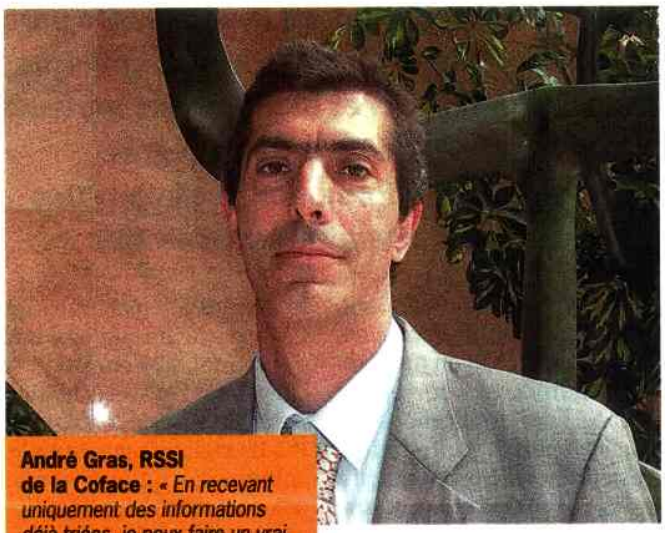
01 Réseaux
26 RUE D'ORADOUR SUR GLANE
75504 PARIS CEDEX 15 - 01 44 25 30 22

NOVEMBRE 2003
Mensuel
OJD : 33128

L'**administration** de la sécurité doit devenir proactive

Que l'on choisisse une console généraliste ou des outils spécialisés, l'administration de la sécurité bute sur le flux d'informations à traiter. Une démarche proactive est alors indispensable. Mais toutes les tâches ne sont pas automatisables. Par Guy Leroy



André Gras, RSSI de la Coface : « *En recevant uniquement des informations déjà triées, je peux faire un vrai travail d'analyse. Il faut alors être capable d'anticiper, une qualité spécifiquement humaine.* »

En entreprise, pare-feu, IDS et autres sondes veillent. Mais les informations qu'ils remontent en temps réel doivent être traitées dans des délais adéquats, afin de réagir efficacement. C'est le rôle dévolu aux superviseurs SIM *(Security information manager)*, disponibles chez les grands de l'administration (IBM, HP, Computer Associates [CA]...) ou chez les spécialistes de la sécurité (tels NetIQ ou ISS).

Généraliste ou spécialisée, chaque solution a ses forces et ses faiblesses. André Gras, RSSI de la Coface, « *apprécie l'approche centralisée de CA à travers un portail unique de pilotage de l'ensemble des composants, même de produits tiers* ». Bernard Foray, RSSI de Gemplus, privilégie l'option inverse : « *Ne pas centraliser réduit le risque de panne générale. De plus, insérer le SIM dans HP OpenView serait très lourd.* »

Reste que la sécurité doit s'intégrer plus fortement aux applications. « *Le RSSI doit avoir une vision métier* », note Jean-Marc Rémy, directeur technique d'Ipelium. Une démarche qui est à l'origine d'outils comme SCC (Security Command Center) *e*Trust, de CA, « *qui montre l'impact des incidents sur les processus métiers* », assure Valère Pascolo, consultant chez CA.

Vient l'autre difficulté de l'administration de la sécurité : trier les informations. « *Tout n'est pas à surveiller,* rappelle Bernard Foray. *Certains fichiers de* logs *atteignent plusieurs gigaoctets par jour. Et il faut définir ce que l'on décide explicitement de ne pas gérer.* » Ce qui nécessite des compétences dans l'entreprise ou via un MSSP. En effet, déplore Jean-Marc Grémy, « *trop d'entreprises pensent qu'avoir investi dans des équipements suffit, et qu'exploiter les données est inutile.* » Philippe Launay, responsable des offres MSSP chez Sodifrance, insiste : « *Nous ne plaçons un IDS que si notre spécialiste est présent pour analyser les* logs, *via WebTrends.* » Une certaine automatisation est toutefois possible en corrélant les informations. Sur quel référentiel le superviseur SIM s'appuiera-t-il pour détecter les menaces ? Gerhard Eschelbeck, directeur technique de Qualys, propose un « *interfaçage avec la base des vulnérabilités du réseau de l'entreprise détectées par notre scanner.* » Habituellement, un IDS alerte quand il détecte, par exemple, le ver Blaster, même si la cible est un serveur Unix, qui ne risque rien. « *Cette information est dans la base de* scans, explique Gerhard Eschelbeck. *Dès lors, une console SIM, comme celle d'ArcSight ou de Netforensics, ne crée pas d'alerte inutile.* » Mieux : si une machine est vulnérable à Blaster, alors la console bloquera les accès vers cette machine sur le pare-feu, sans déconnecter toute l'entreprise.

Un délai qui permet une certaine proactivité

« *Cela laisse le temps d'installer le patch,* décrit Gerhard Eschelbeck. *Dans le cas de Blaster, la vulnérabilité de Windows exploitée était connue depuis trois semaines.* » Ce délai, qui tend à se réduire, permet une certaine proactivité. Un éditeur tel que Micromuse s'interface avec les serveurs spécialisés du Cert, pour être averti des nouveaux risques. Enfin, si les signatures des attaques ne sont pas encore référencées, Stéphane Wuilliez, d'IBM, estime que « *le moteur d'analyse générique de Tivoli Risk Manager détecte la menace* ». ■

SAVOIR FILTRER LA "SUBSTANTIFIQUE MOELLE"

Les utilisateurs veulent « l'essentiel ». La sécurité des applications doit être prioritaire sur les événements réseaux ou systèmes. Il faut aussi pouvoir rejouer l'alerte avec tous ses événements. Outre bloquer l'alerte, il faut pouvoir l'analyser a posteriori pour s'en protéger la fois suivante. Bernard Foray, RSSI de Gemplus, complète : « *Chez nous, tout le monde se sent concerné par la sécurité. L'information circule. Cette méthode est efficace, et permet de corréler plusieurs sources d'informations. S'il y a concordance, il y a danger.* »