Une meilleure approche de la protection virale multiniveau

David Mitchell et Katherine Carr, Sophos, Oxford, UK

Juin 2002

RESUME

Ce livre blanc décrit les différents niveaux constituant l'infrastructure informatique d'une entreprise et évalue à chaque point d'accès les besoins de chacun de ces niveaux en matière de protection virale. Il traite par ailleurs des facteurs dont doit tenir compte l'entreprise au moment de prendre des décisions concernant l'acquisition et la gestion de logiciels antivirus.

L'infrastructure informatique

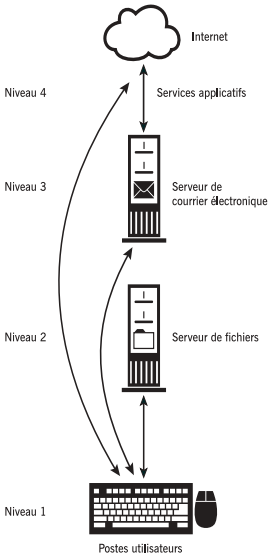
On peut considérer l'infrastructure informatique d'une entreprise comme ayant quatre niveaux :

1 **Les postes utilisateurs** : ce niveau constitue le coeur de l'entreprise et comprend les ordinateurs de bureau individuels, les portables ainsi que toutes les autres machines pour utilisateur final utilisées par les employés.

2 **Les serveurs de fichiers locaux** : ce niveau, situé au-dessus de celui des postes utilisateurs, contient les données et les applications partagées par les ordinateurs de toute l'entreprise.

3 **Les serveurs de courrier électronique** : ce niveau, situé à la périphérie de l'entreprise, est le passage de tout le trafic de courriers électroniques entrants et sortants de l'entreprise.

4 **Les services applicatifs (gérés par des tiers)** : il s'agit du niveau le plus éloigné du centre de l'infrastructure informatique. Il peut résider à l'intérieur ou à l'extérieur de l'entreprise, mais dans les deux cas, le logiciel en cours d'exécution dans le cadre du service est géré par un tiers comme un FAI (Fournisseur d'Accès Internet).



Caractéristiques spécifiques à chaque niveau

Niveau 1 : les postes utilisateurs

Il s'agit de la zone la plus vulnérable d'une entreprise car le contrôle de l'ordinateur reste en grande partie dans les mains de l'utilisateur. L'administrateur peut, jusqu'à un certain point, "verrouiller" les ordinateurs, en particulier sous Windows 2000 et Mac OS X, mais ce contrôle est pratiquement impossible sous Windows 95/98 ou avec d'anciens ordinateurs Macintosh. La vulnérabilité des ordinateurs de bureau et des portables vient du fait qu'ils sont le foyer de réception de tous les types de données, non seulement celles issues de serveurs de fichiers ou de courrier électronique, mais aussi celles provenant du trafic web de type HTTP, de transferts de fichiers de type FTP, des CD-ROM, des assistants électroniques synchronisés, etc.

Les postes utilisateurs sont les plus difficiles à gérer car l'entreprise en compte généralement beaucoup. En fait, la plupart des entreprises estiment qu'il leur est difficile de connaître le nombre exact d'ordinateurs qu'elles possèdent.

Niveau 2 : les serveurs de fichiers

En général, les entreprises ont beaucoup moins de serveurs de fichiers que de postes utilisateurs. En outre, comme les administrateurs ont davantage de contrôle sur ce qui figure sur chaque serveur, les fonctionnalités dont disposent les utilisateurs finaux pour accéder aux machines sont régulées beaucoup plus efficacement. Bien qu'utilisant les données partagées présentes sur ces serveurs, les utilisateurs finaux n'ont pas de contrôle sur ces paramètres. Unix, Windows NT/2000 et NetWare comptent parmi les systèmes d'exploitation les plus utilisés comme serveurs de fichiers.

