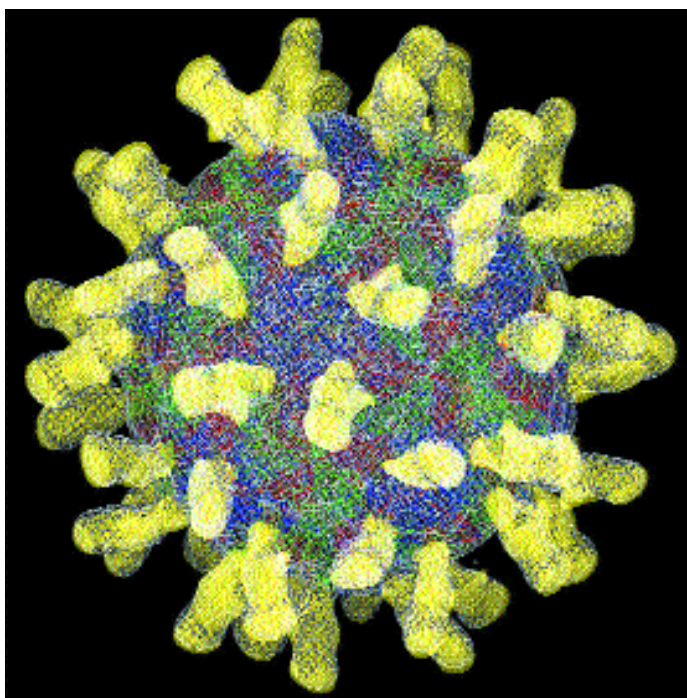


Attaques informatiques

Antivirus : une technologie obsolète?

DEFERLANTE. Le 19 juillet 2001, Code Red infectait 250 000 ordinateurs en l'espace de 9 heures. Quelque temps après, c'était au tour de Nimda. Puis, cette année, du virus Klez, qui se propage par la messagerie.



Attention! Les virus sont de plus en plus nombreux et malins.

Au cours de ces 24 derniers mois, tout un chacun a pu se rendre compte des ravages que les attaques informatiques peuvent causer aux entreprises, ainsi qu'aux particuliers. Il ne passe pas un jour sans qu'un nouveau virus soit découvert. Sans que l'on

trouve de nouvelles vulnérabilités sur les systèmes informatiques. On assiste surtout à un véritable changement du paysage des attaques informatiques. La communauté des «hackers» ou «black hats» est en pleine progression. Elle dispose d'une mine d'informations, par le biais de sites internet, de revues, de conférences (Defcon, etc.), d'écoles. Elle est de mieux en mieux organisée.

Les attaques sont de plus en plus sophistiquées. Mais, paradoxalement, les outils pour les mener sont de plus en plus simples à utiliser. Des hackers en herbe (les «script kiddies») peuvent s'en servir sans pour autant avoir de connaissances pointues en informatique. Et les pertes pour les entreprises se chiffrent en millions de francs.

Il existe un grand nombre d'attaques informatiques, mais, dans cet article, nous allons nous concentrer plus particulièrement sur les virus au sens large du terme.

Les antivirus traditionnels

L'approche classique pour se défendre contre les virus consiste à mettre en place toute une série d'outils pour protéger les biens informatiques. Généralement, tous les postes de travail – et les serveurs – sont équipés d'un antivirus (AV) récent. La mise à jour des signatures est effectuée de manière régulière. La passerelle de messagerie analyse les messages entrant et sortant, ainsi qu'éventuellement, les flux HTTP et FTP. Toutes ces mesures sont bien évidemment nécessaires.

Les limites de l'approche actuelle

Les antivirus actuels fonctionnent selon une approche par signature. Chaque virus est identifié par une signature unique et il est répertorié comme tel. Pour détecter un virus, l'AV parcourt les fichiers, les messages, les flux FTP et HTTP. Il cherche ainsi à identifier une signature listée dans sa base de données. Il devient dès lors crucial de

e-Xpert Solutions SA

Au bénéfice d'une longue expérience dans les secteurs financiers et industriels, e-Xpert Solutions SA propose à sa clientèle des solutions «clé en mains» dans le domaine de la sécurité informatique des réseaux et des applications. Des solutions qui vont de la sécurité d'architecture – tel le firewall, VPN, IDS, FIA, le contrôle de contenu, l'antivirus – aux solutions plus avant-gardistes comme la prévention des intrusions (approche comportementale), l'authentification forte, la biométrie, les architectures PKI ou encore la sécurisation des OS Unix et Microsoft et des postes clients (firewall personnel).

mettre à jour régulièrement cette base de données.

Le logiciel antivirus est mis à jour quasiment en temps réel. Cette méthode, basée sur les signatures, n'en pose pas moins plusieurs problèmes.

