# 3Com (aussi) veut sécuriser les S.I. via le réseau

Cette stratégie n'est pas foncièrement nouvelle. D'autres acteurs majeurs dans l'univers des réseaux, comme Alcatel, Cisco ou Nortel… s'y emploient aussi. 3Com, suite au rachat de TippingPoint, affirme une réelle stratégie sécuritaire. L'un des points forts est son système de

**détection des intrusions**, qui enclenche automatiquement des mises en quarantaine d'équipments infectés ou suspects, selon des règles prédéfinies. Ce dispositif de mise en quarantaine s'exécute en direct sur le réseau; il ne nécessite aucune installation d'agent ni de logiciel sur les postes clients. Tous les postes infectés ou suspects -c'est à dire non conformes- sont automatiquement neutralisés, isolés du réseau. Les règles de mise en quarantaine sont paramétrables de façon très souple – souligne 3Com. Elles s'appuient notamment sur des seuils définis au sein des filtres IPS (prévention des intrusions) et adaptés en fonction des équipements. L'exécution conduit à l'affichage d'une page Web qui propose la résolution du problème par l'utilisateur, le blocage d'un port ou la réaffectation du poste infecté vers un réseau virtuel (VLAN) de mise en quarantaine. Le processus se décompose ainsi: chaque poste client est authentifié via le module de gestion/supervision de 3Com (SMS, system management service – lequel, via RADA, gestionnaire de la mise en quarantaine, agit comme un 'proxy' de serveur d'authenfication Radius, relève le port de connexion au réseau, l'adresse physique MAC du PC). Ensuite, il y a détection d'une « activité illégale » ; le système SMS rapproche l'adresse IP de l'adresse MAC, laquelle est alors mise en « blacklist » et le cas est traité selon la règle prédéfinie: port bloqué, reroutage vers un sous-réseau, etc. L'application de gestion/supervision SMS interroge régulièrement le système pour les mises à jour, et notifie toute intervention auprès de l'administrateur. Concrètement, ce système de sécurisation réside dans un boîtier ou « appliance », qui s'installe entre les commutateurs d'accès (au niveau d'un étage ou d'un bâtiment) et les routeurs du réseau de l'entreprise. Ces dispositifs, aisément installables, pilotent les commutateurs de 3Com 5500 et 7700 -et bientôt les 4400. Ils vont également s'ouvrir à des équipements équivalents de la concurrence. La distribution des informations IPS sur les équipements repose sur une solution Akamaï (envoi des règles de filtrage). Cette solution de TippingPoint assure la mise à jour des signatures des attaques (procédure de vaccin numérique ou '*digital vaccine*'). **EMS: reconfiguration automatique et contrôle de charge** Parallèlement, 3Com capitalise sur sa plate-forme de gestion de réseau, EMS (Entreprise management suite): développée initialement pour les opérateurs télécoms, en Java, elle assure les opérations journalières ou répétitives, comme les mises à jour de versions sur les équipements du réseau, la sauvegarde de données, les rapports sur les attaques réseau… Cet outil, qui s'appuie sur SNMP3, joue un rôle de sécurisation également, il compare les configurations et peut détecter, par exemple, des modifications de ports dans des réseaux déterminés (VLAN, entre autres). Des modules de connexion ('plug-in') permettent d'échanger des infos avec les autres plates-formes de supervision -telles Tivoli d'IBm, Open-View de HP, Unicenter de CA… Et à noter qu'une nouvelle version de SMS tirera parti des fonctionnalités d'EMS. Son prix se situe entre 9.995 et 44.995 dollars selon le nombre d'équipements administrés. **Nouveaux commutateurs d'accès - et un OS unique**

3Com introduit également la gamme de

**commutateurs d'accès 5500**, empilables ('stackables') avec 12 modèles, dont 7 en 10/100 Mbits/s et 5 en Gigabits/s. Ces équipements travaillent sur les niveaux 2, 3 et 4: ils intègrent donc des fonctions de routage et de Voix sur IP (VoIP). Grâce à la technologie XRN (brevet de 3Com), ces commutateurs peuvent être administrés comme étant une seule entité (constituant un « *châssis virtuel*« ). Leur prix s'échelonne entre 2.495 et 13.495 dollars En matière de sécurité, ces 'switches' incluent des listes de contrôle d'accès (ACL) ainsi qu'une authentification sur serveur Radius. La gamme des **commutateurs 7700**, pour sa part, accueille deux nouveaux châssis de périphérie, modulaires, 7750 (10/100 et Giga) avec alimentation via le câble Ethernet (PoE) et support de la VoIP. Leur prix s'échelonne de 1.795 dollars (châssis) à 4.995 pour 48 ports Giga. Tous ces commutateurs utilisent un seul et unique '*operating system*' (3Com OS) identique à celui des 8800.