

2.8 Virus et anti-virus

Pour mettre au point l'organisation permettant de se prémunir des virus, il est important de faire appel à une compétence informatique et de former les utilisateurs.

2.8.1 Virus

Par commodité, nous désignerons par virus tout programme s'exécutant et se propageant à l'insu de l'utilisateur d'une machine. Techniquement, il existe différents types de programmes en fonction du type de fichier infecté, du mode de propagation, des effets du programme (virus, ver, trojan, etc...). En pratique, les virus combinent maintenant ces différentes caractéristiques.

Les virus sont le plus souvent transmis par des programmes ou des messages ; ils peuvent être également transmis par des documents contenant des macros.

Un virus est un programme qui a trois caractéristiques :

- ✓ Il s'exécute à l'occasion de l'exécution d'un autre programme (par exemple, quand vous ouvrez un message ou une pièce jointe)
- ✓ Il se propage en infectant (en « se collant à ») d'autres programmes ou en envoyant des messages
- ✓ Il réalise des actions spécifiques.

Un fichier contenant un virus peut être obtenu initialement par messagerie, téléchargement, lecture d'un support amovible (disquette), connexion à un poste de travail ou à un serveur infecté.

Le mode de propagation d'un virus peut être :

- ✓ par exploration de votre carnet d'adresses de messagerie ou d'un annuaire
- ✓ par création aléatoire d'adresses de messagerie sur un modèle donné (ex prénom.nom@gouv.fr)

- ✓ par utilisation d'adresses récupérées sur un site web
- ✓ par exploration de votre disque dur ou de tout support de fichiers (disquette, clé USB, ...)
- ✓ par transmission entre utilisateurs de supports contenant des virus (disquette, clé USB, ...)
- ✓ par exploration du réseau auquel vous êtes connecté (serveur bureautique par exemple).

Les actions d'un virus peuvent être :

- ✓ rien d'autre que sa propagation
- ✓ l'affichage de messages (par exemple, politiques)
- ✓ la collecte d'adresses mail afin de leur envoyer des courriers électroniques de masse (spam)
- ✓ l'exploitation de failles de sécurité d'un ou plusieurs logiciels présents sur votre ordinateur
- ✓ l'installation d'un programme permettant à un autre utilisateur de se servir de votre ordinateur (par exemple pour attaquer un site web par déni de service)
- ✓ la transmission sur internet de tout ou partie de fichiers trouvés sur un disque

- ✓ la modification de fichiers
- ✓ la destruction de fichiers
- ✓ de rendre un ordinateur inopérant.

Ces trois derniers cas sont rares.

Enfin, les effets supplémentaires d'un virus sont liés à ses effets de masse :

- ✓ privation de ressources informatiques
- ✓ engorgement de la bande passante d'un réseau, voire d'une partie de l'internet
- ✓ allongement des temps de traitement.

2.8.2 Antivirus

La principale défense contre les virus est l'installation préventive et l'utilisation permanente d'un antivirus appliqué à tous les types de fichiers.

Un antivirus est un programme qui peut :

- ✓ détecter la présence d'un virus dans un fichier
- ✓ détecter l'activité d'un virus
- ✓ réparer les fichiers infectés
- ✓ transférer les fichiers infectés sur un support donné
- ✓ détruire les fichiers infectés.

Un antivirus peut/doit être installé sur plusieurs machines : le poste de travail de l'utilisateur, le serveur pare-feu entre l'entreprise et l'internet, le serveur de messagerie pour les messages circulant entre l'entreprise et l'internet, voire pour les messages internes à l'entreprise, les serveurs web.

Comme tout programme, un antivirus est disponible en versions successives, mais repose également sur un fichier de signatures, ces signatures caractérisant les virus qu'il cherche à détecter. Pour un antivirus donné, le nombre de signatures se compte en dizaines de milliers.

Pour chaque nouveau virus, le fichier de signatures ou l'antivirus lui-même doivent être mis à jour. Un virus peut être développé pour une cible précise et ne sera donc pas connu tant que la cible ne l'aura pas détecté.

Tous les éditeurs d'antivirus ne réagissent pas dans les mêmes délais et tous les utilisateurs ne mettent pas à jour leur antivirus immédiatement.

La réparation d'un fichier infecté par un virus peut fonctionner ou non ; si elle fonctionne, on peut récupérer tout ou partie du fichier initial.

2.8.3 Conséquences pour les échanges de documents par une plate-forme de dématérialisation

Un fichier Zip® est le résultat de la compression d'un ou plusieurs autres fichiers. Il existe un certain nombre de virus qui reposent sur l'utilisation du format Zip®. Ces virus fonctionnent non pas en infectant des fichiers Zip®, mais en se cachant à l'intérieur au même titre qu'un autre fichier. Le format Zip® est ainsi utilisé pour propager le virus mais ne déclenche pas son exécution. Les antivirus sont en train de s'adapter à cette nouvelle forme de transmission.

Les épidémies de virus Word® ou Excel® datent de la fin des années 1990. Une résurgence reste possible, mais ce n'est clairement pas ce genre de virus qui défrayeront ces derniers jours la chronique.

La possibilité théorique de l'infection de fichiers pdf a été démontrée en 2001. Ceci était rendu possible dans la version 5.0.5 d'Acrobat® ; cette version peut être corrigée et de toutes façons cette vulnérabilité n'existe plus dans Acrobat 6®. *A priori*, un fichier pdf ne sera donc pas infecté.

L'infection d'autres documents, aux formats moins répandus, est peu probable car ils n'ont pas le nombre critique d'utilisateurs qui rend l'opération intéressante pour les créateurs de virus, comparée à la propagation de virus par la messagerie.