Niveau 3 : les serveurs de courrier électronique

Situés à la passerelle, les serveurs de courrier électronique traitent le transit de courriers électroniques entrants ou sortants. Ils prennent en charge les protocoles comme SMTP (Simple Mail Transfer Protocol) ainsi que les logiciels de courrier électronique comme Lotus Notes/Domino et Microsoft Exchange.

D'après une enquête menée de janvier à mars 2000 pour Pitney Bowes, un employé type gère, selon Fortune 1000, 50 courriers électroniques par jour[(1)]. Certaines grandes entreprises peuvent recevoir plus de 50 000 messages électroniques par jour, d'autres près d'un million. D'après IDC (International Data Corporation), près de 35 milliards de courriers électroniques seront transmis quotidiennement[(2)] d'ici 2005. Ce niveau de trafic, combiné avec la prolifération des virus de courrier électronique "email-aware", signifie que le courrier électronique est désormais le chemin principal emprunté par les virus pour entrer dans les entreprises. Il arrive que certaines entreprises arrêtent quotidiennement des dizaines ou même des centaines de virus à la passerelle.

Niveau 4 : les services applicatifs

Bien que devenant de plus en plus populaires ces dernières années, les "services applicatifs gérés par des tiers" constituent le niveau le moins facilement définissable des quatre. Le terme s'applique essentiellement à une entreprise tierce qui combine un certain nombre de fonctionnalités et de logiciels en un service qu'elle gère au nom d'une autre entreprise. En utilisant ce type de service géré, l'entreprise s'affranchit des charges administratives que représente la gestion du processus.

Le Fournisseur d'Accès Internet (FAI) est un exemple de société offrant des services applicatifs. Une entreprise peut choisir de faire transmettre ses courriers électroniques par un FAI et de les lui faire contrôler pour y vérifier la présence de virus, de spams, de pornographie, etc. C'est ensuite au FAI de décider des mesures appropriées à prendre, s'il convient ou non de transmettre le courrier électronique. Ce service est facturé par le FAI à l'entreprise.

Le serveur dédié de type "appliance" est une autre forme de service applicatif. Situé à la périphérie du réseau, il s'agit généralement d'un serveur spécialisé qui contrôle le trafic entrant et sortant d'une entreprise. Autonome, ce serveur peut, outre le logiciel antivirus, contenir d'autres logiciels, comme un pare-feu. En général, l'entreprise ne peut ajouter aucun de ses logiciels sur le système. Ces serveurs sont gérés à distance par la société qui les vend.

Efficacité du contrôle viral à chaque niveau

Niveau 1 : les postes utilisateurs

Les postes de travail fixes et mobiles constituent le niveau le plus important pour le contrôle de la présence de virus. C'est vers ce niveau que convergent toutes les données provenant de toutes les sources possibles. C'est ici seulement que peut avoir lieu le contrôle des fichiers présents sur les CD-ROM, sur les assistants électroniques lors de leur synchronisation, sur les disquettes, etc. A ce niveau également, les courriers électroniques et leurs pièces jointes peuvent être contrôlés. Si, pour une raison quelconque, le logiciel antivirus est absent de la passerelle ou s'il n'est pas à jour, l'infection du réseau par des virus pourra quand même être bloquée par le poste de travail. Le trafic HTTP provenant du web peut aussi être contrôlé (certaines entreprises préfèrent appliquer une protection supplémentaire au trafic HTTP/FTP, par exemple à la passerelle ; cependant, lorsque la dégradation des performances que cela induit est mise dans la balance face à la menace réelle, qui est faible, la plupart préférent compter uniquement sur le poste de travail pour piéger le virus provenant du trafic HTTP/FTP).

L'une des raisons importantes pour lesquelles un logiciel antivirus doit être installé sur chaque ordinateur est qu'il s'agit du seul endroit où les données chiffrées, comme celles qui utilisent le protocole SSL (Secure Sockets Layer) pour des transactions sûres de type Internet, peuvent être vérifiées. Tant qu'ils ne sont pas déchiffrés, les fichiers chiffrés ne peuvent être vérifiés par aucun logiciel antivirus.

