

Sicherheitsgefahren durch unzureichenden Schutz mit nur einer Anti-Viren-Engine

Warum sich Wartezeiten bei Signatur-Updates nach neuen Virenausbrüchen nur mit mehreren Engines sicher überbrücken lassen

Dieses White Paper befasst sich mit der Bedeutung der Response-Zeit bei Signatur-Updates und welche Unterschiede es zwischen Anti-Viren-Engines im Hinblick auf die Schnelligkeit der Aktualisierung gibt. Erfahren Sie, warum der gleichzeitige Einsatz gleich mehrerer Scanner auf Mail-Server-Ebene zur Verringerung der durchschnittlichen Wartezeiten bei Updates führt und somit die Gefahr durch Vireninfectionen verringert wird.

Einführung

Verantwortungsbewusste Organisationen sind sich bewusst, dass sich ihre Netzwerke nur durch die Verwendung einer E-Mail-Sicherheitslösung vor böswilligen Virenangriffen schützen lassen. Es ist jedoch nicht einfach, bei der Vielzahl aktuell verfügbarer Scan-Engines die für ein Unternehmen am besten geeignete Sicherheitslösung auszuwählen. Zudem ist fraglich, ob sich interne Netzwerke nur durch den Einsatz einer einzelnen Anti-Viren-Engine zuverlässig vor Mass-Mailing-Viren, Würmern und anderen per E-Mail verbreiteten Gefahren hinreichend absichern lassen.

In diesem White Paper wird erläutert, warum nach einem Virenausbruch die durchschnittliche Wartezeit für aktualisierte Virensignaturen nur mit mehreren Anti-Viren-Engines minimiert werden kann – und somit die Gefahr sinkt, dass das Netzwerk infiziert wird. Des Weiteren wird darauf eingegangen, warum der Einsatz mehrerer Anti-Viren-Engines Administratoren eine größere Unabhängigkeit beim Viren-Scanning bietet und ihnen die Möglichkeit bietet, die Scan-Engines einzusetzen, die sich als am leistungsfähigsten erwiesen haben.

Einführung	2
Warum schnelle Reaktionszeiten so wichtig sind	2
Ein Beispiel aus der Praxis: Reaktionszeiten bei Updates für den Sober-Virus	3
Überzeugende Argumente für den Einsatz mehrerer Anti-Viren-Engines	3
Über GFI MailSecurity for Exchange/SMTP	4
Über GFI	5

Warum schnelle Reaktionszeiten so wichtig sind

Ob ein Netzwerk erfolgreich vor Viren geschützt werden kann, hängt maßgeblich davon ab, wie schnell die Viren-Signaturen der Engine nach einem neuen Virenausbruch aktualisiert werden. Viren werden mittlerweile innerhalb weniger Stunden weltweit per E-Mail verbreitet. Ein einziger über die elektronische Post eingeschleppter Schädling reicht bereits aus, um ein ganzes Netzwerk zu infizieren. Daher ist es umso wichtiger, dass aktualisierte Signaturdateien so schnell wie möglich bereitgestellt werden.

Eine von der britischen Regierung Anfang 2004 in Auftrag gegebene Studie ergab, dass 99% der großen Unternehmen in Großbritannien zwar Anti-Viren-Produkte einsetzen, 68% von ihnen aber dennoch im Jahr 2003 von Viren infiziert wurden – vorrangig, weil die Installation von Signatur-Updates nicht schnell genug erfolgt war.

Jeder Anti-Viren-Hersteller behauptet, am schnellsten auf neue Viren reagieren und Updates zur Verfügung stellen zu können. In der Praxis, so hat sich herausgestellt, können diese Versprechungen jedoch nicht eingehalten werden. Es gibt zwar einige Hersteller, die im Allgemeinen schneller auf Virenausbrüche reagieren als ihre Mitbewerber, aber keinen, der

stets als Erster seine Updates zur Verfügung stellt. Kaspersky, McAfee, BitDefender, Norman und andere Anti-Viren-Hersteller stehen daher mit ihren Response-Zeiten abwechselnd an der Spitze.

