

L'ACTUALITÉ S'EST FAIT L'ÉCHO CES DERNIERS TEMPS DE PLUSIEURS AFFAIRES OÙ DES DONNÉES "SENSIBLES" ONT ÉTÉ SUBLISÉES ET SE SONT RETROUVÉES EN DES MAINS AUXQUELLES ELLES N'ÉTAIENT PAS DESTINÉES.

Le défi des entreprises sur la protection des données

Ces affaires sont intéressantes car elles forcent à se préoccuper de la sécurité des informations et de la protection des données (SIPD). Les entreprises sont, la plupart du temps, ignorantes sur les dangers encourus, au mieux démunies contre les risques potentiels et il faut souvent un sinistre conséquent, pouvant atteindre des sommes faramineuses, sans compter les dégâts d'image, pour que celles-ci réalisent leur vulnérabilité et mettent en place des solutions adéquates, car des solutions existent, au même titre que la sécurité physique.

Mais quelles sont les raisons de ces pertes de données, qui occasionnent tant de dégâts ? Des cas connus, on peut en tirer quelques constats :

- Une grande partie des pertes informatiques sont le fait d'employés désabusés ou indéclicats, ou sont provoquées 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 telle que les entreprises maîtrisent difficilement leurs flux de données.

Curieusement, si l'on interroge les entre-



preneurs, ils se disent bien protégés et très souvent dépensent énormément d'argent pour se garantir d'attaques extérieures ; mais comme l'ont montré de récentes affaires, le danger vient de l'intérieur et ces risques-là sont nettement moins bien contrôlés. À cela, plusieurs raisons ; la première étant que l'on ne contrôle bien que ce que l'on connaît, et sur ce point, les chefs d'entreprises sont complètement dépen-

dants des rapports de leur responsable informatique. La deuxième étant que très souvent, ces mêmes dirigeants sont résignés : c'est normal qu'un administrateur système puisse accéder à toutes les données !

Or, rien de plus faux à cela. Un administrateur système est chargé de s'assurer du bon fonctionnement du système, non de la

conseil d'administration. Le rôle des administrateurs et de veiller entre autres à la bonne marche des affaires d'une entreprise et la propriété intellectuelle en fait partie intégrante. Mais là-aussi, comment contrôler ce que l'on ne maîtrise pas bien ? Combien d'informaticiens font partie d'un conseil d'administration ? Comment vérifier qu'un administrateur de bases de données ne soit pas aussi responsable de la sécurité informatique ? Quels moyens sont mis à disposition des chefs de département pour qu'ils puissent en temps réel vérifier qui a accès aux données du département ? Finalement, pour les domaines les plus sensibles tels que rapports financiers, services juridiques, recherche et développement ou liste des clients, quels moyens préventifs sont mis en place pour prévenir en temps réel d'une intrusion interne (l'attribution d'un accès auquel on n'a pas droit) ?

Rares sont les entreprises qui peuvent y répondre par l'affirmative. Ce genre de gouvernance n'est pas une panacée mais il autorise une réduction des risques internes liés à l'informatique car il permet de séparer le législatif de l'exécutif, séparer ceux qui définissent les politiques de sécurité et ceux qui doivent les mettre en œuvre.

L'enjeu économique est énorme car de nos jours, tout est numérisé et donc copiable, téléchargeable, appropriable en quelques secondes et les dommages en résultant peuvent aller de la simple "perte d'image", à une baisse de la compétitivité, un lancement de produit raté voire la fermeture pure et simple de l'entreprise.

Il est clair que la loyauté des employés reste le maillon faible de la sécurité des entreprises (personne ne pourra empêcher un employé de mémoriser cinq adresses de clients par jour et de les recopier chez soi le soir), mais il est du devoir de celles-ci de ne pas laisser les "portes" de leurs systèmes grandes ouvertes pour qu'un employé indéclicat se serve. L'occasion fait le larron et si ces occasions sont rendues plus difficiles par la mise en place de solutions techniques effectives, les entreprises auront rempli leur devoir de diligence. ♦

vérification du contenu. Pour utiliser une métaphore plus parlante, votre garagiste n'a pas à ouvrir les valises que vous avez mises dans le coffre, pour réviser votre véhicule.

Les solutions existent et se situent d'abord dans la gouvernance d'entreprise : gestion des rôles, gestion des identités et des accès aux données, chiffrement des données, séparation des pouvoirs (on ne peut donner un ordre et l'autoriser) ; ce sont des garde-fous qui apportent une meilleure sécurité interne.

À cela s'ajoute l'implication directe du



Didier Assandri