Cédric MERMILLOD
Directeur commercial et co-fondateur d'Oodrive

> *« Le développement du nomadisme qui entraîne le besoin de solutions de sauvegarde adaptées »*

diversité des supports et des environnements utilisés est venue apporter de la complexité, d'autant plus lorsqu'il s'agit de supports personnels relevant des pratiques BYOD », poursuit-il. Dans ce contexte, *« il faut amener l'utilisateur à comprendre que les solutions* Cloud *qu'il utilise à titre personnel ne sont pas forcément adaptées à un usage professionnel pour plusieurs raisons, et notamment celles liées à la sécurité »*, précise Cédric Mermillod. La solution répressive serait de bannir purement et simplement la pratique du BYOD au sein de l'entreprise, avec le risque que les collaborateurs n'utilisent pas suffisamment les outils de la mobilité imposés par l'entreprise. Une autre piste consiste alors à créer, en quelque sorte, une culture et un environnement technique permettant aux utilisateurs d'apporter leur matériel tout en étant dans les règles définies par l'entreprise sur le plan des usages comme de la sécurité. *« Comme nous sommes également un éditeur de logiciels, nous faisons en sorte de mettre à disposition des collaborateurs des solutions* Cloud *qui leur rappellent celles qu'ils utilisent à titre personnel, mais qui ont l'avantage d'être parfaitement sûres pour l'entreprise, notamment parce qu'il s'agit de Cloud privé »*, conclut Cédric Mermillod. Du coup, les solutions grand public se trouvent naturellement marginalisées, au profit des applications professionnelles, bien plus sûres.
Une manière habile de joindre l'utile à l'agréable, en toute sécurité. Le BYOD peut même se révéler comme une bonne solution pour laisser les employés travailler de façon plus productive ! ■

Laurent LOCURCIO

La prévention du risque juridique lié à la sécurité de l'entreprise numérique

Isabelle RENARD
Avocat et ingénieur

> *« Le risque informatique doit être partagé entre le prestataire et le client »*

La sécurité n'est plus une assurance contre le risque mais une garantie pour la pérennité et l'intégrité de votre entreprise. Il convient donc de prévenir les risques inhérents à la gestion des données, la sécurité de votre entreprise étant le garant de vos profits !

Plus que jamais donc le dirigeant d'entreprise doit faire face, en matière de sécurité, aux risques de perte de ses informations : celles-ci constituent maintenant un véritable patrimoine, et parfois même le seul, de l'entreprise ! L'insécurité informatique est donc un risque majeur qui peut conduire à une perte de profits conséquente, voire même à une crise sans précédent ! Les dirigeants d'entreprise doivent en prendre conscience et tenir compte des vulnérabilités de leur système d'informations face aux menaces de cyberattaques, de vol ou d'extraction, par des tiers, de leurs données ainsi que des contraintes légales et réglementaires.

© M. Rabbiosi - Fotolia

Est-ce possible de prévenir juridiquement ces risques informatiques ?

Au préalable, il ne faut pas oublier que le client n'est pas un professionnel de l'informatique. *« Si le client n'est pas conseillé par un spécialiste, il ne remarquera pas les pièges d'un contrat dont le modèle est souvent proposé par le fournisseur. Il est souhaitable qu'il se fasse assister par un professionnel, avocat et/ou société de conseil qui connaisse bien le sujet et ait une expérience de terrain des difficultés qui peuvent se poser lors de l'exécution de ce type de contrat »*, précise Isabelle Renard, avocat et ingénieur.
Certaines clauses sont essentielles et doivent absolument être intégrées au contrat. *« Il convient de vérifier que les niveaux de sécurité proposés par l'hébergeur sont en adéquation avec la sensibilité pour l'entreprise des données et applications concernées. La protection est-elle suffisante : le client peut-il effectuer des tests d'intrusion pour le vérifier ? La clause d'audit est indispensable pour les prestations d'hébergement de haut niveau, car elle permet au client de s'assurer que ses exigences sont respectées, telles que la protection physique des appareils, ou la non mutualisation des serveurs. Cependant, il ne faut pas confondre le prestataire hébergeur avec l'assureur du client. Le risque informatique doit être partagé entre le prestataire et le client, qui doit impérativement mettre en place un plan de continuité d'activité qui se déclenchera en cas d'incident grave et évitera de subir des pertes d'exploitation trop lourdes »*, poursuit Isabelle Renard.

Quelle responsabilité et quelles sanctions pour l'hébergeur ?