Ein Beispiel aus der Praxis: Reaktionszeiten bei Updates für den Sober-Virus

Die folgende Tabelle bietet einen Überblick über den Zeitpunkt, zu dem die einzelnen Anti-Viren-Hersteller mit ihren Updates auf den Ausbruch von W32/Sober.C reagiert haben (MEZ). Der Wurm wurde am 20. Dezember 2003 um 03:00 Uhr MEZ entdeckt.

Hersteller	Veröffentlichung der Signatur-Updates
BitDefender	20.12.03 um 13:20:00 Uhr
Kaspersky	20.12.03 um 14:45:00 Uhr
F-Prot (Frisk)	20.12.03 um 15:25:00 Uhr
F-Secure	20.12.03 um 15:45:00 Uhr
Norman	20.12.03 um 18:25:00 Uhr
eSafe (Alladin)	20.12.03 um 18:35:00 Uhr
Trend Micro	20.12.03 um 19:50:00 Uhr
AVG (Grisoft)	20.12.03 um 20:15:00 Uhr
AntiVir (H+BEDV)	20.12.03 um 22:20:00 Uhr
Symantec	21.12.03 um 04:05:00 Uhr
Avast! (Alwil)	21.12.03 um 09:55:00 Uhr
Sophos	21.12.03 um 14:35:00 Uhr
Panda AV	21.12.03 um 17:05:00 Uhr
McAfee/NAI	22.12.03 um 04:10:00 Uhr
Ikarus	22.12.03 um 10:35 Uhr

Quelle: VirusBTN, Ausgabe Februar 2004

Wie deutlich zu sehen ist, reicht die Reaktionszeit von ein paar Stunden bis zu mehreren Tagen. Symantec hat zum Beispiel länger als einen Tag gebraucht, bis neue Signatur-Dateien zur Verfügung gestellt wurden – genug Zeit für den Virus, mit Symantec-Software geschützte Systeme zu infizieren!

Überzeugende Argumente für den Einsatz mehrerer Anti-Viren-Engines

Leider reicht es nicht aus, eine Scan-Engine einzusetzen, die die schnellsten *durchschnittlichen* Response-Zeiten aufweist, wenn gerade diese Engine bei einem der vielen neu auftretenden

Viren doch einmal nicht schnell genug aktualisiert werden kann. Der gleichzeitige Einsatz mehrerer Anti-Viren-Lösungen minimiert somit das Risiko, durch zu lange Wartezeiten bei Signatur-Updates für einen neuen Virus anfällig zu sein. So besteht eine hohe Wahrscheinlichkeit, dass mindestens eine der Engines schnell genug aktualisiert wird, bevor ein Virus zuschlagen kann.

Der Einsatz von drei oder vier Anti-Viren-Engines bietet somit einen mehrfach optimierten Sicherheitsschutz. Anwender müssen sich nicht auf einen einzigen Hersteller verlassen und dabei hoffen, dass dieser immer am schnellsten reagiert, sondern haben dank der anderen Hersteller-Engines einen weitaus größeren Sicherheitspuffer.

Über GFI MailSecurity for Exchange/SMTP

GFI MailSecurity for Exchange/SMTP ist eine umfassende E-Mail-Sicherheitslösung und bietet Inhaltskontrolle, Exploit-Erkennung, Gefahrenanalyse und Anti-Viren-Schutz für elektronische Post. Sämtliche schädlichen Elemente, die sich per E-Mail übertragen lassen, werden beseitigt, bevor sie E-Mail-Anwender erreichen. Zu den wichtigsten Leistungsmerkmalen von GFI MailSecurity zählen unter anderem mehrere Virus-Engines für eine höhere Erkennungsquote und schnellere Gegenmaßnahmen bei neuen Viren, eine E-Mail-Inhalts- und Anhangskontrolle, um gefährliche Inhalte und Anhänge unter Quarantäne zu stellen, ein Exploit-Schutz zur Abwehr von aktuellen und zukünftigen auf Exploits basierenden Viren (z. B. Nimda, Bugbear), eine HTML-Threats-Engine zum Deaktivieren von HTML-Skripten sowie ein Trojan & Executable Scanner zum Aufspüren potenziell gefährlicher exe-Dateien. Weitere Informationen und eine kostenfreie Test-Version von GFI MailSecurity finden Sie unter <http://www.gfi.com/de/mailsecurity/>.

