Du système d'information en circuit fermé au nuage informatique : l'évolution des enjeux et des risques, les réponses à inventer. (CCI Limoges - 02/02/2010)

Les systèmes d'information sont hébergés, pour l'essentiel, dans des entités aux limites bien définies : entreprises, administrations, organismes divers. Dans ce genre de contexte, les menaces à envisager sont de deux ordres : l'atteinte à l'intégrité ou à la confidentialité des informations et l'altération des moyens d'y accéder. Un certain nombre de moyens techniques et des modes de manipulation des individus peuvent être mis à l'œuvre pour y parvenir. Les défenses passent classiquement par une formation des utilisateurs, la surveillance de l'activité des systèmes, la maîtrise des flux en entrée et en sortie et la mise en place d'une politique de maintien des outils et méthodes de sécurisation employés

Avec la diffusion massive d'Internet et la baisse du cout des matériels il est devenu possible de déporter des traitements vers des sous-ensembles de ces organisations principales et de connecter aux systèmes d'information toute sorte de matériels nomades, de l'ordinateur portable au téléphone multifonctions. Les systèmes d'information ont donc du ouvrir leurs accès de plus en plus largement à des utilisateurs et des matériels ne respectant pas nécessairement les critères de sécurité requis. Face à ces menaces potentielles, il devient nécessaire de mettre en œuvre des protocoles d'authentification robustes des personnes et des matériels, une sécurisation des transmissions ainsi que des procédures de contrôle de la conformité des accès avec des normes de sécurité préétablies. Sur ce dernier point, l'idéal est de proposer des procédures automatiques de mise à niveau du matériel permettant d'éviter, si possible, de bloquer l'utilisateur (mise à jour du système d'antivirus, installation de correctifs de sécurité…)

Face à la croissance de la demande en matière de stockage et de traitement de l'information, de nouveaux enjeux sont apparus : augmenter sans cesse les espaces de stockage, mettre en œuvre des matériels toujours plus puissants, gérer des traitements sans cesse plus complexes ; le tout devant s'accompagner d'une fiabilité maximale. Ces demandes, dans un modèle classique, impliquent évidemment une augmentation des investissements en matériels et en locaux ainsi que la mise en place de systèmes de sécurisation et de supervision complexes. Parfois, ces équipements ne sont utilisés à leur pleine capacité que durant un temps très court.

Une des solutions semble résider dans l'externalisation et la mutualisation des données et des traitements dans de vastes centres de calcul (Cloud Computing). Dans cette optique, les capacités de stockage deviennent quasi-illimitées à l'échelle d'une entreprise. Les serveurs effectuant les traitements peuvent être virtualisés et donc déplacés ou remplacés instantanément au gré des besoins. Les logiciels ou les composants métiers peuvent également être fournis prêts à l'emploi et utilisés à distance moyennant un abonnement.

L'entreprise n'est donc plus menacée par une saturation de ses ressources, d'une panne d'un ou plusieurs de ses matériels, ou d'un dépassement de ses capacités de traitement, tous ces facteurs pouvant être ajustés dynamiquement en fonction de données d'infogérance.

Par contre, les lieux de traitement et de stockage, l'aire de communication des informations qui, parfois se limitaient à un bureau, vont peu à peu évoluer vers un étalement couvrant la planète, et ce, quelque soit la taille des entreprise. La sécurité et l'accessibilité des informations vont donc dépendre de multiples facteurs géopolitiques ainsi que de la qualité et de la compétence des prestataires choisis. Par ailleurs un grand nombre de problèmes juridiques peuvent surgir.

Pour répondre à ces menaces, plusieurs pistes s'offrent : conception raisonnée des architectures informatiques, élaboration de normes et de législations internationales adéquates, formation des utilisateurs, classification et cloisonnement des informations en fonction de leur criticité.

Les entreprises, les chercheurs ainsi que les organismes de formation ont évidement un rôle clef à jouer à ce niveau, mais ces actions doivent s'appuyer sur des orientations définies au niveau international par les responsables politiques et professionnels, tant au niveau des décisions juridiques et économiques qu'à celui du choix des solutions technologiques.

Philippe NANEIX