Comment s’assurer contre le cyber-risques ? | Le Net Expert Informatique

Comment s’assurer contre le cyber-risques ?

Diverses études montrent que les entreprises sont mal préparées pour lutter contre le hacking. Les grands assureurs affinent leurs stratégies commerciales.

Sony, Home Depot, JP Morgan, TV5 Monde, Target… Le nombre d'entreprises victimes de cybercriminalité explose. Mais les couvertures d'assurance contre ce type de méfait ne font qu'émerger. Les vols de données, espionnages et autres attaques de systèmes informatiques coûtent pourtant 300 à 1000 milliards de dollars, selon la société de sécurité informatique McAfee.
La Suisse n'est pas épargnée. Dernier exemple en date: Implenia. Selon une étude récente de l'Université de Saint-Gall (https://www.alexandria.unisg.ch/Projekte/238276), plus de 90% des entreprises ont été touchées par des attaques de hackers, l'année passée. «Les PME se sentent, à tort, à l'abri. Leur protection est insuffisante», juge son auteur, Martin Eling.
Elles semblent effectivement ne pas être préparées, comme en témoigne le sondage de KPMG auprès de 64 entreprises, présenté mercredi à la presse. Son auteur, Matthias Bossardt, parle d'un «cycle de complaisance». **Plus de la moitié des sociétés interrogées croient que leur organisation est capable de détecter des attaques. Mais 45% n'ont pas de plan pour y répondre**. Même si celles-ci ne cessent de se transformer, 79% des entreprises interrogées n'ont pas changé leurs plans, ces 12 derniers mois. 7% d'entre elles n'ont même pas pris de mesure, après une attaque.

En moyenne, 229 jours s'écoulent jusqu'à la mauvaise surprise
Les entreprises ne découvrent que fort tard qu'elles sont piratées. «**En moyenne, 229 jours s'écoulent jusqu'à la mauvaise surprise**», explique Manuel Meier, directeur général de la division entreprises pour Zurich Insurance. Sur le plan global, le coût du cyber-risque correspond à celui des catastrophes naturelles. Mais sa complexité est supérieure. L'incendie ou l'effraction sont plus aisés à localiser et immédiatement visibles. «La cybercriminalité, dont l'origine est souvent étrangère, change la façon d'appréhender un sinistre», analyse l'assureur.
Le thème s'est imposé aux Etats-Unis, où «un tiers des entreprises ont déjà signé un contrat de cyberassurance», affirme Manuel Meier. Le marché américain est estimé à 1,3 milliard de dollars en 2013 par le rapport «Betterley», contre 150 millions d'euros en Europe continentale.
«Le cyber-risque nous préoccupe surtout depuis cinq ans», précise Carin Gantenbein, responsable de ce risque au sein de Zurich Insurance. L'importance du cyber-risque s'est accrue fortement à la suite de l'«obligation de notification», soit le devoir d'annoncer quand une infraction s'est produite, fait valoir Manuel Meier. Le client qui a été frappé par une attaque doit être averti, par exemple si les informations contenues sur sa carte de crédit ont été violées. Aux Etats-Unis, l'entreprise est pénalisée par un risque de publicité et par un coût d'information qui peut atteindre «plusieurs douzaines de millions de francs», explique Carin Gantenbein, responsable de ce risque au sein de Zurich Insurance. Son bénéfice est réduit d'autant. Les entreprises suisses actives aux Etats-Unis, ou ayant un client américain, sont directement touchées si la filiale américaine l'est, parce que l'obligation d'annonce la touche immédiatement.
A l'origine, les entreprises parlaient de sécurité «informatique». Parce que c'est le département du même nom qui était en charge du sujet. Mais elles se sont aperçues que tout leur personnel était concerné et qu'il ne suffisait plus d'avoir un pare-feu ni de changer leurs mots de passe régulièrement.
Si le hacking s'est aussi vite répandu, c'est parce que presque tous les objets sont connectés à Internet, de la voiture à la maison, multipliant les opportunités de piratages. Les risques d'intrusion dans les systèmes informatiques dépassent les produits de consommation et frappent aussi les hôpitaux et leur responsabilité civile en cas de vol de documents.
Les assurances peuvent offrir leur service habituel de transfert de risque. Mais ce dernier ne va jamais couvrir l'ensemble des cyber-risques, même s'il contribue à la réduction des coûts économiques. «Les coûts juridiques d'une attaque sont énormes», observe Manuel Meier. Une grande partie de la couverture d'assurance se concentre sur ceux-ci. «Il arrive que la couverture d'assurance soit entièrement utilisée pour les risques juridiques et qu'il ne reste rien pour la responsabilité civile», fait valoir Carine Gantenbein. L'assurance paie les coûts d'annonce et de rétablissement des données ainsi que l'interruption d'activité. Mais elle ne couvre pas les conséquences d'un piratage, comme l'absence de transaction ou la perte de confiance. Les entreprises peuvent décider de couvrir elles-mêmes les cyber-risques dans une filiale dite «captive» ou faire appel à un réassureur. La définition du prix pose toutefois problème. Il manque encore un historique. «Les assureurs sont dans une phase d'essais et d'erreurs», analyse Manuel Meier.
En outre, les risques d'interruption d'activité conduisent à des estimations compliquées, puisque tout est interconnecté. «Les clients utilisent les mêmes nuages (clouds). Si l'un d'entre eux est attaqué, certaines entreprises ne peuvent plus livrer leurs produits», explique Zurich Insurance.