Les difficultés qu'entraîne le contrôle à ce niveau de l'infrastructure informatique viennent des problèmes administratifs généraux que pose la gestion des postes utilisateurs. Le nombre élevé de machines impliquées peut être en soi source d'erreurs. Si les directives de l'administrateur ne sont pas rigoureusement appliquées et suivies, les utilisateurs peuvent trafiquer les paramètres et compromettre la sécurité du réseau. Par ailleurs, il va sans dire qu'un logiciel antivirus est efficace uniquement s'il est maintenu à jour.

Niveau 2 : les serveurs de fichiers

Le contrôle de ce niveau est beaucoup plus direct car on compte généralement moins de serveurs que de postes de travail et les premiers sont beaucoup plus faciles à gérer pour un administrateur.

Très récemment encore, beaucoup d'entreprises se fiaient à des contrôles planifiés sur le serveur ; si un fichier infecté parvenait à atteindre le serveur, la vérification du système pouvait empêcher son ouverture si un utilisateur tentait d'y accéder. Pourtant, l'émergence de nouveaux types de virus comme W32/Nimda, un virus

Windows 32 qui se propage de manière agressive via partages réseau, courriers électroniques et sites Web, a entraîné un renforcement des contrôles effectués sur les serveurs de fichiers. Alors que, par le passé, certaines entreprises préféraient utiliser seulement le contrôle à la demande et programmé sur les serveurs, l'introduction du contrôle sur accès est désormais considérée comme un moyen efficace d'être rapidement averti de l'entrée d'un virus dans l'entreprise et d'empêcher sa propagation rapide sur le réseau.

Le contrôle au niveau des serveurs de fichiers a cependant une limite : toutes les données présentes dans l'entreprise ne sont pas visibles à ce niveau et les fichiers de CD-ROM/DVD, le trafic HTTP/FTP, etc. aboutissent directement sur les postes de travail, sans passer par ces serveurs.

Niveau 3 : les serveurs de courrier électronique

Depuis l'arrivée du ver de macro Word WM97/Melissa en mars 1999, le nombre de virus et de vers de courrier électronique a connu un essor sans précédent. Les exemples les plus significatifs sont le virus W32/Magistr, les vers Visual Basic Script comme Love Bug (VBS/Loveletter) et VBS/Kakworm ou le ver Windows 32, W32/Klez. Ces virus et ces vers tentent de se propager de différentes manières, le plus fréquemment en s'envoyant sous la forme d'une pièce jointe à un courrier électronique à certaines adresses du carnet du destinataire ou à l'ensemble d'entre elles. Ainsi, en un temps très court, des centaines de milliers d'utilisateurs peuvent être infectés. Etant donné la rapidité d'exécution de l'opération et le nombre de "victimes", le contrôle à la passerelle s'avère maintenant presque aussi important que le contrôle sur les postes de travail.

En effectuant des contrôles à la passerelle, l'entreprise supprime la menace avant qu'elle n'atteigne les postes de travail. Cela fait gagner un temps précieux à l'administrateur puisque, au lieu de traiter le problème sur chaque poste, il n'a plus à le faire qu'à un seul endroit, le serveur de courrier électronique. Le fait d'empêcher un virus d'accéder au réseau fait également gagner du temps à l'ensemble de l'entreprise. En effet, l'irruption de vers comme Love Bug avait complètement interrompu le fonctionnement des réseaux d'entreprise et paralysé l'activité commerciale. Des vers comme W32/Sircam avaient ajouté en pièces jointes des documents trouvés sur le disque dur et les avaient transmis, compromettant ainsi l'intégrité et la confidentialité des données des entreprises ainsi que leur réputation.

Les logiciels antivirus de passerelle contrôlent les courriers électroniques et leurs pièces jointes lorsqu'ils entrent et sortent de l'entreprise. Les produits de courrier électronique incluent par ailleurs un contrôle des boîtes aux lettres et des bases de données, ce qui signifie que si des virus n'ont pas été détectés lors du contrôle en temps réel initial (par exemple, s'il y a eu un retard dans la mise à jour des logiciels antivirus), ils sont piégés lors d'un contrôle programmé ou à la demande ultérieur.

