



GFI MailSecurity

for Exchange/SMTP/Lotus

Virenschutz, Inhaltsrichtlinien, Exploit-Erkennung und Trojaner-Abwehr für E-Mails

Aufgrund des stetig wachsenden E-Mail-Traffics und der damit verbundenen Gefahren ist es notwendiger denn je, elektronische Post auf sicherheitsgefährdende, anzügliche oder vertrauliche Inhalte zu überprüfen. Zerstörerische Viren, die E-Mail-Server und Firmennetzwerke binnen Minuten zusammenbrechen lassen, werden weltweit innerhalb weniger Stunden per E-Mail verbreitet. Sicherheitsprodukte, die zur Absicherung nur eine einzige Anti-Virus-Engine einsetzen, gewährleisten keinen zuverlässigen Schutz. Eine weitaus größere Bedrohung stellen Backdoor-Viren (Trojaner) und andere gefährliche Programme dar, die mit Hilfe von E-Mails eingeschleust werden und Hackern einen Zugang zum Netzwerk verschaffen. Reine Anti-Virus-Produkte bieten keinen ausreichenden Schutz vor E-Mail-Exploits und ähnlichen Angriffen.

Nur durch den Einsatz einer umfassenden Lösung für differenzierte, anwenderbasierte E-Mail-Inhaltsrichtlinien und Virenabwehr lassen sich E-Mail-Server und Netzwerk zuverlässig sichern. GFI MailSecurity übernimmt die Rolle einer "E-Mail-Firewall": Viren, Exploits und ähnliche per elektronische Post übertragene Schädlinge werden bereits auf Server-Ebene abgewehrt – ebenso wie gezielt gegen ein Unternehmen gerichtete E-Mail-Angriffe.

Vorteile

Warum GFI MailSecurity zur Abwehr von E-Mail-Viren und -Malware?

- Unterstützt die branchenführenden Messaging-Plattformen Microsoft Exchange 2000, 2003, 2007 und Lotus Domino
- Unterstützt mehrere Anti-Virus-Engines für eine höhere Viren-Erkennungsrate und schnellere Gegenmaßnahmen
- Spürt dank des leistungsfähigen Trojan & Executable Scanner neue schädliche exe-Dateien OHNE zusätzliche Viren-Updates auf – MyDoom wurde sofort abgewehrt!
- Deaktiviert E-Mail-Exploits und HTML-Skripten per Email Exploit Engine und HTML Sanitizer

■ Virenkontrolle mit mehreren Scan-Engines

GFI MailSecurity setzt zur Überprüfung eingehender E-Mails mehrere Viren-Scanner ein. Der Einsatz verschiedener Scanner verkürzt die durchschnittliche Wartezeit bis zum Erhalt aktualisierter Signatur-Updates und verringert die Gefahr, mit einem neuen Virus infiziert zu werden. Es gibt keinen Anti-Virus-Hersteller, der immer am schnellsten auf akute Bedrohungen reagiert. Wird ein neuer Virus bekannt, hängt ein rasches Bereitstellen entsprechender Updates z. B. davon ab, wo der Schädling entdeckt wurde. Die Verwendung mehrerer Scan-Engines erhöht die Chance, dass mindestens eine von ihnen zeitnah aktualisiert wird und rechtzeitig Schutz bietet. Zudem wendet jede Lösung ihre eigene Heuristik an und besitzt individuelle Abwehrmethoden. Einige Scanner erkennen bestimmte Virenarten samt Untergruppen besser als andere, die wiederum ihre speziellen Stärken haben. Fakt ist: Je mehr Scan-Engines eingesetzt werden, desto umfassender ist der Schutz.

