

Une sécurité efficace doit passer par la simplification du système

Pour contrer les menaces qui ne cessent de s'accroître, les experts misent sur une protection plus globale des systèmes d'entreprises.

JACQUES MEDINA*

L'année 2005 s'était à peine achevée que déjà les premières analyses portant sur la sécurité des systèmes d'information des entreprises paraissent. Et elles ne sont guère encourageantes. Le centre de coordination de sécurité américain (US-CERT) fait par exemple état d'une hausse de 38% des vulnérabilités publiées entre 2004 et 2005, soit un total de 5198 événements répertoriés l'an dernier. Parmi celles-ci, 812 ont concerné les systèmes d'exploitation Windows, 2328 ceux d'Unix/Linux et 2058 des multiplateformes. Pourtant, si l'on en croit l'analyse annuelle conjointe du FBI et du Computer Security Institute (CSI) rendue publique en septembre 2005, certains types d'attaques seraient en baisse, principalement les accès non autorisés (au sens large du terme).

Les nouvelles menaces relèvent du contrôle

Comment interpréter ces chiffres? En fait, le nombre de vulnérabilités ou d'attaques n'est plus un indicateur universel

comme il a pu l'être par le passé. Certes, pour tous les événements de type scan, fingerprinting, déni de service simple ou distribué, la volumétrie demeure un paramètre valide permettant d'établir le niveau d'exposition au risque de certains systèmes ou services. Toutefois, cette approche quantitative n'est pas adaptée aux nouvelles menaces (la grande famille des virus, vers, chevaux de Troie, rootkits et autres variantes de code «malicieux» en tête), qui requièrent une analyse beaucoup plus détaillée.

Ce qui est nouveau, c'est en effet l'exploitation qui en est faite. En lieu et place des attaques de masse qui immobilisaient des réseaux entiers, l'objectif de l'assaillant aujourd'hui est plutôt de prendre discrètement le contrôle d'un grand nombre de victimes afin de les utiliser pour des attaques de masse comme les dénis de service distribués, le spam ou le phishing, pour lequel le nombre de cas déclarés a doublé sur les 12 derniers mois, dépassant les 3000 cas mensuels. C'est l'avènement des «botnets», ces

réseaux de machines compromises contrôlables à distance. Selon *SCmagazine*, en novembre 2005, 25.000 nouveaux «zombies» apparaissent quotidiennement!

Davantage de plateformes et donc de risques

Les vecteurs de risques s'amplifient également avec l'utilisation de plus en plus répandue des réseaux sans fil, des assistants personnels, des softphones, des connexions de type «small office», dont le déploiement ne s'accompagne pas toujours du respect des normes de sécurité adéquates.

Quant aux applications, on peut disserter sans fin sur les risques liés au «peer to peer», à Skype et consorts, aux messageries instantanées ou à toute autre technologie qui permet de contourner les règles de sécurité d'une architecture classique. Enfin, bien qu'elles soient surmédiatisées, on ne peut passer sous silence les menaces spécifiques à la téléphonie sur IP.

Comment peut-on donc se protéger? Le discours qui consiste

à dénigrer la sécurité périphérique au profit d'une sécurité multicouche est trop simpliste. Oui, on a toujours besoin du firewall, mais ce dernier doit être apte à contrôler même le trafic le plus complexe. Oui, un système de protection contre les attaques est nécessaire, pour autant qu'il soit géré de manière cohérente et que son administration ne soit pas un cauchemar. Oui, il faut contrôler les flux de données, qu'elles soient encryptées ou non.

Gage d'efficacité: la cohabitation techno-humaine

Mais dès lors, comment détecter un intrus au sein d'une infrastructure? Comment empêcher l'infection d'une station de travail par un virus ou un spyware sans en affecter la productivité? Assurer le déploiement des correctifs de sécurité sur un serveur sans risque pour les applicatifs? Identifier de manière certaine un utilisateur, lui attribuer des droits et contrôler en permanence son activité? S'assurer de l'innocuité des requêtes vers les serveurs web? De nouvelles tech-

nologies apportent des éléments de réponses à toutes ces questions. Leur dénominateur commun est d'offrir une sécurité accrue avec une administration et une exploitation simplifiées.

Reste que LA réponse n'est pas uniquement d'ordre technologique. Le facteur humain est en effet primordial, chez les utilisateurs comme chez les administrateurs du réseau. Sans une sensibilisation régulière, il est illusoire d'attendre des utilisateurs qu'ils abandonnent les pratiques dont ils ne savent pas toujours qu'elles sont à risque. De même que sans ressources raisonnables nécessaires à l'exploitation, les administrateurs sont tentés d'abandonner certaines solutions, comme les sondes de détection d'intrusion.

C'est donc en choisissant les technologies les mieux appropriées à ses besoins et en les faisant bien cohabiter avec les collaborateurs que l'entreprise s'assurera une protection efficace de son système d'information.

* Security Architect, Navixia SA