# Combien d'intrus sommeillent dans le SI de votre entreprise ?

*Londres – « Ce qui ne vous tue pas vous rend plus fort ! »* Quand Art Coviello, dirigeant de RSA (filiale sécurité d'EMC), cite Nietzsche, il ne rassure pas forcément les auditeurs de la RSA Conference Europe 2011 qui se tient ces jours-ci à Londres.

**Qui n'a pas peur du grand méchant loup ?**

Puis, il enfonce le « cloud » en précisant que les grosses attaques constatées récemment ne sont que le haut de l'iceberg. *« Le périmètre à surveiller a changé. Les gens, les collaborateurs, sont devenus le nouveau périmètre*, lance Art Coviello. *En effet, une attaque invisible sur l'un des collaborateurs de l'entreprise peut servir à détecter de nombreuses informations dans son système d'information ou sur ses vulnérabilités, mais peut aussi servir de passerelle pour une attaque vers une autre entreprise, partenaire ou cliente. »*

Et pour rassurer définitivement, il assène : *« Les terroristes, cybercriminels ou états espions sont de mieux en mieux armés et organisés pour réaliser des attaques très sophistiquées. Ils savent entrer dans votre réseau et adapter leur comportement pour ne pas être détectés. »*

**Règle de trois pour une sécurité plus efficace**

Aussi noir soit ce tableau, il dépeint malheureusement la réalité que découvrent bien souvent nombre d'entreprises faisant appel à des spécialistes pour analyser leur système d'information. D'ailleurs, le dirigeant de RSA se défend de surfer sur les peurs : *« Nous n'avons jamais vendu des produits en utilisant la peur comme argument. Nous relatons toujours des faits avérés et mesurés et proposons des outils pour s'en prémunir. »*

Pour se protéger au mieux face aux nouvelles menaces, RSA prône trois approches complémentaires (pour lesquelles l'éditeur propose évidemment des solutions) :
– Une approche basée sur **l'analyse des risques** permettant d'identifier les vulnérabilités, la probabilité qu'elles se produisent et les conséquences qui pourraient en découler. Des outils basés sur un *framework* de gestion des risques et de la conformité sont alors conseillés. *« Et le Risque management est un processus continu et itératif »*, martèle Art Coviello ;
– **Le système doit être agile.** La solution systémique se doit d'analyser en temps réel les événements, avec une mise à jour continue des informations sur les schémas d'attaques et autres signatures. Objectif : obtenir une défense en temps réel.
– Enfin, **l'outil doit être contextuel**. Il s'agit de définir les priorités selon les informations à protéger. Enfin, la solution doit disposer d'un maximum d'information sur le SI de l'entreprise (événements, données de log, etc.) pour effectuer des analyses de type Big Data. Seul moyen selon RSA d'obtenir réellement une vue complète de la situation. Et pour parvenir à ce résultat, une solution d'analyse des données Big Data à grande vitesse est essentielle. Tiens, EMC propose justement des appliances GreenPlum…

Prenant le relais de son patron, Thomas P. Heiser, président de RSA, ajoute lui quatre points

essentiels à vérifier pour l'entreprise :
– **Communiquer et communiquer encore** envers les intéressés ;
– **Réévaluer les politiques de continuité d'activité** (PCA) pour les rendre proactives afin qu'elles interviennent automatiquement dès détection d'une attaque ;
– Ne laissez jamais pourrir une crise. *« Il faut briser les silos dans l'entreprise. Dans ce cas, une structure à plat, avec égalité de tous sur ce point, est une des clés de la réussite »,* précise Thomas P. Heiser ;
– Intégrer rapidement l'innovation et les nouveautés liées à la sécurité. *« Chacun doit être impliqué dans ce processus : le dirigeant, les responsables sécurité, les directions opérationnelles… La sécurité reste l'affaire de toute l'entreprise »,* conclut Thomas P. Heiser.