WHITE PAPER

Einsatzmöglichkeiten von GFI MailSecurity

Informationen zur Auswahl des optimalen Betriebsmodus' für Ihr Netzwerk

GFI MailSecurity lässt sich als SMTP-Gateway oder VS API-Version für Exchange 2000/2003 einsetzen. In diesem White Paper erhalten Sie Informationen zu beiden Betriebsarten, um leichter entscheiden zu können, welcher Modus für Ihr Netzwerk am besten geeignet ist oder ob beide Modi gleichzeitig zum Einsatz kommen sollten.

Einführung

GFI MailSecurity bietet zwei verschiedene Betriebsmodi: Den SMTP-Gateway-Modus und die VS API-Version für Exchange 2000/2003. Das Produkt kann entweder in jeweils einem dieser Modi oder in beiden gleichzeitig eingesetzt werden. Dieses White Paper erläutert die Einsatzmöglichkeiten von GFI MailSecurity im Detail, damit Sie entscheiden können, welcher Modus für Ihr Netzwerk am besten geeignet ist.

Warum der Einsatz beider Modi: VS API und SMTP-Gateway?

GFI MailSecurity ist die einzige Lösung für E-Mail-Inhaltssicherheit, die sowohl einen SMTP-Gateway- als auch VS API-Modus unterstützt. Für optimale Sicherheit wird empfohlen, beide Modi gleichzeitig einzusetzen. Grund hierfür ist, dass beide Betriebsarten ihre besonderen Vorteile haben und in Zusammenarbeit einen umfassenderen Schutz für Netzwerke und E-Mail-Server bieten.

Im SMTP-Gateway-Modus kontrolliert GFI MailSecurity alle ein- und ausgehenden E-Mails, bevor sie auf Ihren Mail-Server gelangen. Hierfür muss die Sicherheitslösung vor Ihrem E-Mail-Server (oder auf dem Exchange Server, falls Sie Exchange 2000/2003 einsetzen) installiert werden. Im VS API-Modus wird GFI MailSecurity auf Ihrem Exchange 2000/2003-Server installiert und überprüft eingehende, ausgehende UND innerhalb des Netzwerks verschickte E-Mails mit Unterstützung des Microsoft VS API-Interface.

Sie sollten GFI MailSecurity möglichst in beiden Modi einsetzen. Aus Administrations- und Performance-Gründen ist zu empfehlen, komplexere und zeitaufwändigere Checks auf Gateway-Ebene durchzuführen. Würden diese Kontrollen auch für die interne E-Mail-Kommunikation erfolgen, wären sehr viele Mitteilungen zu verwalten und überprüfen. Der VS API-Modus hingegen sollte auf dem Exchange Server eingesetzt werden, um zu verhindern, dass sich eingeschleppte Viren (z. B. per Diskette, CD, Web oder Notebook) im Netzwerk verbreiten. Zudem können auf diese Weise interne Anwender überwacht oder davon abgehalten werden, mit Hilfe von E-Mail-Exploits an Daten zu gelangen. Dieser Modus hilft Ihnen zudem, den Versand von Anhängen mit ausführbaren Dateien durch unautorisierte

Anwender zu verhindern, deren Ziel es ist, an Informationen von Kollegen zu gelangen, die umfangreichere Zugriffsrechte im Netzwerk besitzen.

Informationen zum SMTP-Gateway-Modus von GFI MailSecurity

Wenn Sie GFI MailSecurity am Netzwerk-Perimeter installieren möchten oder Microsoft Exchange 2000/2003 nicht einsetzen, müssen Sie GFI MailSecurity im SMTP-Gateway-Modus installieren.

Im SMTP-Gateway-Modus kontrolliert GFI MailSecurity alle ein- und ausgehenden E-Mails, bevor sie auf Ihren Mail-Server gelangen. Dafür müssen alle für Ihren Mail-Server bestimmten E-Mails als erstes von GFI MailSecurity empfangen werden. Umgekehrt muss die Software die letzte Anwendung sein, die ausgehende E-Mails vor dem Versand über das Internet passieren. Damit dieser Kontrollmechanismus funktioniert, muss GFI MailSecurity als Gateway für die gesamte E-Mail-Kommunikation dienen. Diese Installation wird als "Smart Host“ oder Mail-Relay-Server bezeichnet. GFI MailSecurity wird somit effektiv als Mail-Relay-Server eingesetzt.

GFI MailSecurity VS API Exchange 2000/2003-Modus

Wenn Sie Microsoft Exchange 2000/2003 einsetzen, kann GFI MailSecurity mit Exchange 2000/2003 über die neue Schnittstelle Microsoft Virus Scanning API (VS API) integriert werden.