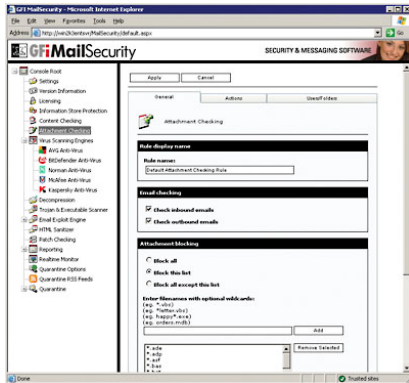
■ Überprüfung auf Trojaner und ausführbare Dateien

Der GFI MailSecurity Trojan & Executable Scanner entdeckt unbekannte böswillige exe-Dateien (z. B. Trojaner), indem er überprüft, welche Auswirkungen das Starten einer ausführbaren Datei hat. Trojaner können unerkannt auf den Rechner eines Benutzers gelangen und einem Angreifer uneingeschränkten Zugriff auf die Daten des Computers ermöglichen. Unbekannte Trojaner werden von herkömmlicher Anti-Virus-Software NICHT identifiziert, da deren Überprüfungen nur auf Signaturen basieren. Der Trojan & Executable Scanner hingegen setzt zuverlässige und intelligente Scan-Methoden ein, die den Gefährdungsgrad einer exe-Datei bestimmen. Die Datei wird disassembliert, die Überprüfung ihrer Prozessabläufe findet in Echtzeit statt, und vorgegebene Aktionen werden mit einer Datenbank bekannter böswilliger Aktionen verglichen. Danach stellt der Scanner sämtliche exe-Dateien unter Quarantäne, von denen verdächtige Aktionen ausgehen, z. B. das Aufnehmen einer Modem- oder Netzwerk-Verbindung oder der Zugriff auf Adressbücher.

GFI MailSecurity



Konfigurationsoberfläche

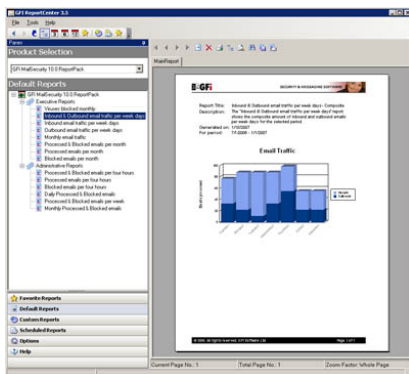


Konfiguration der Anhangskontrolle



Unterstützung mehrerer Anti-Virus-Engines

GFI MailSecurity ReportPack



Benutzeroberfläche

Norman Virus Control & BitDefender bereits im Lieferumfang enthalten

GFI MailSecurity wird im Bundle mit Norman Virus Control und BitDefender ausgeliefert. Norman Virus Control ist eine professionelle Anti-Virus-Engine, die bereits 32 Mal mit dem "Virus Bulletin 100% Award" ausgezeichnet wurde. Zudem ist das Produkt ICISA- und Checkmark-zertifiziert. BitDefender ist eine sehr schnelle und flexibel einsetzbare Anti-Virus-Engine und hebt sich durch die Anzahl der Formate hervor, die erkannt und gescannt werden können. BitDefender ist ebenfalls ICISA-zertifiziert und wurde mit dem "Virus Bulletin 100% Award" und dem "European IT Prize 2002" prämiert. GFI MailSecurity sucht automatisch nach neuen Virendefinitionen für Norman Virus Control und BitDefender und aktualisiert diese ohne Benutzereingriff. Im Preis von GFI MailSecurity ist ein Update-Service für 1 Jahr enthalten.

Anti-Virus-Engines von Kaspersky, McAfee und GRISOFT (optional)

Für noch mehr Sicherheit ist es möglich, die Anti-Virus-Engines von Kaspersky, McAfee und/oder GRISOFT als dritte, vierte oder sogar fünfte zusätzliche Lösung zur Virenabwehr oder als Ersatz für eine der anderen Engines einzusetzen. Kaspersky Anti-Virus ist ICISA-zertifiziert, überzeugt durch seine unübertroffene Scan-Tiefe und wird wegen seiner schnellen Bereitstellung aktualisierter Virensignaturen und der heuristischen Technologie, die unbekannte Viren effizient neutralisiert, geschätzt. Die Stärken der McAfee Anti-Virus-Engine liegen in der Identifizierung von Angriffen, die nicht direkt über Viren, sondern z. B. mit Hilfe von ActiveX-Steuerelementen gestartet werden. GRISOFT entwickelt bereits seit fünfzehn Jahren Anti-Virus-Produkte und ist mit AVG Anti-Virus einer der weltweit führenden Anbieter von Lösungen zur Identifizierung und Analyse von Viren.