Über GFI

GFI (www.gfisoftware.de) ist ein führender Entwickler und Anbieter von Produkten für Netzwerk- und Inhaltssicherheit sowie von Kommunikationslösungen. Das Produktportfolio von GFI umfasst unter anderem den Fax-Connector GFI FAXmaker für Exchange- und SMTP-Mail-Server, die Sicherheitslösung GFI MailSecurity for Exchange/SMTP zur Überprüfung von E-Mail-Inhalten und zum Schutz vor E-Mail-basierten Exploits und Viren, die Server-basierte Anti-Spam-Software GFI MailEssentials for Exchange/SMTP, die E-Mail-Archivierungslösung GFI MailArchiver, GFI LANguard Network Security Scanner (N.S.S.) für Sicherheits-Scans und Patch-Management, GFI Network Server Monitor zum automatischen Versand von Warnmitteilungen und zur Fehlerbehebung bei Netzwerk- und Server-Problemen, GFI LANguard Security Event Log Monitor (S.E.L.M.) zur Ereignisprotokoll-basierten Eindringlingserkennung und netzwerkweiten Verwaltung von Ereignisprotokollen, GFI LANguard Portable Storage Control (P.S.C.) zur netzwerkweiten Kontrolle wechselbarer Speichermedien sowie GFI WebMonitor zur Überwachung von HTTP/FTP-Verbindungen mit Virenschutz für ISA Server. GFI-Produkte sind im Einsatz bei Microsoft, Telstra, Time Warner Cable, NASA, DHL, Caterpillar, BMW, der US-Steuerbehörde IRS und der USAF. GFI unterhält Niederlassungen in den USA, Großbritannien, Deutschland, Zypern, Rumänien, Australien und Malta und wird von einem weltweiten Netzwerk von Distributoren unterstützt. GFI ist "Microsoft Gold Certified Partner" und erhielt die Auszeichnung "Microsoft Fusion (GEM) Packaged Application of the Year". Weitere Informationen erhalten Sie unter <http://www.gfisoftware.de>.

© 2005 GFI Software Ltd. Alle Rechte vorbehalten. Die in diesem Dokument aufgeführten Informationen geben den von GFI zum Zeitpunkt der Veröffentlichung vertretenen Standpunkt zum Thema des White Papers wieder. Änderungen aufgrund von veränderten Marktbedingungen sind vorbehalten. Die in diesem Dokument präsentierten Informationen stellen keine Verpflichtung seitens GFI dar, und für ihre Genauigkeit wird nach dem Datum der Veröffentlichung keine Garantie übernommen. Dieses White Paper dient nur der Produktinformation. GFI ÜBERNIMMT KEINE AUSDRÜCKLICHE ODER STILLSCHWEIGENDE HAFTUNG FÜR DIE IN DIESEM DOKUMENT PRÄSENTIERTEN INFORMATIONEN. GFI, GFI FAXmaker, GFI MailEssentials, GFI MailSecurity, GFI MailArchiver, GFI LANguard, GFI Network Server Monitor, GFI WebMonitor und die zugehörigen Produkt-Logos sind eingetragene Marken oder Marken von GFI Software Ltd. in den Vereinigten Staaten und/oder anderen Ländern. Alle in diesem Dokument aufgeführten Produkte oder Firmennamen sind Eigentum der jeweiligen Inhaber.