En termes de temps, de coûts et de réputation, le contrôle des courriers électroniques à l'entrée et à la sortie de l'entreprise est donc clairement recommandé. Cependant, comme pour les serveurs de fichiers, la limite est que ces serveurs n'interceptent pas toutes les données circulant dans l'entreprise, et il faut donc ne pas omettre de contrôler au niveau du poste de travail les données provenant de supports de type utilisateur et les courriers chiffrés.

Niveau 4 : services applicatifs

Le recours à un prestataire de services applicatifs pour gérer les opérations de protection de vos données à la périphérie de l'entreprise présente un avantage

important : les administrateurs peuvent ainsi libérer du temps pour d'autres tâches. En outre, les coûts induits par la mise en place d'une protection à ce niveau sont beaucoup plus faciles à déterminer que pour n'importe quel autre niveau.

Par contre, ces avantages sont contrebalancés par l'absence complète de contrôle du processus par l'entreprise ou par l'administrateur. L'entreprise est quasiment dépendante des paramètres, des décisions et de l'efficacité du prestataire de services. Si des problèmes pratiques surgissent, par exemple en matière d'acheminement des données, l'entreprise ne peut rien faire. Des problèmes de respect des informations privées doivent par ailleurs être considérés car cette approche signifie que le personnel situé hors de l'entreprise peut visualiser les données contenues dans les courriers électroniques. Si le service est exécuté via un serveur de type "appliance", l'entreprise peut exercer un contrôle plus fort, mais l'équipement est quand même géré par une société tierce.

Choix d'une solution antivirus

Au moment d'analyser les facteurs qui affectent le choix d'une solution antivirus, il faut déterminer ses priorités entre le besoin de maximiser la sécurité et celui de minimiser les coûts. Une protection au niveau 4, celui des services applicatifs, minimise les coûts alors qu'une protection au niveau 1 accorde plus d'importance à la sécurité.

Il va sans dire que toutes les entreprises devraient être protégées au niveau 1, celui des postes utilisateurs. Les solutions proposées par les éditeurs de logiciels antivirus diffèrent, mais Sophos, par exemple, inclut automatiquement une protection du serveur de fichiers avec les licences pour les postes de travail.

Après avoir protégé les niveaux 1 et 2, les entreprises peuvent alors choisir de protéger les niveaux 3 et/ou 4 en fonction des coûts et des problèmes de sécurité que cela implique. Le fait de mettre en place un logiciel antivirus au niveau 3, à la passerelle, donne à l'entreprise davantage de contrôle ainsi qu'une meilleure garantie de respect des informations privées. En revanche, confier sa protection antivirus à un fournisseur de services applicatifs (au niveau 4) peut être la meilleure solution pour une entreprise où le facteur coût est prédominant.

Certaines entreprises préfèrent utiliser deux fournisseurs : un pour les niveaux 1 et 2 et un autre pour les niveaux 3 ou 4. Les principaux éditeurs de logiciels antivirus fournissent les mêmes niveaux élevés de détection : ils coopèrent pour s'assurer que cela reste le cas. Leurs différences reposent plutôt sur le niveau et la qualité du support technique qu'ils offrent. Quant à l'utilisation de deux fournisseurs différents, comme la plupart des sujets abordés dans ce document, il s'agit de choisir le meilleur compromis. Dans ce cas, il s'agit d'un compromis entre la tranquillité d'esprit qu'apporte le doublement des fournisseurs et les coûts supplémentaires que représentent l'acquisition et l'administration de deux produits distincts.

Sources

1 "Pitney Bowes messaging study highlights differences in communications strategies among workers in small, medium and large businesses", Communiqué de presse, 21 août 2000

2 http://one.ie/report/email/marketoverview.asp