

## 3Com paye pour sa sécurité

3Com veut accélérer la correction des vulnérabilités de sécurité en rémunérant les chercheurs indépendants qui pourraient lui révéler les failles qui se présentent dans ses produits matériels et logiciels.

Le programme **Zero Day Initiative** est considéré comme stratégique par l'industriel qui espère ainsi apporter à la fois un plus haut niveau de protection sur ses produits, mais surtout réduire singulièrement ses délais de réaction, et même se révéler très proactif en anticipant les risques d'attaques sur les réseaux. Un point de vue qui est confirmé par certains observateurs, mais qui n'a pas fini d'inquiéter de nombreux autres, et en particulier les revendeurs des produits 3Com. En effet, en rémunérant l'information ponctuelle qui lui est fournie, 3Com court le risque d'une part de générer une démarche commerciale de recherche de ces failles de sécurité, et surtout de voir se diffuser l'information avant même que son réseau ne soit mis au courant. David Endler, directeur de la recherche sécurité de la division TippingPoint, une solution de sécurité acquise par 3Com en 2004, affirme le contraire : « *Nous sommes en train d'adresser un nombre important de chercheurs qui ne vont pas nécessairement contacter les vendeurs lorsqu'ils découvrent des failles de sécurité* ». Il est vrai qu'une incitation financière est un plus certain, mais c'est aussi un argument à double tranchant ! Lorsqu'un individu découvre une faille, il se connecte au portail de 3Com. Les services de l'éditeur s'engagent à valider sous trois jours la réalité de la menace. Si cette dernière est vérifiée, la personne qui l'a découverte recevra une prime via un service de virement monétaire du type PayPal. Une question reste cependant en suspens : quelle sera la rémunération que 3Com versera individuellement ? L'éditeur a déclaré qu'il engageait des « *ressources considérables* », mais n'a encore affiché aucun chiffre !