Worum handelt es sich bei VS API, und warum sollte diese Technologie verwendet werden?

Exchange 2000/2003 bietet ein neues Virus-Scanning API, das auf sehr niedriger Ebene im Exchange Store implementiert wird. Dies hat den Vorteil, dass die Leistungsfähigkeit der Viren-Scanner voll ausgeschöpft wird. Zudem ist gewährleistet, dass jede Mitteilung gescannt wird, bevor eine Anwendung auf die Nachricht oder ihren Anhang zugreifen kann. Dieser Low-Level-Zugriff erleichtert die Abwehr von Schädlingen wie dem Melissa-Virus.

Zusätzlich wird durch VS API das Problem der Skalierbarkeit bei Servern mit einer großen Anzahl von Benutzern/Mailboxen verringert. Des Weiteren ermöglicht die Echtzeit-Kontrolle der VS API, dass Nachrichten und Anhänge vor der Weiterleitung nur einmal und nicht etwa mehrmals (der Anzahl der Empfänger entsprechend) gescannt werden müssen. Dieses einmalige Scannen verhindert auch, dass kopierte Nachrichten erneut gescannt werden. Weitere Informationen zur VS API von Microsoft stehen unter http://support.microsoft.com/default.aspx?scid=kb;EN-US;q285667 bereit.

Einschränkungen bei der Verwendung des VS API Exchange 2000/2003-Modus

Obwohl zum Kontrollieren von Inhalten und zum Schutz vor Viren unter Exchange 2000/2003

der Einsatz der VS API empfohlen wird, gibt es einige Einschränkungen, derer sich System-Administratoren bewusst sein sollten:

1. Die Viren-Scan-API scannt nur die Informationsspeicher. Dies bedeutet, dass z. B. bei der Installation von GFI MailSecurity unter Exchange 2000/2003 auf einem Front-End-Server keine E-Mails gescannt werden können, da auf diesem Server keine elektronische Post gespeichert wird. In diesem Fall ist GFI MailSecurity im SMTP-Gateway-Modus einzusetzen.

2. Anhangskontrollregeln sind sehr umsichtig anzuwenden, da ansonsten die interne E-Mail-Kommunikation behindert werden könnte. Zu restriktive Regeln bewirken, dass zu viele E-Mails unter Quarantäne gestellt werden. Zudem könnten einige MAPI-Anwendungen, die unter Exchange laufen, vbs- oder exe-Dateien verwenden.

3. Ausgehende E-Mails, die freigegeben worden sind, müssen vom Anwender erneut versendet werden. Wenn beispielsweise eine exe-Datei zunächst unter Quarantäne gestellt und dann freigegeben worden ist, erhält der Absender eine Nachricht, dass diese Datei innerhalb von 24 Stunden erneut verschickt werden kann. Dies liegt daran, dass im VS API-Modus der Empfänger nicht immer mit 100%iger Sicherheit bekannt ist.

4. Im VS API-Modus werden die einzelnen Bestandteile einer E-Mail kontrolliert. Das VS API-Interface von Exchange leitet diese verschiedenen Komponenten der E-Mail einzeln an GFI MailSecurity weiter, d. h., den Textkörper, Anhang 1, Anhang 2 usw. Somit werden immer einzelne Bestandteile der Mitteilung unter Quarantäne gestellt, nicht die gesamte Nachricht. Sämtliche Bestandteile werden von allen Checks auf Viren untersucht. Beispielsweise wird eine E-Mail, die gefährliche Inhalte aufweist, nicht vollständig gelöscht, sondern nur der Teil der Mitteilung, der infiziert ist.

5. Im VS API-Modus ist bei der E-Mail-Übermittlung mit Geschwindigkeitseinbußen beim Zugriff auf Mitteilungen zu rechnen. Dies ist unvermeidlich, da sämtliche Nachrichten zu kontrollieren sind, bevor sie von Anwendern geöffnet werden können. Die Verzögerung beträgt normalerweise maximal eine Sekunde. Bei einer Mitteilung, die 15 MB groß ist, kann es aber länger dauern, bis der Scan abgeschlossen ist. Diese Leistungseinbußen gelten für alle VS API-basierten Anti-Viren-Lösungen. Je weniger Sicherheitschecks durchgeführt werden, desto geringer sind jedoch die Beeinträchtigungen.