Malgré les mises à jour rapides (côté client), un certain temps est nécessaire aux éditeurs d'AV pour analyser les nouveaux virus et actualiser leurs bases de données. Ce délai peut être trop long dans certains cas. Les statistiques montrent en effet une forte tendance à la propagation très rapide des virus. Cette propagation est directement liée à l'utilisation des e-mails et des services internet. Il devient alors de plus en plus difficile pour les éditeurs d'AV d'assurer, à temps, une mise à jour des bases de données.

Le deuxième problème est que cette méthode ne permet pas de détecter les virus inconnus. A savoir, les virus non répertoriés dans la base de données. Or, il existe des outils extrêmement simples et efficaces pour générer des virus. Ceux-ci sont donc à la portée des non-spécialistes et sont d'une facilité d'utilisation impressionnante. Il est possible, avec ces outils, de choisir son mode de propagation, l'action que doit effectuer le virus lorsqu'il atteint sa cible (comme installer une «backdoor»), etc. Les possibilités sont pratiquement illimitées et ouvrent la porte à de nouvelles formes d'attaques.

Un autre problème est la mise à jour des bases online, réali-

sées de plus en plus sur Internet. Dans certains cas, il peut être difficile, voire impossible, de les mettre à jour. Les raisons peuvent en être multiples: saturation du réseau Internet, saturation de l'éditeur AV, attaques de type déni de services.

Comment stopper les attaques inconnues?

Entre l'apparition de nouveaux virus et la mise à jour des signatures, il existe un fossé temporel. La tendance montre que ce fossé va devenir de plus en plus grand. Pour résoudre ce problème, une approche intéressante est l'analyse comportementale. Cette technologie fait partie de la famille des outils de prévention d'intrusions. L'idée de base est de mettre en œuvre une solution capable de détecter et de stopper les attaques inconnues.

L'approche comportementale

L'approche comportementale consiste à analyser, en temps réel, les applications et le système d'exploitation. L'idée est de détecter le comportement malicieux d'un programme : par exemple, le web serveur IIS essayant d'accéder à des fichiers système sensibles. Ce comportement est alors bloqué par le logiciel de protection.

Ces systèmes sont généralement capables de prévenir les actions suivantes :

- ouverture, visualisation, modification ou effacement de fichiers;
- tentative de formatage des disques;

- accès aux périphériques machines (CD-Rom, USB, carte réseau, etc.);
- modification des paramètres système;
- initialisation de la communication réseau;
- exécution de scripts malicieux (code mobile);
- prévention contre les «Buffer Overflow» (BoF).

Cette méthode nécessite un «apprentissage» préalable afin de connaître le comportement dit «normal» de la machine. Une fois ce comportement appris, le système est opérationnel et permet de protéger les machines de façon très efficace.

Où installer ces logiciels?

Pour la mise en œuvre de ces solutions, je recommanderai deux axes : la sécurisation des serveurs et la sécurisation des postes clients

Sécurisation des serveurs

Les infrastructures serveurs d'une entreprise sont des éléments très importants. Pour garantir leur intégrité et leur disponibilité, l'installation de logiciels d'analyse comportementale est une solution très intéressante. Dans un premier temps, il peut être intéressant de protéger les serveurs les plus sensibles, comme les frontaux de la DMZ ou les serveurs internes (ERP, DB, applications financières, etc.).

Sécurisation des postes clients

La plupart des postes clients ont un accès à la messagerie inter-

net et peuvent ainsi surfer sur le Web. Il devient dès lors vital de les protéger contre les nouvelles attaques et notamment contre les «backdoors» et autres virus.

Il existe des solutions pour sécuriser ces postes. Elles utilisent la technologie comportementale et sont généralement couplées à un «firewall» personnel. Pour la mise en œuvre de telles solutions dans le cadre d'une entreprise, il est important de ne pas négliger la gestion centralisée de ces logiciels.

Vers des solutions d'analyse du comportement

Il ne fait plus de doutes que les attaques informatiques sont de plus en plus efficaces et virulentes. Les solutions antivirus ne sont, à mon avis, plus suffisantes pour assurer la protection des biens informatiques. Cela ne veut pas dire qu'il ne faut plus y avoir recours. Je pense toutefois qu'il est et qu'il sera désormais plus important, pour faire face aux nouvelles menaces, de se diriger vers des solutions d'analyse du comportement. Ces outils sont complémentaires aux antivirus. ●

Sylvain Maret
Directeur veille
technologique

Contact

e-Xpert Solutions SA
Route de Pré-Marais 29
1233 Bernex (GE)
Tél : +41 22 727 05 55
info@e-xpertsolutions.com

