« La cyber-assurance devient une priorité pour les dirigeants d’entreprise »

	« La cyber-assurance devient une priorité pour les dirigeants d’entreprise »

Face à la recrudescence de la cybercriminalité, les dirigeants de PME et ETI s'interrogent de plus en plus sur ces nouveaux risques et la façon de s'en protéger. Le point avec Philippe Gaillard, directeur des Risques Techniques chez Axa Entreprises.

Qu'est-ce-que le cyber-risque aujourd'hui ? Comment -a-t-il évolué ces dix dernières années ?
Le cyber-risque prend de plus de plus de place dans notre quotidien. Pourtant les cyber- attaques et virus au sens large ne sont pas vraiment nouveaux. Jusqu'aux années 2000, les cyber-attaques étaient principalement des virus ou des vers informatiques qui étaient le résultat d'une sorte de compétition entre jeunes prodiges de l'informatique qui tentaient de pénétrer des systèmes prestigieux connus pour être inviolables. Autour des années 2005, les cyber-attaques ont évolué et se sont dirigées vers les Etats et les défenses nationales. Depuis 2010, on observe une recrudescence de ces attaques. Elles sont de plus en plus complexes, et prennent des formes de plus en plus variées. On commence à voir de l'espionnage industriel, des attaques entre concurrents, de l'extorsion et de la fraude. C'est toute cette évolution qui fait que les entreprises, quelle que soit leur taille, sont victimes de plus en plus de cyber-attaques. En cinq ans, la cybercriminalité s'est accélérée en nombre, et transformée en complexité et en variété d'objectifs.

Quels sont les cyber-attaques le plus souvent répertoriées ?
Il existe trois grandes catégories de cyber-attaques.
Le sabotage, qui peut soit être une vengeance envers un tiers, soit une compétition entre sociétés mal intentionnées à l'instar de ce qui pouvait donner lieu autrefois à un incendie volontaire de la part d'un mauvais concurrent.
Seconde catégorie, l'espionnage, qui consiste à aller chercher de l'information dans les autres entreprises, que ce soit de l'information commerciale ou technologique. Dans ce cas, ce sont les directions générales et les équipe de R&D qui sont les plus ciblées.
Troisième catégorie : la criminalité ou la piraterie qui consistent à voler des données ou à paralyser un système en espérant avoir une rançon en échange. Il est important de savoir que ces cyber-attaques agissent dans la durée. D'abord, elles se préparent longtemps à l'avance, car lorsqu'il s'agit d'espionnage par exemple, les criminels doivent commencer par chercher à comprendre la culture et les points sensibles de l'entreprise qu'ils visent. A la suite de cela, ils injectent un logiciel malveillant dans le système informatique de l'entreprise et le font évoluer pour se rapprocher progressivement de la cible finale. Entre le moment où se font les premières intrusions dans l'entreprise et le moment où est découverte cette action malveillante, il se passe bien souvent un an, voire plus.

Pouvez-vous nous donner un exemple type de cyber-attaque ?
Aujourd'hui, la plupart des comités de direction des grandes entreprises sont sur le réseau Linkedin. La technique utilisée par un cybercriminel pour pénétrer dans le système de l'entreprise est assez simple. Il repère des personnes qui travaillent sur un sujet sur lequel il y a eu un séminaire par exemple ; il envoie un mail piégé aux personnes susceptibles d'avoir été présentes à ce séminaire en leur faisant croire qu'il y participait également. Dans ce mail, il y a une pièce jointe qui annonce par exemple un compte rendu du séminaire. De fait, parmi les personnes réceptionnaires de cet email, il y a en a qui ont réellement participé à ce séminaire. Pour ceux et celles qui ouvrent la pièce jointe, le virus pénètre aussitôt dans leur système informatique. Le mal est fait. Le virus paralyse ensuite l'ordinateur de la personne qui aura ouvert la pièce jointe ; ladite personne appelle alors son help desk, qui bien souvent intervient à distance sur les ordinateurs. Pour prendre la main, l'expert informatique en charge de réparer l'ordinateur saisit le mot de passe administrateur. Il est aussitôt enregistré par le virus qui peut ensuite, tout doucement, progresser dans le système informatique de l'entreprise ciblée jusqu'à parvenir par exemple au serveur de la direction générale ou celui de la R&D.

