

# Sécurisation des réseaux : pas si simple que cela !

Ils démontrent en effet que, même pour les vulnérabilités les plus critiques, les entreprises mettent en moyenne 30 jours à corriger seulement la moitié des systèmes vulnérables, ce qui laisse l'entreprise exposée pendant une longue période.

Par ailleurs, il faut sans arrêt remettre sur le métier son ouvrage, puisque 50% des attaques les plus connues et les plus critiques sont remplacées chaque année par de nouvelles vulnérabilités, tout aussi dangereuses. En outre, la durée de vie de certaines vulnérabilités est quasi illimitée, cette demi-vie étant principalement due au déploiement de nouvelles machines ou serveurs sur lesquels on n'a pas encore apporté les correctifs nécessaires. Enfin, 80% des vulnérabilités sont exploitées dans les 60 jours suivant leur annonce publique. La nouvelle génération de menaces visant les entreprises se caractérise par une propagation rapide du problème assortie de dégâts importants. De plus, elles utilisent des vulnérabilités souvent inconnues et plusieurs vecteurs d'attaque tout en ciblant un dysfonctionnement précis pour inhiber l'activité métier de l'entreprise. Enfin, elles reposent généralement sur des intrusions au sein des périmètres déjà sécurisés. Ceci explique sans doute pourquoi IDC considère que le segment des outils d'évaluation et de management des vulnérabilités devrait croître de 25% l'an pour atteindre 846 millions de dollars d'ici 2006, soit une croissance supérieure à celle des anti-virus, des coupe-feu et des IDS. Quoiqu'il en soit, Qualys fait les recommandations suivantes à qui veut se prémunir contre ce genre d'attaques : - lancer régulièrement des audits de sécurité sur les réseaux et les systèmes, - s'assurer de la mise à jour constante des anti-virus, - gérer et appliquer le correctifs dès leur mise à disposition, - enfin, réévaluer continuellement et proactivement la politique de sécurité. Qualys publie d'ailleurs une liste dynamique des vulnérabilités les plus critiques et les plus répandues. Nos lecteurs pourront la consulter en allant sur le lien suivant : [www.qualys.com/RV10](http://www.qualys.com/RV10)