

Pourquoi un seul moteur antivirus ne suffit pas

Des moteurs anti-virus multiples sont nécessaires pour réduire le lapse de temps entre l'apparition d'un virus et la mise à jour d'une signature

Ce livre blanc explique l'importance du temps de réponse. Il expose les différences entre les moteurs anti-viraux et explique pourquoi le fait d'avoir des scanners multiples au niveau du serveur réduit le temps de réponse d'où les chances d'être affecté par le virus.



Introduction

Les entreprises responsables et organisées s'accordent pour dire qu'elles ont besoin de protéger leurs réseaux contre les attaques virales en installant un produit de sécurisation de messagerie. Le problème reste de savoir comment faire le bon choix de moteur antiviral parmi toutes les solutions disponibles? Et aussi, un seul moteur antivirus est-il suffisant pour bien protéger le réseau interne de tous les virus, vers, et autres menaces emails?

Ce livre blanc explique pourquoi plusieurs moteurs antivirus sont nécessaires dans le but de réduire le temps de réaction à l'apparition d'un nouveau virus, et par là même les chances d'infections de votre réseau. L'utilisation de moteurs antivirus multiples permet aussi aux administrateurs chargés de la sécurité du réseau d'être développeurs indépendants quand il s'agit des antivirus, les laissant utiliser ce qui se fait de mieux en termes de moteurs antivirus disponibles sur le marché.

2
.2
.3
.3
4
.5

Le besoin d'une réaction rapide

Un des facteurs les plus importants pour une protection effective de votre réseau contre les attaques virales est la rapidité à laquelle vous recevez les nouveaux fichiers de signatures antivirales à la sortie d'un nouveau virus. Les emails permettent aux virus de se répandre à la vitesse de la lumière, et un seul virus email suffit à infecter l'intégralité de votre réseau. C'est alors qu'il est crucial de savoir combien de temps les fichiers de signatures de votre solution antivirus prendront pour être mis à jour lorsqu'un nouveau virus apparaît.

Une étude menée par le gouvernement Britannique de 2004 a trouvé, par exemple, que bien que 99% des grandes entreprises anglaises utilisent des produits antivirus, 68% d'entre elles étaient infectées par des virus en 2003, largement dû au fait que les mises à jour des signatures n'avaient pas été déployées assez rapidement.

Chaque fournisseur d'antivirus du marché annoncera que son produit a le temps de réaction le plus rapide. Toujours est-il qu'en réalité, il en est différemment. Alors qu'en moyenne, certaines entreprises sont plus compétentes que d'autres, il n'existe pas de compagnie qui soit toujours la première et la plus rapide à réagir à l'apparition d'un virus. Il faut avouer que certaines compagnies sont plus rapides à plusieurs occasions, mais jamais la même compagnie ne fournira en premier une protection virale. Une fois il s'agira de Kaspersky, ensuite de McAfee,



une autre fois de BitDefender ou Norman, et ainsi de suite.

Cas: Réaction au virus Sober

Le tableau ci-dessous montre les temps de réaction des compagnies d'antivirus (CET) lors de l'apparition de W32/Sober.C (ver détecté le 20 Décembre 2003 à 03h00, CET).

Compagnie	Temps de réaction
BitDefender	2003-12-20 at 13:20 h
Kaspersky	2003-12-20 at 14:45 h
F-Prot (Frisk)	2003-12-20 at 15:25 h
F-Secure	2003-12-20 at 15:45 h
Norman	2003-12-20 at 18:25 h
eSafe (Alladin)	2003-12-20 at 18:35 h
Trend Micro	2003-12-20 at 19:50 h
AVG (Grisoft)	2003-12-20 at 20:15 h
AntiVir (H+BEDV)	2003-12-20 at 22:20 h
Symantec	2003-12-21 at 04:05 h
Avast! (Alwil)	2003-12-21 at 09:55 h
Sophos	2003-12-21 at 14:35 h
Panda AV	2003-12-21 at 17:05 h
McAfee/NAI	2003-12-22 at 04:10 h
Ikarus	2003-12-22 at 10:35 h

Données extraites du VirusBTN de Février 2004

Il est clair que les différences s'échelonnent d'heures en jours. Symantec par exemple a mis plus d'une journée pour déployer des nouveaux fichiers de signatures – assez de temps pour que votre réseau soit infecté!