Automatisches Entfernen von HTML-Skripten

Die HTML-Fähigkeit von E-Mails ermöglicht es Hackern und Viren-Programmierern, Befehle in HTML-E-Mails einzubinden und diese auszulösen, sobald die Nachricht geöffnet wird. GFI MailSecurity scannt nach Skript-Code im Textkörper der Mitteilung und deaktiviert alle Befehle, bevor die "gesäuberte" HTML-E-Mail an den Empfänger weitergeleitet wird. GFI MailSecurity ist das einzige Produkt, das mit Hilfe einer von GFI patentierten Technologie vor potenziell gefährlichen HTML-E-Mails schützt und HTML-Viren und -Angriffe abwehrt.

Identifizierung von E-Mail-Exploits

GFI ist führend bei der Erforschung von Exploits, die per E-Mail verbreitet werden. Auf Grundlage der Forschungsergebnisse wurde die Email Exploit Engine entwickelt. Mit ihrer Hilfe lassen sich auch zukünftige E-Mail-Viren und -Angriffe erkennen, bei denen bekannte Anwendungs- oder Betriebssystem-Exploits verwendet werden. Zum Beispiel stellten die Viren Nimda und Klez von vornherein keine Gefahr für mit GFI MailSecurity geschützte Netzwerke dar. Beide Viren basieren auf bekannten Exploits, für deren Erkennung kein gesondertes Software-Update der GFI-Lösung notwendig war. In den GFI SecurityLabs werden ständig neue E-Mail-Exploits entdeckt. Alle notwendigen Informationen zum Schutz vor diesen Bedrohungen werden automatisch an GFI MailSecurity weitergeleitet. GFI MailSecurity ist die einzige Software für E-Mail-Sicherheit, mit der sich E-Mail-Exploits identifizieren lassen.

Identifizierung von Spyware

Mit Hilfe des Trojan & Executable Scanner von GFI MailSecurity lassen sich schädliche ausführbare Dateien, darunter auch Spyware und Adware, erkennen. Per E-Mail übertragene Spyware kann zusätzlich über die optional erhältliche Anti-Virus-Engine von Kaspersky identifiziert werden. Die Kaspersky-Lösung stellt hierfür eine spezielle, umfangreiche Datenbank bereit, mit der sich auch Trojaner und Adware aufspüren lassen.

Anhangskontrolle

Leistungsfähige Regeln zur Anhangskontrolle ermöglichen es Administratoren, Anhänge nach Benutzer und Dateityp unter Quarantäne zu stellen. Auch Anlagen mit ausführbaren Dateien können somit überprüft werden, bevor sie an Empfänger weitergeleitet werden. GFI MailSecurity scannt zusätzlich nach Sicherheitsverletzungen durch interne Quellen, z. B. Benutzer, die vertrauliche Datenbank-Dateien per E-Mail verschicken. Des Weiteren können Sie Anhänge wie MP3- oder mpg-Dateien löschen lassen.

■ Optimale Datenaufbereitung durch leistungsfähiges Reporting-Modul

Das GFI MailSecurity ReportPack ist als vollständig integrierbares, umfassendes Reporting-Modul für GFI MailSecurity erhältlich. Ob Trend-Reports für die Geschäftsführung (ROI) oder tägliche Detailberichte zu Sicherheitsproblemen für die IT-Abteilung, das GFI MailSecurity ReportPack liefert übersichtliche Grafiken und Tabellen zum genauen Verständnis von E-Mail-relevanten Security-Pattern. Das Reporting läuft automatisch nach einem definierbaren Zeitplan ab. Einmal eingerichtet, ist keine weitere Konfiguration erforderlich. Das Zusatzmodul bietet eine umfangreiche Auswahl an vordefinierten und individuell anpassbaren Reports, die stündlich, täglich, wöchentlich oder monatlich erstellt werden können, unter anderem zu den Bereichen:

- Anzahl abgewehrter Viren
- Anzahl eingehender E-Mails
- Anzahl ausgehender E-Mails
- Gesamte E-Mail-Kommunikation (ein- und ausgehend)
- Anzahl verarbeiteter E-Mails
- Anzahl blockierter E-Mails
- u. v. m.