Si ce marché se situe avant tout aux Etats-Unis, en raison des coûts juridiques, il devrait s'étendre à l'Europe. L'Union européenne débat aussi de l'introduction du devoir d'obligation», indique Manuel Meier. Le temps à cet effet est réduit, sous peine de sanctions supplémentaires. L'UE pourrait mettre en œuvre cette obligation en 2016. La sanction atteindrait 5% du chiffre d'affaires ou jusqu'à 100 millions d'euros.

Le marché suisse de la cyberassurance est encore minuscule, selon l'étude de l'Université de Saint-Gall, réalisée sur mandat du courtier Kessler. Il s'élève à 5 millions de francs. Mais Martin Eling est d'avis qu'il devrait décupler en cinq ans. Dans le monde, le marché devrait quintupler pour s'élever à 10 milliards de dollars.

Les assureurs répondent à ces défis en offrant une combinaison de services de prévention (pare-feu, logiciels) et de protection. C'est une chasse gardée des grands groupes internationaux. Les acteurs actifs dans ce domaine sont AIG Europe Limited, Allianz Global Corporate & Specialty AG (AGCS), Chubb Insurance Company of Europe SE, Zurich et Axa Winterthur. Les grands groupes suisses doivent souvent signer des accords de partenariat. Axa Winterthur travaille par exemple avec Nexos AG, tandis que Zurich Insurance collabore avec Kudelski.

Axa Winterthur offre des mesures de préventions et de couverture de sinistres spécifiques. Dans le cas d'une perte de données, Axa assume la réinstallation du système d'exploitation et des programmes ainsi que la récupération des données. En cas de perte de chiffre d'affaires, à l'image d'une boutique en ligne dont le système est bloqué à la suite d'une attaque et indisponible pendant trois jours, l'assureur verse le manque à gagner, déduit de la franchise.

Auprès de Zurich Insurance, l'assurance cyber-risque est définie selon le principe des modules. La composante de base est toujours la responsabilité civile, laquelle peut s'accompagner de la récupération des données et des coûts d'annonce, s'il y a des clients américains et dès 2016 européens. Elle offre aussi la couverture du risque de chantage. Le prix dépend du nombre de données sensibles et de la branche. Une petite banque est bien plus chère qu'une PME industrielle. Le tarif d'une couverture correspond à 0,6% du chiffre d'affaires, mais des changements sont fréquents. Les statistiques sont encore insuffisantes.

Au sein des entreprises, le travail de sensibilisation intègre chaque employé, selon Carin Gantenbein. Les PME n'ont pas les moyens d'établir de tels processus. L'assureur offre à ses clients des conseillers pour les sinistres, la communication et l'analyse des processus.

Pour les personnes privées, il existe une assurance cybermobbing pour les privés. L'assureur se charge d'éliminer certaines histoires répandues sur le Web. Un privé n'obtiendra pas satisfaction s'il téléphone à Google pour changer un site, explique Manuel Meier.

Et dans cinq ans? Si l'obligation de notification est introduite dans l'Union européenne, la Suisse suivra, promet le directeur de Zurich Insurance. Le marché en deviendra plus transparent. On en parlera davantage, la perception sera supérieure. Et l'offre d'assurance sera élargie.

Source : http://www.letemps.ch/Page/Uuid/01ccdc38-f4e7-11e4-bb1f-074820583190/Les_solutions_des_assureurs_face_au_cyber-risques
Par Emmanuel Garessus