Comment réagissent les dirigeants de PME-PMI face à la cybercriminalité ?
Il y a encore deux ans, les dirigeants de PME-PMI ne s'inquiétaient pas vraiment des cyber-attaques. Mais depuis douze mois, face aux dernières attaques médiatiques qu'ont pu connaître de grands groupes, l'inquiétude est en train de monter fortement. Selon notre dernier baromètre de juin 2014, sur 500 chefs d'entreprises interviewés, 46% placent le cyber-risque parmi leurs préoccupations majeures. Ce qui était un quasi non sujet il y a encore un an tend à devenir une priorité. D'autant plus que les PME et ETI sont mal protégées et donc deviennent des cibles très vulnérables. Par ailleurs, elles peuvent être des sous-traitants de grosses entreprises et par conséquent être une porte d'entrée pour les cybercriminels qui visent ces grands groupes.

Comment les entreprises peuvent-elle se protéger des cyber-attaques ?
Une bonne protection doit être équilibrée et reposer sur trois piliers. Le premier, c'est bien évidemment la technologie pour empêcher les virus de pénétrer les systèmes informatiques, pour les détecter et les traiter. Cela est nécessaire mais totalement insuffisant ! Le second, c'est l'information et la formation des salariés. Il est primordial de sensibiliser les collaborateurs aux bonnes pratiques afin d'éviter les comportements qui mettent l'entreprise en danger. En troisième lieu, il faut travailler sur la résilience de l'entreprise pour limiter les effets d'une possible attaque notamment en anticipant les capacités de rebond et de continuité d'activité. Les entreprises doivent admettre que, quoi qu'elles fassent, elles peuvent être attaquées. A l'instar d'une porte blindée, si un voleur veut pénétrer dans les lieux, et qu'il peut y mettre les moyens, il finira bien par entrer. Donc, partant du principe que toute entreprise sera attaquée à un moment ou un autre, il est important de proposer des solutions qui aident l'entreprise à limiter les dégâts et redémarrer au plus vite.

Existe-t-il des assurances qui protègent les entreprises de la cybercriminalité ?
Axa Entreprises est l'assureur d'une PME sur trois en France ; nous mettons un point d'honneur à les accompagner pour répondre à leurs besoins. Face aux cyber-risques, nous avons conclu un partenariat avec le département cyber sécurité du Groupe Airbus, qui est la référence dans le domaine.
Pour les ETI et les grandes entreprises, nous proposons de réaliser un audit de risques, mené par un ingénieur d'Axa et un ingénieur d'Airbus qui interviennent en binôme. Cet audit donne lieu à un diagnostique complet de la situation de l'entreprise face aux cyber-risques. Sur cette base, en fonction des situations, nous pouvons proposer une solution d'assurance qui combine deux volets complètement imbriqués : un contrat d'assurance qui couvre toutes les conséquences des cyber-attaques ainsi qu'un accompagnement dans le temps en ingénierie pour aider l'entreprise à maitriser son risque cyber et à l'améliorer.
Pour les PME, nous avons élaboré une approche simplifiée. Aussi bâtie en collaboration avec l'expertise du groupe Airbus, cette approche repose sur un questionnaire très simple, accessible à tous. A partir des réponses à ce questionnaire, nous pouvons réaliser une mesure du risque cyber et ainsi proposer une offre d'assurance avec des garanties et un tarif adaptés. Sur cette même base un diagnostic cyber est remis au client d'AXA Entreprises pour l'accompagner dans ses actions de prévention contre les risques cyber. Les PME ayant rarement les contacts nécessaires, se trouvent bien souvent démunies quand survient un sinistre cyber. Par conséquent, au-delà des garanties de dommage, de responsabilité civile, de protection des données personnelles et d'accompagnement à la gestion de crise, la valeur de l'offre d'assurance réside beaucoup dans sa capacité à proposer un accompagnement global de proximité de l'entreprise, en amont et en aval, avec des services pragmatiques, rassurants et réactifs.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source :
http://www.latribune.fr/loisirs/la-tribune-now/20150128tribd355efe7a/la-cyber-assurance-devient-une-priorite-pour-les-dirigeants-d-entreprise.html