

PRATIQUE

# Des outils pour simplifier la vie des utilisateurs

## ■ Les équipementiers multiplient les appareils « tout-en-un ».

Lutter contre les 12 milliards de pourriels ou « polluriels », ou « spams », mais aussi contre les 150 à 200 virus informatiques qui naissent chaque jour, et surtout simplifier la gestion de la sécurité informatique... Telles sont les principales tendances que les éditeurs et les équipementiers de la sécurité informatique proposent cette année.

Côté spams, « la grande crainte dans les entreprises, c'est le "faux po-

sitif". A savoir prendre un bon courrier pour un mauvais courrier et l'éliminer », précise Cécile Feroldi, responsable chez l'éditeur Aladdin Knowledge System, qui mise sur la gestion de l'antispams par l'utilisateur lui-même. Ce dernier reçoit une à deux fois par jour la liste des courriels bloqués par le serveur de sécurité. Il peut ainsi retrouver et habilitier les interlocuteurs qui l'intéressent.

Après avoir commercialisé des logiciels spécialisés et dédiés à une seule tâche, les éditeurs rassemblent de plus en plus leurs offres dans des suites intégrées qui couvrent les différents aspects

de la sécurité informatique : antivirus, antispams, antispyswares (contre les logiciels espions), pare-feu, passerelle pour réseau privé virtuel...

Dotées de consoles d'administration, certaines suites intégrées sont directement embarquées à bord de boîtiers électroniques appelés « Appliances ».

**Sans attendre l'antidote.** Cet effort de simplification séduit au point que la plupart des grands éditeurs comme Aladdin, CA, McAfee, Sophos, Symantec ou Trend-Micro commercialisent leurs suites logicielles intégrées

sous le nom de « Virtual Appliances ». Au risque de semer quelque peu le trouble dans les esprits entre suite logiciels et équipement de sécurité.

Côté antivirus et antivers, de nouveaux moteurs de détection ne se contentent pas de protéger le poste de travail ou les serveurs, mais défendent aussi le réseau. Grâce à l'analyse comportementale proactive, ils neutralisent les menaces qui ne sont pas encore connues. « L'an passé, 70 % des nouveaux virus ont été bloqués chez nos clients avant même d'avoir l'antidote », reconnaît Cécile Feroldi.

Cela a inspiré Hewlett-Packard, qui intègre désormais son nouveau logiciel Virus Throttle aux serveurs ProLiant et aux commutateurs ProCurve 5300. Sur ce créneau, le moteur de Trend Micro a été sélectionné par Cisco pour équiper ses routeurs, commutateurs et pare-feu.

A cet égard, l'équipementier intensifie sa politique d'alliances avec des éditeurs comme Arbor, Network Intelligence, Qualys, Sophos ou Symantec afin d'imposer son concept propriétaire de « réseau qui se défend tout seul ». Une idée qui devrait faire des émules.

**Eliane Kan et Erick Haehnsen**



## REVUE DE DÉTAIL

### ● Faire barrage aux pourriels.

MailInBlack a mis au point une astucieuse parade pour combattre les « robots spammers ». Lorsque ces machines à produire des pourriels envoient pour la première fois un message aux clients de MailInBlack, les expéditeurs reçoivent une réponse automatique pour s'authentifier en tapant à la main une série de chiffres aléatoires affichée sur le site Web de la start-up. C'est ainsi qu'elles doivent prouver qu'elles ne sont pas des automates. C'est à cette seule condition que leur courrier sera acheminé dans la boîte aux lettres de leur destinataire.

### ● Externaliser le contrôle de la messagerie.

Cyber Networks, spécialiste de l'infogérance, s'allie avec l'opérateur Blackspider Technologies France pour renforcer le contrôle du flux de messagerie de ses clients. Ce dernier, fournisseur de services de sécurité d'e-mails, dispose d'un outil externe d'analyse qui détecte les spams et les virus avec une capacité de plusieurs millions

de messages par jour. Les indésirables sont filtrés puis stockés dans l'entrepôt de données de Blackspider. Ce qui libère la bande passante et l'espace de stockage de la messagerie de l'entreprise, tout en évitant les risques de panne informatique. Une interface placée au niveau de l'administrateur et de l'utilisateur final assure un suivi du trafic du courrier électronique.

