



Mardi 10 Août 2004

LMI n° 1020 du 02/04/2004

Panorama

Une palette d'outils pour surveiller l'architecture

La surveillance de la sécurité d'une infrastructure informatique nécessite la mise en oeuvre de nombreuses briques technologiques, complémentaires les unes des autres. Une débauche d'équipements générant un grand nombre d'alertes, qui peuvent être au besoin centralisées sur une console d'administration spécifique.

Les briques technologiques sont nombreuses dans la sécurité et le seront de plus en plus. L'année qui vient de s'écouler a vu le nombre d'outils antipourriel (antispam) exploser. Celle qui vient sera peut-être celle des anti-"spywares", ces logiciels espions qui observent à la loupe les comportements des utilisateurs. Et chacun de ces modules génère des alertes. Reste donc à centraliser ces dernières pour rendre le système de sécurité plus cohérent et performant. Un véritable casse-tête auquel tentent de répondre les fournisseurs. Pour ISS ou Watchguard, la solution passe par des tout-en-un intégrant toutes les briques. Pour d'autres, comme Symantec, il s'agit d'offrir une réponse à chaque problématique. Après quelques acquisitions, l'éditeur propose un antivirus, un outil d'audit, une sonde d'intrusions... Pour d'autres enfin, il faut créer des partenariats entre fournisseurs. Check Point avait lancé une initiative en ce sens en 1998 avec OpSec, pour rapprocher les interfaces de programmation (API) des fournisseurs. Netscreen avait répondu avec le Global Alliance Program. Beaucoup de vœux pieux, mais peu de résultats. Et les éditeurs de consoles d'administration sont toujours contraints de passer des accords bilatéraux avec les fournisseurs. La norme de définition des alertes n'est pas pour demain et les amateurs de politiques de sécurité cohérentes devront encore attendre.

Mais la cohérence est-elle seulement un Graal à atteindre à tout prix ? Pas si sûr. Dans les antivirus, par exemple, la plupart des éditeurs disposent d'équipes techniques repérant et décryptant les nouvelles souches pour identifier leurs signatures et fournir une réponse à leurs clients. Mais si tous prétendent se montrer les plus réactifs, difficile d'avoir une vue objective sur la question. "Une fois c'est l'un, une fois c'est l'autre", résume Stéphane Bouché, directeur de Secuserve, un prestataire de services intégrant dans son offre les produits Sophos, F-

MATERIEL

PC et Laptops

Serveurs et Mainframes

Périphériques

Stockage

LOGICIEL

Systèmes d'exploitation

Progiciels

Développement

RESEAUX

Administration

Sécurité

Télécoms

Internet

ECONOMIE

SSII et Intégrateurs

Editeurs et Constructeurs

Distributeurs

Opérateurs

MANAGEMENT

Témoignages

Expertises

Droit et Contrats

RESSOURCES HUMAINES

Recrutement

Emploi/Carrières

Formation

Rémunération

CYBERATTITUDE

Culture

Communautés

Humour/Contrepoints

Thématiques

SANS FIL**SECURITE****HAUT DEBIT****STOCKAGE****EBUSINESS**

Métiers

DISTRIBUTION**DEVELOPPEMENT****MANAGEMENT**

Secure et TrendMicro. Autrement dit, mieux vaut, dans les grandes sociétés, choisir la ceinture et les bretelles : se payer deux antivirus qui feront le même travail, mais chacun à son rythme. Quitte à faire quelques concessions à la sacro-sainte cohérence.

Olivier Descamps

PARTENAIRES

[Eudora 6.1 Email - Maintenant disponible en français](#)

[Maintenez vos performances informatiques - Visitez le site Compuware](#)

[Observatoire LMI - HiTechPros](#)

[Iomega REV 35GO/90GO : sauvegarde révolutionnaire](#)

[Web-profils.com, la place de marché du conseil et de l'ingénierie](#)

[Actualités](#) | [Magazine](#) | [Newsletters](#) | [Abonnement](#) | [Agenda](#) | [Comparateur de prix](#) | [Evénements](#) | [Contacts](#) | [Guide LMI](#) | [Agenda Séminaires IT](#)

© **Le Monde Informatique 1997, 1998, 1999, 2000, 2001, 2002, 2003, 2004**

Toute reproduction ou représentation intégrale ou partielle, par quelque procédé que ce soit, des pages publiées sur ce site, faite sans l'autorisation de l'éditeur ou du webmaster de Le Monde Informatique est illicite et constitue une contrefaçon. IDG France s'est engagé à respecter la confidentialité des données personnelles régies par la loi 78-17 du 6 janvier 1978.

[Politique de rediffusion](#) .