Protection Linux : Sophos s'adapte au code source

En plus d'être la proie de possibles attaques virales, les serveurs Linux peuvent aussi héberger des menaces pour d'autres environnements qu'ils approvisionnent, comme par exemple des virus Windows?

Même si les systèmes d'exploitation de Microsoft restent la cible privilégiée des hackers, Linux est lui aussi l'objet de menaces, sans doute moins récurrentes, et doit être protégé, car il en va de la survie des données de l'entreprise. Mais l'ouverture du noyau Linux à la communauté des développeurs 'open source' présente une autre difficulté : les modifications apportées au code. Une différence essentielle avec la source verrouillée d'un OS propriétaire, comme Windows. Pour faire face au grand nombre de distributions et de noyaux Linux, ainsi qu'à la possibilité pour les entreprises de modifier le code source de Linux pour l'adapter à leur besoin, Sophos a adopté une solution active : sa nouvelle solution antivirus dispose d'une capacité de recompilation automatique en fonction des modifications apportées au noyau Linux par une nouvelle distribution ou par le client. Unix n'est pas oublié : PureMessage 5.1 pour Unix est une nouvelle version de la solution de protection des passerelles de messagerie. Plusieurs fonctions innovantes permettent en particulier de durcir le filtrage des messages de spam, devenus un vecteur courant des codes malicieux menaçant l'intégrité des systèmes d'entreprises. L'antispam est mis à jour toutes les cinq minutes et les campagnes de spam internationales sont identifiées proactivement par la technologie de détection par Génotype de Sophos. Enfin, le programme analyse et identifie par un algorithme prédictif intelligent le langage source des messages entrants. **Alerter contre le phishing et les ordinateurs zombies**

Même parfaitement protégés contre toute infection, les entreprises, en particulier les institutions financières et les sociétés de commerce en ligne, ne sont pas à l'abri d'une usurpation criminelle de leur identité dans des tentatives de phishing. De plus en plus fréquentes, celles-ci peuvent créer des dégâts importants sur l'image et la crédibilité des entreprises auprès des consommateurs. Sophos annonce la mis en place du service **PhishAlert**, qui s'appuie sur le réseau de veille mondial des SophosLabs pour avertir très rapidement ses clients de toute campagne de phishing les concernant, pour leur permettre de réagir rapidement et efficacement. Ce service vient compléter **ZombieAlert**, qui surveille la diffusion de messages illégitimes à partir d'ordinateurs ?zombies' dans un réseau d'entreprise. Ces zombies sont des machines infectées pour être contrôlées à distance par des utilisateurs clandestins. Ces derniers peuvent ainsi s'en servir comme plates-formes de diffusion de spam ou de lancement d'attaques par déni de service à partir des messageries (DoS). « *Les derniers mois montrent un accroissement rapide et une évolution inquiétante des types de menaces pesant sur les systèmes des entreprises, qui associent de plus en plus fréquemment les techniques de spam, de spywares et de virus et brouillent les distinctions entre celles-ci*« , vient confirmer Annie Gay, directeur général de Sophos France et Europe du Sud. « *Un éditeur de solutions globales de sécurité comme Sophos se doit d'être présent sur tous les fronts, en proposant à ses clients à la fois des solutions proactives et des services qui leur permettent de réagir efficacement et sans délai à toute forme d'agression informatique contre leur activité*« .