

4. La protection du réseau de l'entreprise

La protection des postes de travail de l'entreprise est une chose, la protection du réseau en est une autre.

Le premier type de protection a pour but de limiter les risques humains relatifs à l'utilisation des outils informatiques. Le second sert à sécuriser les échanges au sein du réseau et à empêcher un pirate de s'y introduire.

La protection du réseau d'une entreprise passe par la mise en place d'outils spécifiques, destinés à vérifier l'utilisation qui en est faite et à empêcher des attaques, mais aussi par des processus permettant à l'administrateur d'examiner son état pour cibler les tentatives d'intrusion et y parer le plus rapidement possible.

a ■ SE PROTÉGER EFFICACEMENT DES VIRUS

Il existe plusieurs éléments indispensables du réseau à sécuriser pour faire face aux virus, notamment :

- les postes de travail ;
- les serveurs et passerelles ;
- les ressources partagées.

L'antivirus ne suffit plus pour se protéger efficacement : les nouveaux virus utilisent de nouvelles méthodes de propagation et d'action que les antivirus ne reconnaissent pas toujours... à moins que l'éditeur n'ait inclus leur reconnaissance dans la base virale initiale, et que cette dernière n'ait été mise à jour...

Il est cependant recommandé d'installer différents antivirus complémentaires sur les postes clients et sur les serveurs (serveur *proxy*, serveur de mail, etc.).

Le déploiement de correctifs de sécurité est également indispensable et primordial, de plus en plus de virus utilisant les dernières failles système pour se propager. Ces correctifs, qui concernent aussi bien les postes clients et les serveurs que les autres ressources présentes sur le réseau (routeurs, imprimantes, pare-feu, etc.), doivent être testés avant leur intégration, pour vérifier qu'ils ne provoqueront pas d'interférences ou de conflits avec les autres logiciels installés.

Il faut ensuite sensibiliser les utilisateurs aux virus en expliquant leur fonctionnement, leur mode de propagation, les risques effectifs qu'ils représentent, etc.

Il est par ailleurs impératif de tout mettre en œuvre pour empêcher la désactivation des antivirus sur les postes clients par l'utilisateur (ce qui constituerait même une faute grave, en cas de retrait volontaire avéré). Sur certaines configurations, il est possible de verrouiller l'accès à certaines fonctions pour l'utilisateur. Un virus aura alors beaucoup plus de mal à se propager et ne pourra pas obtenir les droits d'administrateur de la machine (qui contrôlent tous les paramètres et accès de l'ordinateur).

Concernant les serveurs, les antivirus doivent être capables de filtrer tous les ports (port HTTP, port FTP, port SMTP pour le mail, pour ne citer qu'eux). Un *firewall* ou un *anti-spam* seront installés, de même que des logiciels de filtrage de contenu, d'URL ou de port (qui permettent une analyse lexicale par mots clés et détectent certains virus).

Des solutions d'IDS/IPS – que nous verrons plus loin – serviront également à bloquer les virus.

En cas d'infection par virus d'une machine, voici les procédures à effectuer pour limiter les dégâts :

- Déconnecter la machine du réseau en débranchant le câble réseau ou en désactivant la connexion sans fil, pour éviter la propagation du virus sur le réseau.
- Ne pas éteindre la machine immédiatement pour éviter d'accroître les dégâts (certains virus détruisent le contenu des disques durs au redémarrage de la machine) et conserver un maximum d'informations sur l'agression.
- Faire une copie physique du disque dur infecté.
- Vérifier l'origine de la contamination (en vérifiant les *logs* et l'historique).
- Vérifier que d'autres machines du réseau n'ont pas été infectées.
- Réparer la machine (grâce à un antivirus) et la reformater pour tout réinstaller (si le virus n'a pas été complètement éradiqué ou si un doute subsiste quant à un éventuel autre virus).
- Changer les mots de passe qui auraient pu être captés par l'intermédiaire d'un *keylogger*.
- Répertorier l'attaque et l'analyser pour étalonner les protections mises en place.
- Porter plainte contre X en cas d'attaque avérée.