Sophos introduit une 'appliance' de sécurité, télé-administrable

Vu les attentes du marché en matière de sécurisation des messageries, la tentation était trop forte…

Au risque de court-circuiter certains de ses clients déjà fabricants de boitiers ou 'appliances' (comme IronPort -le partenariat avec DataSwift a déjà été suspendu), l'éditeur Sophos se mue en constructeur ou, du moins, concepteur et fournisseur d'une première unité '*plug and play*' pour grands comptes: l'ES 4000. L'éditeur britannique, s'est tourné vers le constructeur Network Engines (*) (Boston, et succursale européenne à Eindhoven) pour la fabrication d'une unité « *complète, robuste et performante* » -la première d'une gamme qui ne demande qu'à s'étendre – a expliqué Annie Gay, directeur de Sophos Europe du Sud. L'appliance ES 4000 peut protéger plusieurs milliers d'utilisateurs de messagerie de tout ce que l'on peut craindre (ou presque!) en étant connecté au Net: virus, vers (dont les redoutables 'chevaux de Troie'), spams, 'phishing', 'spywares'… Retenons que le système est capable de traiter plus d'un million de messages par jour. Le boîtier au format U1 (extra plat ou presque) pèse son poids, y compris en… euros: son architecture est doublée (configuration en miroir, RAID 1). Doté de deux processeurs Xeon d'Intel (64 bits, 3,2 GHz), avec 2 giga-octets de mémoire, il héberge **deux disques SCSI de 146 giga-octets**, extractibles à chaud, tout comme ses deux alimentations en redondance. Pourquoi une telle capacité disque? Pour permettre, au sein d'un grand ou moyen compte, la mise en quarantaine de tous fichiers suspects (sachant qu'il est possible de rechercher les messages filtrés à partir des mots clés prohibés, spécifiés lors de la configuration du filtre 'anti-malwarespam). On retiendra également que Sophos prend le risque de proposer une garantie de remplacement de toute pièce défectueuse avec envoi anticipé (la pièce vous est envoyée avant que celle défaillante ne soit reçue). L'éditeur, désormais « constructeur », propose également un service de maintenance et d'assistance (24/24h sur 7 jours), avec supervision pro-active permanente sur la « bonne santé » du système et la possibilité d'une **maintenance à distance**. Un tableau de bord, au format Web, permet de vérifier pas moins de 50 points. Toutes les commandes sont en mode menu « wizard » (pas de lignes de commandes); donc, a priori (à défaut de l'avoir testée), l'assurance d'une facilité d'installation et de supervision. Le système effectue automatiquement la 'découverte' des utilisateurs connectés, enregistrés dans un annuaire Active Directory, et l'intégration d'un agent 'Postix MTA' assure la compatibilité avec Microsoft Exchange, SendMail… Et la compatibilité avec les **annuaires LDAP** ? Elle est prévue « *dans les tout prochains mois.* » On retiendra des écrans « tableaux de bord » attrayants (avec statistiques sur les attaques virales, de spams, les pics de trafic, la « vélocité » des transferts, etc.) et, en aval, moult rapports avec 'charts' en couleurs -sans oublier les clignotants, vert, orange, rouge… la mise à jour s'effectuant toutes les 5 minutes. On y retrouve toutes les fonctionnalités qui font la réputation de Sophos: filtrages de spams, filtrage sur réputation (listes noires/blanches des sites Web), gestion des mises en quarantaine et des 'logs', etc. Le prix de cette 'appliance' haut de gamme, qu'il est prévu d'insérer dans des architectures sécurisées multi-sites (consolidation, reprise/redondance à distance…), est en conséquence: 8.265 euros pour le boîtier, avec 3 ans de garantie. Licence annuelle utilisateurs, avec support technique, surveillance « pro-active »: de 10 K-euros pour 500 utilisateurs à 54 K-euros pour 5.000 utilisateurs. ____ (*) Network Engines a été l'un des premiers à

intégrer ISA Server 2004 de Microsoft (*Internet security & acceleration server*).