Cloud computing : bien assurer les cyber-risques

0

13 Jan 2016 cloud, cyber risques, cyberassurance, données by Aurelie Magniez

Trop d'entreprises ne prêtent pas suffisamment attention aux garanties dont elles disposent réellement dans leur contrat d'assurance en cas d'atteinte à leur système d'information. Particulièrement en cas d'usage de services dans le cloud, les déconvenues après survenance d'un sinistre peuvent être importantes : pas de garantie en cas de simple perte de données, sur les conséquences d'une contrefaçon ou d'un contrôle de la Cnil et encore moins sur la gestion de la E-réputation. Voici un focus des 5 garanties à sécuriser dans un contrat d'assurance.

1. Disposer d'une garantie adéquate sur ses données

Assurance et donnée

Dans un contrat d'assurance standard, il n'est pas rare de lire que les dommages immatériels non consécutifs à un dommage matériel ou corporel ne sont pas couverts. Or, la plupart des pertes ou altérations de données dans un système informatique résultent d'une défaillance du système en lui-même ou de l'effet d'un « malware » (virus, troyen…). Il est donc primordial que les dommages immatériels non consécutifs rentrent dans le périmètre des garanties. Il faut aussi s'assurer que le contrat d'assurance ne prévoit pas des obligations trop lourdes à la charge du client lui-même en termes de sauvegarde des données. Alors que le cloud computing a pour principal avantage d'externaliser la donnée chez un tiers, lui-même responsable d'assurer un back-up, il serait incohérent d'avoir un contrat d'assurance exigeant une sauvegarde des données chez le client lui-même ou par lui-même.

Données personnelles

Les données personnelles constituent une valeur clé du fonds de commerce de toutes les entreprises. Suite à une faille de sécurité ou une fraude informatique, des données risquent d'être altérées ou communiquées à des tiers. Il peut en résulter des sanctions administratives ou pénales au titre de la législation informatique et libertés. A ce titre, les assureurs ne couvrent que très rarement un tel risque. En revanche, au titre des réclamations des personnes physiques concernées, l'assureur devrait proposer des solutions. Avec l'adoption d'une réglementation européenne uniforme, l'obligation de déclaration de telles failles va être obligatoire auprès de l'office compétent (en France, la Cnil) et des personnes ciblées. Ce sujet est donc à anticiper avec son assureur.

Données contrefaisantes

Dans les contrats pour un cloud public (contrat généralement d'adhésion donc non négociable), il est de plus en

plus souvent prévu une clause prévoyant la responsabilité du client auprès du prestataire sur les données qu'il héberge. Le risque le plus important porte sur les données susceptibles d'être la contrefaçon d'une œuvre protégée. Puisque le risque existe et qu'il n'est pas toujours limité dans son montant, l'assureur doit pouvoir proposer une solution.

2. Disposer d'une garantie adéquate sur ses logiciels et applications

Lorsque le contrat cyber-risque couvre bien les données, une autre déconvenue peut intervenir sur les logiciels et applications. Lorsqu'ils se trouvent atteints ou corrompus dans leur fonctionnement, ils ne rentrent pas toujours dans le champ des garanties. Les frais de réinstallation ou même de nouvelle acquisition du logiciel seraient donc à la charge exclusive de l'assuré, ce qui peut apparaître ici aussi comme un comble, dans le cadre d'une offre SaaS dans le cloud. L'espoir de l'assuré serait éventuellement de pouvoir faire jouer l'assurance responsabilité civile de son prestataire, mais il vaut mieux être couvert par son propre assureur que celui des autres…

3. Disposer d'une garantie en cas d'interruption du réseau ou des télécommunications

Beaucoup de contrats d'assurance excluent toute garantie en cas de sinistre résultant d'un dommage indirect. Dans le cloud, tel est le cas typique d'une perte de chiffre d'affaires ou de bénéfices liée à l'interruption des télécommunications. Même si les télécommunications ont fait de grands progrès techniques, le crash du réseau de tout un opérateur n'est pas un cas d'école et le client du service web est alors dans un état de vulnérabilité fort. Ce point doit trouver une réponse dans le contrat d'assurance.

4. Disposer d'une garantie sur le matériel de ses collaborateurs lorsque le BYOD est autorisé

Si l'entreprise accepte que ses collaborateurs accèdent à ses applications métiers dans le cloud, directement à partir de son terminal personnel (BYOD), la sécurité d'un système d'information s'appréciant par rapport à son maillon le plus faible, le terminal d'un particulier sera très probablement très vulnérable et c'est l'ensemble du système d'information de l'entreprise qui le devient par ce biais. Si des solutions techniques pour sécuriser aussi les connexions depuis un terminal personnel (double mot de passe par exemple) existent, beaucoup d'assurances cyber-risques écartent purement et simplement toute couverture des terminaux personnels des salariés. Ce point dont donc être abordé avec son assureur, le cas échéant.

5. Disposer d'une assurance pour sa e-réputation

Une faille de sécurité informatique peut fragiliser une entreprise et dégrader son image auprès du public lorsque des bloggeurs avertis ou journalistes s'en font l'écho dans les réseaux sociaux et autres média. C'est pourquoi, l'assureur doit aussi couvrir ce risque en proposant la mise en place d'une cellule de gestion de crise avec intervention de professionnels de l'e-réputation.

Le contrat d'assurance idéal n'existe pas. Certains risques, non évoqués ici, sont considérés comme non assurables sur le marché (exemple des pénalités de retard sur l'implémentation d'une solution SaaS). Cependant, l'entreprise, après avoir dressé une cartographie des risques la concernant avec appréciation de leur criticité, peut alors plus efficacement négocier avec son assureur. A ce titre, l'intervention d'un courtier spécialisé peut s'avérer d'autant plus pertinente qu'il peut soumettre aux assureurs des polices spécifiques.

Eric Le Quellenec
Directeur du département Informatique conseil

Alain Bensoussan-Avocats est un cabinet d'avocat entièrement dédié au droit des technologies avancées depuis 1978. Pour la 5e année consécutive depuis 2010, il a été distingué par ses pairs, « Best Lawyer » de l'année en « Droit des Technologies ».
Site : **http://www.alain-bensoussan.com/**