L'assurance du cyber-risque, prochaine étape de la sécurité Internet ?

Le patrimoine le plus exposé de l'entreprise, c'est-à-dire son système d'information, serait-il le moins couvert et le moins garanti. Pour protéger l'entreprise contre la cyber-criminalité et les autres menaces en ligne, on est souvent tenté d'accumuler des dispositifs techniques, eux-mêmes vulnérables. Qu'en est-il alors du risque réel encouru. La pression subie par le DSI ou le RSSI concernant la sécurité informatique et la gestion de ce risque est permanente. Les dispositifs techniques se sont multipliés et sont de plus en plus sophistiqués, face à des menaces qui elles-mêmes deviennent de plus en plus évoluées. Mais deux problèmes majeurs subsistent.

Le premier concerne les nouvelles menaces, qui sont toujours de plus en plus nombreuses. L'apparition d'une nouvelle menace vient de plus en plus rapidement après que la précédente ait été « traitée » par les dispositifs techniques. On considère qu'il faut désormais mettre à jour son anti-virus plusieurs fois par jour pour qu'il soit réellement efficace. Jusqu'à quand les fournisseurs d'outils de sécurité pourront-ils suivre ce rythme . Les solutions des acteurs de la sécurité (comme Sophos, McAfee, ou Symantec pour ne citer que les anti-virus) deviennent de plus en plus élaborées et intelligentes, c'est vrai. Mais l'apparition de nouveaux services tels que la VoIP ou le sans-fil, et surtout la multiplication des débits Adsl nous font changer d'échelle.

Le second problème n'est pas plus rassurant : le fait de rajouter des dispositifs techniques de protection à des dispositifs existants (car bien sûr on ne défait rien) ajoute un point de vulnérabilité ! C'est tout le paradoxe des solutions techniques : plus de sécurité introduit plus de risque, donc plus d'insécurité !

Ces deux états de faits ont conduit les décideurs à accepter qu'un risque existe, qu'il est important, et qu'il n'est pas couvert (car trop important justement, ce qui effraie les assureurs !) Pis, ce risque existe, et existera sans doute toujours.

Traiter de la sécurité, c'est un métier, réduire les risques c'est un autre métier. Pour qu'une assurance accepte de couvrir un risque, il faut qu'il soit ou qu'il devienne acceptable. Il faut donc tout d'abord l'évaluer, puis si besoin le réduire, pour qu'il devienne transférable à l'assureur.

Née du développement d'Internet, la notion d'assurance pour un cyber-risque a fait son apparition il y a quelques années aux USA. De grandes entreprises multinationales y font appel. Le montage fait en général intervenir :

– un Cabinet d'audit, qui dressera une cartographie des risques,

– une assurance couvrant le risque résiduel défini contractuellement.

Ces services étaient jusque-là réservés aux grands groupes ayant des moyens importants (présence d'un RSSI, coût très élevé des audits,..). Une jeune société lyonnaise, SDN, spécialiste dans la gestion de la sécurité et dans la prévention du cyber-risque, a eu l'idée de démocratiser ces services en les adaptant aux besoins des TPE, des PME, et des unités déportées des grands groupes (agences ou sites de taille modeste).

Ces structures n'ont en général (et n'auront sans doute jamais) ni un DSI, ni un RSSI, ni le temps, ni les compétences, ni les moyens de gérer ces problèmes au quotidien. Développé en partenariat avec ACE Europe, leader dans le domaine du dommage NTIC immatériel, le service « Cyberprotect » se compose de deux éléments :

– un dispositif de surveillance, matérialisé sous forme de boîtier filtrant, qui ne se substitue pas aux dispositifs en place mais qui analyse et prévient le risque d'être touché, et qui peut momentanément couvrir une défaillance éventuelle d'un équipement en cause. Relié à un centre d'expertise qui contrôle en permanence le trafic et mesure en permanence les nouveaux risques, ce dispositif peut intervenir de façon proactive sous forme d'alertes.

– une assurance couvrant le risque résiduel, en cas de défaillance des équipements de sécurité Internet mis en place par l'entreprise. Les biens assurés sont alors couverts : pertes d'exploitation, reconstruction des données.

Le service, d'ores et déjà opérationnel, est lancé commercialement ce mois-ci. Entièrement packagé, il a bénéficié du soutien de l'Oseo/Anvar, et il est distribué par des partenaires informatiques et des courtiers en assurance (site : www.cyberprotect.fr). SDN a poussé la simplification à l'extrême car le produit est livré avec un kit d'installation qui ressemble étonnamment à celui d'une « Internet-Box » courante.

La cyber-tranquillité pour 150 euros par mois, gérée par des « risk-managers » non informaticien. Rendez-vous dans quelques mois pour un premier bilan?