Fabrice Naftalski, membre de l'AFAI associé EY, avocat spécialisé en droit des TIC, explique que

Trois questions à

Matthieu Bourgeois, avocat, associé, spécialiste en droit des nouvelles technologies de l'informatique et de la communication de KGA Avocats et à Amira Bounedjoum, juriste, élève-avocat de KGA Avocats

GPO Magazine : Les cyberattaques sont-elles la crainte n°1 des entreprises en matière de sécurité informatique ? Comment ont évolué dans le temps ces attaques ?

> Les cyberattaques représentent l'une des formes de criminalité qui connaît le taux de croissance le plus fort. Entre 2012 et 2013, les cyberattaques ont doublé[1] et en 2013, 93 % des entreprises françaises de plus de 250 salariés en ont été victimes. L'impact pour les entreprises victimes de ces attaques se traduit tant financièrement (pertes d'exploitation en raison de l'arrêt du service informatique, frais d'investigation et d'investissement pour le rétablissement de la sécurité du système...) qu'en termes d'image. À titre d'exemple, l'attaque subie par la société Orange et sa condamnation[2] récente pour défaut de sécurité des données, relayée par plusieurs médias, ont été très nocives pour l'image de cette entreprise. La multiplication des attaques et les préjudices considérables qui en découlent en font un risque majeur pour toute entreprise.

GPO Magazine : De quelle manière les entreprises, notamment les PME, peuvent-elles se protéger juridiquement face aux cyberattaques ?

> Contre les cyberattaques, les entreprises, doivent se protéger sur le plan technique et juridique.
Sur le plan technique, il est fortement recommandé aux entreprises de mettre en place notamment une politique d'habilitation d'accès au Système d'Information (SI), d'authentifier chaque utilisateur de l'entreprise et de sécuriser tous les postes de travail, notamment par des antivirus performants, activés et mis à jour. Le réseau informatique de l'entreprise doit également être sécurisé *via*, par exemple, une limitation des flux réseaux et un chiffrement des communications. Sur le plan juridique, tout accès/intervention sur le SI de l'entreprise doit donner lieu à la formalisation d'un contrat indiquant les limites de l'habilitation d'accès conférée. Des accords de confidentialité peuvent également être signés par le personnel de l'entreprise mais aussi par tout prestataire externe.
Des services spécialisés de la justice, tels que la Brigade d'enquête sur les fraudes aux technologies de l'information (BEFTI) ou l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) assistent les entreprises victimes de cyberattaques et coordonnent les enquêtes de la police.

GPO Magazine : Faut-il faire de la prévention dans ce domaine?

> Absolument ! Il convient de rappeler que les entreprises, même victimes d'attaques virtuelles, demeurent responsables de leurs données. La majorité des cyberattaques étant internes aux entreprises, une sensibilisation dans ce domaine est indispensable. Cette sensibilisation peut prendre la forme de chartes éthiques et informatiques qui, lorsqu'elles sont déployées comme un règlement intérieur, ont une force contraignante. La prévention passe également par la réalisation d'audits de sécurité. ■

1. Selon l'étude menée par Iron Mountain et Pwc sur la gestion des risques de l'information dans les entreprises
2. Délibération de la formation restreinte de la Cnil n°2014-298 du 7 août 2014 prononçant un avertissement à l'encontre de la société Orange

« *plusieurs cas peuvent se présenter dans lesquels la responsabilité de l'hébergeur peut être relevée, étant précisé en synthèse que depuis la transposition en droit français de la directive concernant le commerce électronique du 8 juin 2000 (par la loi pour la confiance dans l'économie numérique du 21 juin 2004), l'hébergeur n'a pas d'obligation générale de surveillance des contenus hébergés en dehors des hypothèses très spécifiques visant des infractions d'une extrême gravité* ».

Le principe de responsabilité de l'hébergeur est posé par l'article 6-3 de la loi pour la confiance dans l'économie numérique du 21 juin 2004 qui dispose que les personnes physiques ou morales qui assurent, même à titre gratuit, pour mise à disposition du public par des services de communication au public en ligne, le stockage de signaux, d'écrits, d'images, de sons ou de messages de toute nature fournis par des destinataires de ces services ne peuvent pas voir leur responsabilité civile engagée du fait des activités ou des informations stockées à la demande d'un destinataire de ces services si elles n'avaient pas effectivement connaissance de leur caractère illicite ou de faits et circonstances faisant apparaître ce caractère ou si, dès le moment où elles en ont eu cette connaissance, elles ont agi promptement pour retirer ces données ou en rendre l'accès impossible. ■

Fabrice NAFTALSKI
Avocat spécialisé en droit des TIC, membre de l'AFAI associé EY

« L'hébergeur n'a pas d'obligation générale de surveillance des contenus hébergés [...] »

Linda DUCRET