

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



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

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 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...[lire la suite]

NOTRE MÉTIER :

PRÉVENTION : Vous apprendre à vous protéger des pirates informatiques (attaques, arnaques, cryptovirus...) sous forme de conférences, d'audits ou de formations ;

RÉPONSE A INCIDENTS : Vous aider à rechercher l'origine d'une attaque informatique, recueillir les preuves pour une utilisation auprès de la justice ou des assurances, identifier les failles existantes dans les systèmes informatiques et améliorer la sécurité de l'existant ;

SUPERVISION : Assurer le suivi de la sécurité de votre installation pour la conserver le plus possible en concordance avec l'évolution des menaces informatiques.

MISE EN CONFORMITÉ CNIL : Vous assister dans vos démarches de mise en conformité avec le RGPD (Règlement Européen relatif à la Protection des Données à caractère personnel).

Besoin d'un Expert ? contactez-vous

NOS FORMATIONS : <https://www.lenetexpert.fr/formations-cybercriminalite-protection-des-donnees-personnelles>
(Numéro formateur n°93 84 03041 84 (Autorisation de la Direction du travail de l'Emploi et de la Formation Professionnelle))



Denis JACOPINI est Expert Judiciaire en Informatique spécialisé en « Sécurité » « Cybercriminalité » et en protection des « Données à Caractère Personnel ».

- Audits Sécurité (ISO 27005) ;
- Expertises techniques et judiciaires (Avis techniques, Recherche de preuves téléphones, disques durs, e-mails, contentieux, détournements de clientèle...);
- Expertises de systèmes de vote électronique ;
- Formations et conférences en cybercriminalité ; (Autorisation de la DRTEF n°93 84 03041 84)
- Formation de C.I.L. (Correspondants Informatique et Libertés) ;
- Accompagnement à la mise en conformité CNIL de votre établissement.

Le Net Expert
INFORMATIQUE
Cybersécurité & Conformité

[Contactez-nous](#)



Réagissez à cet article

Source : *Cyberattaques: pourquoi s'assurer n'est pas la meilleure solution – Challenges.fr*