



Article de Jacques Bourdeau
Ingénieur en sécurité & CISSP
ESI Technologies

Sécurité informatique : protéger autrui pour mieux se protéger

L'entraide est un principe largement établi dans nos sociétés. Les religions et les philosophies qui l'intègrent en priorité ne se comptent plus. Si l'on peut y voir une leçon de vie en général, l'idée s'applique aussi au monde des technologies de l'information.

Le ver informatique nous en fournit une démonstration intéressante. Plusieurs vers ont pour objectif d'inonder des serveurs en particulier afin de les rendre inaccessibles, comme Blaster, qui a cherché à bloquer la distribution des mises à jour de Microsoft. Même lorsqu'ils n'ont pas de cible précise, les vers sont très nuisibles, leur énorme volume ayant pour effet de freiner l'ensemble des communications. Par conséquent, si un réseau bloque la propagation de Blaster au-delà de ses propres limites, il évitera que l'infection dont il souffre ne contamine d'autres réseaux, réduisant globalement les conséquences néfastes du virus.

Bien-sûr, une organisation ne pourra empêcher la propagation à elle seule. Par contre, si tout un chacun y met du sien, le fléau sera combattu avec beaucoup plus d'efficacité. Une brique unique, posée par une seule personne ou une seule entité, peut paraître insignifiante dans la construction d'un mur de défense solide. Toutefois, elle revêt de l'importance dans la mesure où suffisamment d'autres briques sont ajoutées par d'autres entités.

De trop nombreuses entreprises sous-estiment la portée de ce principe. Ce qui les amène, par exemple, à configurer leurs pare-feu de façon à se protéger des intrusions au sein de leur réseau, sans se préoccuper pour autant de ce qui peut en sortir. Pourtant, tous les pare-feu sont en mesure de contrôler les entrées et les sorties, comme la plupart des mécanismes de sécurité d'ailleurs (authentification, filtrage, anti-virus, etc.). Si le serveur de courrier principal est le seul autorisé à acheminer les courriels vers Internet, un poste infecté par MyDoom, NetSky ou un autre ver véhiculé par le courrier ne pourra pas se propager.

Le contrôle des sorties ajoute une couche de protection au système de sécurité d'une entreprise. Il permet de déceler plus facilement les failles ayant permis quelque intrusion que ce soit dans son réseau. Par exemple, la présence d'un logiciel espion (ou *spyware*) ne sera pas détectée par un antivirus puisqu'il ne s'agit pas d'un virus. Par contre, elle pourrait l'être grâce aux mesures de protection en sortie. Celles-ci enregistreront également les activités illicites menées sur Internet par les employés durant les heures de travail.

Autre considération militant en faveur de la protection d'autrui, une entreprise qui lance une attaque informatique, même involontaire, vers ses clients, fournisseurs ou partenaires pourrait avoir à en subir les conséquences. Certains d'entre eux, en effet, s'expliqueront mal pourquoi des mesures n'ont pas été prises pour prévenir la situation. On peut très bien imaginer que leur confiance envers l'entreprise en faute s'en trouve diminuée, ce qui peut provoquer un relâchement des liens commerciaux.

En informatique, la protection globale est l'affaire de tout le monde. Autre exemple éloquent à cet égard, l'usurpation d'adresses IP (ou *IP spoofing*) ne peut être bloquée par le coeur d'Internet sans compromettre l'ensemble des communications sur le réseau des réseaux. Il incombe donc aux fournisseurs d'accès et aux organisations d'empêcher que ce trafic hostile ne franchisse leurs passerelles. Ici encore, l'efficacité de la protection repose sur le nombre.

L'union fait la force! Comme toute communauté, celle qui est formée autour d'Internet a besoin de l'engagement de ses membres. Il suffit de faire sa modeste part pour bénéficier de l'aide de millions de pairs.