### ● L'approche est originale.

sachant que la majorité des logiciels antipourriels se contentent de faire du filtrage classique par mot clé. Ce qui oblige les grandes entreprises à mobiliser l'équivalent d'un demi-poste pour débloquer les messages piégés par erreur. L'offre MailInBlack est proposée sous forme d'abonnement à l'année. A titre d'exemple, 35 euros pour protéger un carnet personnel de 1 à 50 adresses.

● **Protection des réseaux renforcée.** Sonic-Wall enrichit ses pare-feu avec trois fonctions d'antivirus, d'antispyswares et de

détection d'intrusion. Proposée sous forme d'abonnement annuel, cette technologie repose sur un moteur qui inspecte de manière détaillée les paquets de données reçues afin de détecter les virus, les intrusions illicites et les logiciels espions au niveau même de la passerelle de sécurité. Ce service d'abonnement annuel coûte par exemple 220 euros pour la protection de 10 postes, hors coût d'acquisition du pare-feu.

### ● Logiciel gratuit pour sécuriser les mobiles.

Téléphones et PDA ne sont plus à l'abri des attaques virales ou de courriels indésirables dans les SMS qu'ils reçoivent. C'est ce qu'observe le TrendLabs SM, réseau mondial de centres de recherche antivirus de Trend-Micro, éditeur de logiciels de sécurité informatique. Tirant parti de cette étude, ce dernier offre un bouclier de protection pour certains modèles de téléphones ou de PocketPC équipés de Microsoft Windows Mobile 2003 ou de Symbian OS téléchargeable gratuitement (jusqu'en juin) avec un PC : le logiciel Trend Micro Mobile Security s'installe sur les

mobiles par simple synchronisation des données. Des versions pourront être téléchargeables depuis le téléphone ou le PDA avec une connexion GPRS ou 3G. De la même manière, les utilisateurs pourront actualiser leurs bases de signatures d'antivirus et leur moteur d'analyse des courriels en se connectant avec leur mobile sur le site de l'opérateur.

### ● Tirs nourris contre les logiciels espions.

Les logiciels espions s'infiltrent silencieusement dans les réseaux d'entreprise et les ordinateurs. Cette invasion peut être repoussée avec les solutions antispyswares et antiadware de Symantec qui luttent respectivement contre les espions et les logiciels publicitaires abusifs. Symantec Client Security 3.0 et Symantec AntiVirus Corporate Edition 10.0 détectent et suppriment ces intrus électroniques avant qu'ils ne se déploient. Le premier garantit une protection avancée des postes de travail sur le réseau fixe mais aussi des PC portables au moyen de ses fonctions de détection d'intrusion,

de pare-feu et d'antivirus gérées depuis une console d'administration unique. De son côté, Symantec AntiVirus Corporate Edition 10.0 offre une protection antivirus et antispyswares complète pour les postes de travail et les serveurs d'entreprise.

### ● Filtrage dynamique des accès.

Le nouveau pare-feu applicatif de Deny-All renforce la sécurité des applications Web contre d'éventuelles attaques grâce à un système de sécurité active. Cette solution intéresse notamment les banques en ligne, en ne laissant passer que les requêtes légitimes. La version « rWeb 3.5 » de Deny-All (12.000 euros environ) contrôle de manière dynamique l'ouverture de chacune des pages à consulter. Ce qui limite la navigation au seul contenu accessible par les liens Internet proposés sur sa page d'accueil. Cette stratégie empêche l'internaute d'accéder à des pages confidentielles en tapant, par exemple, leur adresse, et elle allège l'administration du site puisqu'il n'est plus nécessaire de mettre à jour les règles de filtrage.