■ Granulare, anwenderbasierte E-Mail-Inhaltsrichtlinien/Filterung

Mit der leistungsfähigen Engine zum Erstellen von Inhaltsrichtlinien können Sie neben anwenderspezifischen Regeln auch Stichwörter festlegen, nach denen potenziell gefährliche Inhalte herausgefiltert und bis zur Freigabe durch den Administrator unter Quarantäne gestellt werden. Hierdurch lassen sich auch anstößige oder beleidigende Inhalte schnell identifizieren.

■ Individuell anpassbare Quarantäne-Filter

Innerhalb des Quarantänebereichs können mehrere Suchordner (ähnlich wie bei Microsoft Outlook) angelegt werden, mit deren Hilfe sich herausgefilterte E-Mails einfacher und schneller verwalten lassen. Erstellen Sie beispielsweise für einen bestimmten Anwender einen Quarantäne-Ordner für Mitteilungen, die per Virenkontrolle abgefangen wurden, sowie einen weiteren für E-Mails, die die Anhangskontrolle als verdächtig eingestuft hat. So können Sie schneller entscheiden, welcher Ordner zuerst kontrolliert werden soll. Die Überprüfung des Ordners für die Anhangskontrolle ist unter Umständen wichtiger, da er E-Mails enthalten kann, die der Empfänger besonders dringend benötigt.

■ Einfache Überwachung des Quarantänebereichs per RSS-Feeds

GFI MailSecurity nutzt die Vorteile von RSS-Feeds (Really Simple Syndication), um Administratoren bei neu unter Quarantäne gestellten E-Mails sofort automatisch zu informieren. Systemverantwortliche bleiben somit über den aktuellen Status des Quarantänebereichs auf dem Laufenden, ohne sich dort manuell anmelden zu müssen.

■ Web-basierte Konfiguration für Remote-Management

Die Konfiguration und Überwachung von GFI MailSecurity sowie die Verwaltung von Quarantäne-Mitteilungen können dank der Web-basierten Konfigurationskonsole auch per Fernzugriff erfolgen – über jeden Rechner, der mit einem Internet-Browser ausgestattet ist. Sämtliche Administration kann somit standortunabhängig erfolgen.

Systemanforderungen

- Windows 2000 Server/Advanced Server (mit Service Pack 1 oder höher) oder Windows 2003 Server/Advanced Server oder Windows XP
- Microsoft Exchange Server 2000 (SP1), 2003, 2007, 4, 5, 5.5 oder Lotus Domino oder andere gängige SMTP-/POP3-Mail-Server
- Bei Einsatz von Small Business Server: Service Pack 2 für Exchange Server 2000 und Service Pack 1 für Exchange Server 2003
- Microsoft .NET Framework 1.1/2.0
- MSMQ – Microsoft Messaging Queuing Service
- Internet Information Services (IIS) – SMTP-Service und World Wide Web-Service
- Microsoft Data Access Components (MDAC) 2.8

Auszeichnungen



Ihre Testversion steht unter <http://www.gfi.com/de/mailsecurity/> zum Download bereit!

GFI Software
Magna House, 18 – 32 London Road
Staines, Middlesex
TW18 4BP
UK
Tel +44 (0) 870 770 5370
Fax +44 (0) 870 770 5377
sales@gfi.co.uk

GFI Software
15300 Weston Parkway
Suite 104
Cary, NC 27513
USA
Tel +1 (888) 243-4329
Fax +1 (919) 379-3402
sales@gfiusa.com

GFI Asia Pacific Pty Ltd
83 King William Road
Unley 5061
South Australia
Tel +61 8 8273 3000
Fax +61 8 8273 3099
sales@gfiap.com

GFI Software
GFI House
San Andrea Street
San Gwann SGN 1612
Malta
Tel +356 21 382418
Fax +356 21 382419
sales@gfi.com

Microsoft
GOLD CERTIFIED
Partner

GFI
www.gfi.com