Le bon sens est la première barrière contre les virus

Les virus existaient avant le développement de l'Internet. Ce sont des petits programmes informatiques qui se transmettent d'un ordinateur à l'autre à l'occasion d'échanges de disquettes ou bien d'envois de fichiers joints aux messages.

Certains virus n'attendent pas ces échanges de données entre utilisateurs. Ils sont programmés pour utiliser le carnet d'adresses personnelles, installé sur le logiciel de messagerie de l'utilisateur. Ainsi, ils se propagent vers ces adresses informatiques, par les réseaux de messagerie.

Jusqu'en novembre 1999, lire un message n'exposait pas au risque. Seuls les fichiers joints étaient porteurs de virus. A cette date, le virus *BubbleBoy* aurait été développé directement dans la zone du message électronique. Même s'il s'agissait du seul virus connu de ce type, nous sommes conduits à réfléchir avant d'ouvrir un message.

Les logiciels de protection reconnaissent plusieurs dizaines de milliers de virus. Cela donne une idée du nombre de personnes qui s'adonnent à cette activité...

La dissémination mondiale en quelques heures est facilitée par deux facteurs :

– l'interconnexion des ordinateurs sur la planète ;

– l'homogénéité des installations logicielles (langage informatique commun et faiblesses communes).

Pour sa propagation, le virus *Iloveyou* du 4 mai 2000 (fichier attaché en extension *.vbs*) a utilisé une faille d'un logiciel de messagerie.

Un minimum de bon sens de la part de l'internaute permet un premier niveau de protection. Même dans un réseau administré, cette responsabilité lui incombe.

Ainsi, l'utilisateur veillera à :

– ne pas ouvrir un message électronique envoyé par un inconnu et/ou sur un thème inattendu ;

– ne pas télécharger un fichier attaché non attendu ;

– ne jamais télécharger un fichier attaché dont l'extension est *.vbs* (*visual basic script*) ;

– ne jamais télécharger un logiciel sans l'aval de votre administrateur-système et surtout pas sur un site non dépositaire de la marque ;

– ne pas installer des programmes non validés par votre administrateur-système, ou même des écrans de veille personnels ;

– faire particulièrement attention aux messages qui arrivent alors que les médias signalent une alerte virale, même s'ils proviennent de correspondants connus. Les protections sont mises à jour dans des délais courts (quelques heures suffisent aux développeurs car les virus sont des programmes simples) : si les messages ne sont pas urgents, il vaut mieux attendre avant de les ouvrir ;

– vérifier que son matériel bénéficie de la mise à jour régulière des logiciels de protection et que les disquettes provenant de l'extérieur du réseau sont controlées ;

– télécharger régulièrement, s'il travaille sur un ordinateur personnel, les mises à jour mises à disposition par les fournisseurs sur le Web (commande *Update*) ;

– respecter les consignes de sécurité données par les administrateurs-système.