Radware étend la protection des réseaux du siège aux filiales

Si les hackers ciblent les sièges sociaux, ils s'attaquent également aux sites distants, généralement moins bien équipés en dispositif de sécurité. Ces attaques sont de plus en plus nombreuses, ce qui nécessite d'étendre la protection des systèmes au-delà des sièges sociaux, et donc de déployer des solutions de sécurité au sein des agences et des filiales.

Ken Myung, responsable informatique chez Audiovox, le confirme : « *Nous avons besoin de notre réseau pour générer du chiffre d'affaires et ainsi permettre au personnel interne et à nos commerciaux d'être plus productifs en utilisant leurs emails ou d'autres applications stratégiques*« . « *Le nombre d'attaques au niveau des applications ciblant les centres de données, les bordures de réseau et même les réseaux locaux ne cesse d'augmenter. Les menaces proviennent de l'interne, de l'externe, voire d'autres lieux professionnels*« , déclare Charles Kolodgy, directeur de la recherche dans le domaine des produits de sécurité chez IDC. « *Par conséquent, les entreprises et les opérateurs doivent protéger leurs applications à l'aide de systèmes de prévention des dénis de service et des intrusions limitant les attaques contre l'ensemble de l'infrastructure du réseau*« . **Une solution de bout en bout signée Radware** Spécialiste des solutions IAS (*Intelligent Application Switching*), Radware fait évoluer sa gamme de produits DefensePro afin d'assurer une sécurité unique de bout en bout, du coeur du réseau aux agences régionales et aux filiales, en passant par la passerelle de l'entreprise. La solution de DefensePro 100 est destinée à protéger les réseaux étendus avec une gamme de commutateurs de sécurité pour la prévention des intrusions. Elle est dotée de fonctions de comparaison des signatures, de mises à jour régulière, de détection des anomalies et de réduction des risques de déni de service. DefensePro 100 permet d'effectuer une recherche bidirectionnelle et de protéger l'ensemble du trafic réseau contre les attaques au niveau des applications. Il intercepte les signatures virales, vers et virus cachés, et bloque les attaques à tous les niveaux, du réseau à l'application. En identifiant et en réduisant les anomalies de protocole et de trafic en temps réel, la solution empêche les attaques par DoS/DDoS (déni de service distribué) et par SYN flood (afflux de requêtes SYN). Elle assure ainsi une protection contre le trafic malveillant et le piratage.