Secure Computing plaide pour la sécurisation des messageries

Comme souvent, les études révèlent les mauvais élèves et mettent en avant les solutions des éditeurs…. C'est le cas du **rapport IDC** sur les fuites de données par les messageries. 100 professionnels ont été interrogés quant à leurs **méthodes de sécurisation de leurs comptes.**

Il se révèle que **72% d'entre eux avouent ne pas disposer d'outils** véritables contre la fuite de données via e-mail. Plus cinglant encore, **89% d'entre eux n'ont pas de solution anti-spam performante.**

L'étude tire donc un premier bilan : « *seule une petite proportion d'entreprises est protégée. Actuellement, beaucoup de ces entreprises s'appuient sur des* ***technologies vieillissantes****, incapables de faire face à la recrudescence actuelle des* ***attaques de spam*** *et aux technologies toujours plus sophistiquées utilisées*« .

C'est dans un contexte d'accroissement du nombre de messages non-sollicités que Secure Computing lance son initiative **STAMP** (*Seven Technologies for Advanced Mail Protection*). L'éditeur propose 7 technologies de protection pour les environnements de messagerie.

Partant du principe que les solutions anti-spam de pointe peuvent **bloquer jusqu'à 99% des messages**, Secure Computing affirme avoir identifié l'architecture nécessaire pour lutter efficacement contre la fuite de données.

Les 7 points tournent autour de la notion de sécurité de la messagerie en temps réel, avec une bande passante réduite, une protection dite multi-tiers face aux menaces entrantes incluant une intelligence mondiale. Une détection complète des contenus, un **chiffrement robuste**. Mais aussi une architecture appelée hybride dans le sens où elle permet de **choisir ou de combiner des solutions sur site, hébergées ou virtualisées.**

Autant de mesures qui combinées peuvent donner lieu à un **éventail de bonnes pratiques** pour se préserver des messages étrangers impromptus. La meilleure défense à toute infection restant cependant la plus grande vigilance.