

LE TEMPS

L'invité Mercredi 10 février 2010

La sécurité informatique et le secret bancaire?

Par Jerry Krattiger *

Une bonne gouvernance implique que les gestionnaires de bases de données n'ont pas à avoir accès au contenu des bases de données qu'ils gèrent.

Le cas d'Hervé Falciani, cadre informaticien de HSBC qui a remis aux autorités françaises des données sur les clients de cette banque privée basée à Genève, est intéressant car il force à se préoccuper de sécurité informatique et à réfléchir à la manière de gérer les risques informatiques. Le malaise est encore alimenté par la décision récente du gouvernement allemand, cautionnée par Angela Merkel, d'acheter des CD contenant plusieurs milliers de noms de clients de banques suisses. Ces deux affaires montrent clairement la vulnérabilité des entreprises et placent la sécurité informatique non plus à un niveau purement technique, mais à un niveau stratégique de gouvernance d'entreprise. La sécurité informatique devient un élément clef de la réduction des risques et les manquements au contrôle d'accès à l'information digitale représentent un danger considérable pour toutes les entreprises.

Malheureusement, il faut souvent un sinistre conséquent, pouvant atteindre des sommes faramineuses, sans compter les dégâts d'image, pour que les organisations prennent conscience de leur vulnérabilité et mettent en place des solutions de gestion des rôles, de gestion des identités et des accès ou de chiffrements. Plus que jamais, les secrets d'affaires, la propriété intellectuelle et les données sur les clients sont des avantages concurrentiels, il est de la responsabilité et de l'intérêt des organisations de mettre tout en œuvre pour s'assurer du respect de la confidentialité de ces données et de protéger ses avantages compétitifs digitalisés.

Le cas encore embrouillé de HSBC et divers autres «accidents» spectaculaires et évitables doivent attirer l'attention des managers. En 2008 déjà, le fisc allemand avait acheté des données clients d'une banque du Liechtenstein à un gestionnaire de base de données. Les problèmes auxquels la Société Générale s'est trouvée confrontée à la suite de l'affaire Kerviel donnent un exemple des plus spectaculaires où le fait d'oublier d'enlever les droits d'accès d'un employé à la suite d'un changement de fonction au sein de l'organisation (du back-office au trading) a manqué de provoquer la faillite d'une des banques les plus prestigieuses de l'Hexagone. Ces événements représentent des manquements graves de sécurité et sont inexcusables car évitables.

De ces cas connus, on peut tirer quelques constats:

Une grande partie des dégâts informatiques sont le fait d'employés désabusés ou indécidés ou sont provoqués par inadvertance.

L'informatique reste pour beaucoup de dirigeants d'entreprises, de conseils d'administration et de managers un monde hermétique.

La surveillance et le contrôle des informaticiens est un élément important de la gestion des risques.

La quantité de données qui peuvent être stockées sur des clefs USB ou des ordinateurs portables est aujourd'hui telle que les entreprises maîtrisent difficilement leurs flux de données.

Une gestion des risques et une sécurité informatique effectives sont aussi une nécessité pour assurer la conformité légale. A partir de 2009, l'article 729 du Code des obligations exige la mise en place d'un système de contrôle interne. Cette législation requiert des entreprises un meilleur contrôle de leurs risques informatiques par le biais d'une traçabilité, c'est-à-dire que les entreprises devront pouvoir dire qui fait quoi et quand dans leurs systèmes informatiques et surtout si tel employé est autorisé à avoir accès à ces données. A ce jour, peu d'entreprises ont une gestion structurée des rôles et des droits d'accès permettant ce genre de traçabilité.

Certes, les entreprises sont relativement bien protégées contre les attaques venant de l'extérieur. Les fuites de données venant de l'intérieur sont en revanche moins contrôlées et c'est justement à l'interne que se passent 70% des sinistres. Pourtant il existe des solutions qui permettent la gestion des rôles, la gestion des identités et accès ou le chiffrement des données. Ces garde-fous apportent une meilleure sécurité interne. Ces solutions peuvent être mises en place de différentes façons et combinées de sorte à avoir plusieurs couches de sécurité qui se complètent l'une l'autre. Ainsi, pour une gestion adéquate, les clefs de chiffrement doivent être réparties sur deux personnes distinctes.

A cela s'ajoute la nécessité de mettre en place une gouvernance informatique comprenant une séparation des droits pour les utilisateurs et les informaticiens. Il faut distinguer la réglementation, qui définit les politiques de sécurité et les contrôles, de la mise en œuvre de ces politiques. Concrètement, cela veut aussi dire que les gestionnaires de bases de données n'ont pas à avoir accès au contenu des bases de données qu'ils gèrent et que ces données doivent être compartimentées et rendues anonymes. Il est clair que la loyauté des employés reste le maillon faible de la sécurité des entreprises, mais il est du devoir des entreprises de ne pas laisser les «portes» de leurs systèmes grandes ouvertes pour qu'un collaborateur indélicat se serve. Si ces occasions sont rendues plus difficiles par la mise en place de solutions techniques effectives, les entreprises auront rempli leur devoir de diligence.

Nous vivons dans un monde digitalisé et virtualisé. L'utilisation effective de l'information est en passe de devenir un avantage compétitif de la même façon que le secret bancaire représente, encore, un avantage compétitif pour la place financière suisse. La situation de faiblesse dans laquelle le gouvernement suisse semble se trouver est telle que l'on peut même envisager l'éventualité d'un bluff de la part du gouvernement allemand afin de déstabiliser la place financière helvétique, inciter un grand nombre de fraudeurs à s'auto-dénoncer et prendre le secret bancaire d'assaut. La brèche semble être ouverte, la Suisse réussira-t-elle à défendre ses intérêts nationaux et protéger un des avantages concurrentiels de sa place financière?

LE TEMPS © 2009 Le Temps SA