La raison pour des moteurs antivirus multiples

Malheureusement un moteur au temps de réaction moyen le plus rapide ne vous sera d'aucune aide si ce moteur n'est pas le plus rapide pour un certain virus, ce qui résulterait à l'infection de votre réseau pour cette fois là. Etant donné l'incapacité de n'importe quel moteur antivirus individuel à toujours être le premier à lancer une mise à jour de signature pour un nouveau virus, le bon sens veut qu'en combinant des moteurs multiples, les chances qu'au moins l'un d'entre eux soit mis à jour à temps augmentent, avec quoi les chances qu'un réseau soit protégé.

En d'autres termes, posséder trois ou quatre moteurs antivirus augmente trois fois vos chances



de protéger votre réseau. Ainsi, vous n'avez pas besoin d'espérer que votre seul fournisseur soit le plus rapide à réagir à chaque fois et vous pouvez à la place être couvert par trois ou quatre fournisseurs.

A propos de GFI MailSecurity for Exchange/SMTP

GFI MailSecurity for Exchange/SMTP est une solution de vérification du contenu, détection d'exploits, scanneur de chevaux de Troie et d'exécutables, analyse de menaces et antivirus, qui enlève tout type de menaces basées sur les emails avant qu'il n'affectent vos utilisateurs de messagerie. Les fonctions-clés de GFI MailSecurity comprennent plusieurs moteurs d'antivirus, pour un taux de détection plus élevé et une réponse plus rapide face à de nouveaux virus; une fonction de vérification du contenu et des pièces jointes de messagerie, pour mettre en quarantaine les pièces jointes et les contenus dangereux; un bouclier contre les exploits, pour se protéger des virus existants et futurs basés sur des exploits (par exemple Nimda, Bugbear); un moteur de menaces HTML, pour désactiver les scripts HTML; un scanneur de chevaux de Troie et d'exécutables, pour détecter des exécutables dangereux, et plus encore. Pour plus d'informations et pour télécharger une version d'évaluation complète, veuillez aller à la page http://www.gfi.com/fr/mailsecurity/.



A propos de GFI Software

GFI Software est l'un des leaders dans le domaine de la sécurité de réseau, de la sécurité du contenu et des logiciels de messagerie. Ses produits-clés comprennent le connecteur fax GFI FAXmaker for Exchange et serveur fax sur réseau ; GFI MailSecurity, vérification du contenu / d'exploits et antivirus ; GFI MailEssentials, progiciel anti-spam basé sur le serveur ; GFI LANguard Network Security Scanner (N.S.S.) qui vérifie la sécurité du réseau et permet aux administrateurs d'installer à distance les patchs et services packs ; GFI Network Server Monitor, qui envoie automatiquement des alertes et corrige les problèmes du réseau et des serveurs; et GFI LANguard Security Event Log Monitor (S.E.L.M.) qui effectue une détection d'intrusion et une gestion de journaux d'événement sur l'ensemble du réseau ; et GFI LANguard Portable Storage Control qui permet de surveiller les média amovibles sur l'ensemble du réseau. Les clients de GFI Software comprennent Microsoft, Telstra, Time Warner Cable, Shell Oil Lubricants, NASA, DHL, Caterpillar, BMW, US IRS et USAF. GFI Software est installé aux Etats-Unis, au Royaume-Uni, en Allemagne, à Chypre, en Roumanie, en Australie et à Malte et opère par le biais d'un réseau mondial de distribution. GFI Software est un partenaire certifié Microsoft Gold et a remporté le titre de progiciel de l'année « Microsoft Fusion (GEM) Packaged Application Partner of the Year ». Pour plus d'information à propos de GFI, visitez http://www.gfsfrance.com.

© 2005 GFI Software Ltd. Tous droits réservés. L'information contenue dans ce document représente la position actuelle de GFI Software concernant les questions citées à la date de publication. GFI Software doit répondre à des conditions de marché variables, le présent document ne doit donc pas être interprété comme un engagement de la part de GFI Software, et GFI Software ne peut garantir la véracité des informations présentées après la date de publication. Ce document blanc est offert uniquement à titre d'information. GFI SOFTWARE NE PROCEDE A AUCUNE GARANTIE EXPRESSE OU IMPLICITE DANS LE PRESENT DOCUMENT. GFI Software, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI LANguard, GFI Network Server Monitor, GFI DownloadSecurity et le logo sont soit des marques commerciales ou des marques déposées de GFI Software Ltd. aux Etats-Unis et/ou ailleurs. Tous les noms de produits ou de sociétés cités dans la présente peuvent être les marques déposées de leurs propriétaires respectifs.

