en témoigne notre approche chez AIG. Le conseil dans la prévention en amont et l'accompagnement réactif en cas de crise sont aussi importants aujourd'hui que les indemnités", explique Christophe Zaniewski, directeur général d'AIG en France.

DSI de Saretec et porteur de l'offre cyber du Groupe Saretec, Alain Guède précise que le Cyber-risque ne devrait pas seulement être appréhendé en termes de technique ou d'assurance mais en termes de services. En tant que Société d'expertise en assurance après sinistre, l'approche du Groupe Saretec est centrée sur les conséquences comme point de départ à la déclinaison de services à définir pour construire une prévention efficace et couvrir toutes les prestations en cas d'attaque. « Nous avons une approche 360° couvrant la prévention, la réparation technique après l'attaque et l'évaluation des dommages, des responsabilités et des conséquences financières, voire la gestion de crise ».

En somme, ce qui a changé c'est surtout le "servicing", c'est-à-dire les offres de prestation. AIG propose par exemple des consultations d'experts juridique, informatique, en communication et en négociation dans le cas de ransomware par exemple. Lorsque AIG a proposé sa première offre de cyberassurance, durant deux ans ce sont surtout les entreprises du CAC 40 très exposées qui étaient intéressées. Aujourd'hui, la cyberassurance semble être devenue un outil essentiel de la protection contre la cybercriminalité, ou presque.

La cyberassurance, pas la meilleure solution

Michael Bittan est partagé. « Je ne suis pas certain que la cyberassurance soit la meilleure des solutions face à la cybercriminalité ». Selon lui, il serait plus efficace d'investir dans la protection en amont. « Les entreprises ne laissent pas souvent des personnes de l'assurance remettre en état le service informatique quand elles disposent pour la plupart d'équipes qui s'en occupent déjà en interne et qui connaissent déjà parfaitement le système d'information».

Selon Michael Bittan, les grands groupes s'assurent souvent ad minima car cela prend sur le budget cyber et n'apporte pas grand-chose de plus si la compagnie a déjà un niveau de maturité élevé concernant la cybersécurité. "Le vrai marché c'est sans doute les PME", estime Michael Bittan.

L'une des raisons pour lesquelles ce nouveau marché que constitue la cyberassurance peine à décoller réside sans doute dans le fait qu'il n'est pas certain que le cyber risque puisse être couvert dans son ensemble.

Comment se protéger en amont

Alors, que faire si la cyberassurance n'est pas une solution ? Les experts s'accordent à dire : se protéger. Contrairement à Michael Bittan, Alain Guède demeure persuadé que l'assurance est un outil essentiel cependant, il évoque aussi trois manières de réduire les risques. Tout d'abord, instaurer dans l'entreprise une politique de gestion des patchs afin que les failles soient réparées plus efficacement : l'attaque Petya avait utilisé la même faille que WannaCry un mois plus tôt.

Ensuite, instaurer des parcs homogènes. "La plupart des grands groupes renouvellent leur parc informatique par tiers ce qui fait que les systèmes d'exploitation sont différents et cette pluralité ralentit la diffusion des patchs qui doivent être adaptés à chaque ordinateur", selon Alain Guède.

Enfin, il est utile de réfléchir à une politique de bac à sable, c'est-à-dire sous-traiter à une entreprise la gestion des mails. La société déroule les mails à votre place et les fait exploser sans risque pour le serveur ce qui permet de se débarrasser d'éventuels virus. "C'est comme une maison, si vous êtes cambriolés alors que votre porte était grande ouverte il ne faut pas s'en étonner. En revanche, si vous avez disposé des alarmes partout et que vous fermez à double tour il y a moins de risque que ça arrive", conclut Alain Guède.

#CYBERATTAQUE #ASSURANCE