Vergleich zwischen SMTP-Gateway- und VS API-Modus

	SMTP-Gateway	VS API
Überprüfung interner E-Mails	Nein	Ja
Überprüfung eingehender/ausgehender E-Mails	Ja	Ja
Erfordert Windows 2000/XP/2003*	Ja (*)	Ja
Erfordert Active Directory	Nein	Ja
Erfordert Exchange 2000/2003	Nein	Ja
Scans der einzelnen E-Mail-Komponenten	Nein	Ja
Kann auf einem Rechner mit GFI MailEssentials betrieben werden	Ja	Ja
Läuft unter Exchange 5.5	Ja	Nein
Unterstützt Notes oder SMTP-Server	Ja	Nein
Betrieb in DMZ oder als Mail-Relay möglich	Ja	Nein
Erfordert Ticketing-System**	Nein	Ja
Absolut zuverlässige Identifizierung, ob E-Mail eingehend/intern***	Ja	Nein

* nur auf Gateway

**Bei der SMTP-Gateway-Version sind mehr Informationen über die E-Mail verfügbar. Daher können ausgehende E-Mails ohne die Verwendung eines Ticketing-Systems unter Quarantäne gestellt werden.

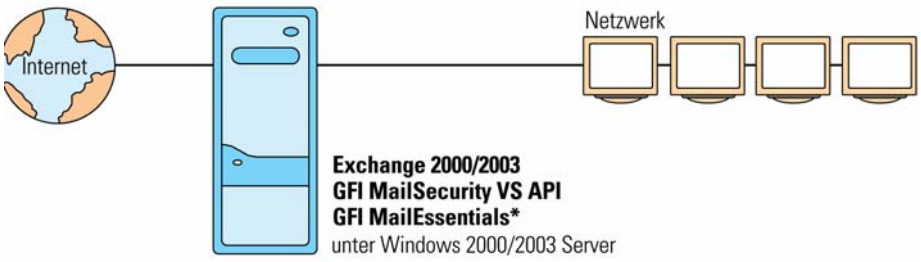
*** Bei der SMTP-Gateway-Version lässt sich durch die umfangreicheren Informationen zu einer E-Mail leichter erkennen, ob es sich um eine ein- oder ausgehende E-Mail handelt.

Installation von GFI MailSecurity

Installationsoption 1

Bei kleineren Netzwerken mit Exchange 2000/2003, bei denen zudem kein gesonderter Mail-Relay in der DMZ zum Einsatz kommen soll, empfiehlt sich die alleinige Verwendung des VS API-Modus.

Kleine Netzwerke (z. B. Small Business Server)

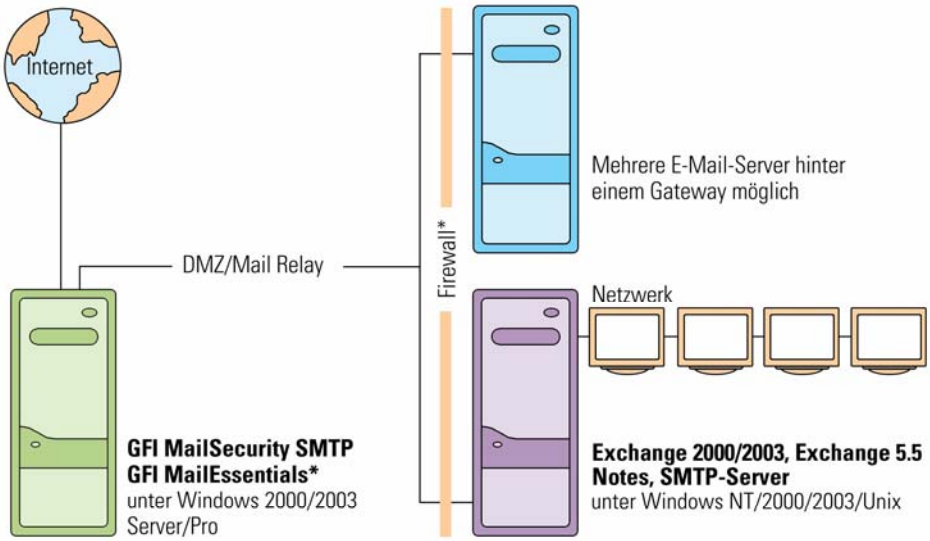


Regeln
Quarantäne für eingehende und ausgehende verdächtige Anhänge
Virenkontrolle für eingehende, ausgehende und interne Mitteilungen
Aktivierung der Exploit-Engine und HTML-Threats-Engine sowie des Trojan & Executable Scanner *optional

Installationsoption 2

Wenn Sie Exchange 2000/2003 nicht einsetzen, ist GFI MailSecurity im SMTP-Gateway-Modus zu installieren. Dies gilt beispielsweise unter Exchange 5.5, Lotus Note oder einem anderen SMTP-/POP3-Server.

NT-Netzwerke und Windows 2000/2003-Netzwerke ohne Einsatz von GFI MailSecurity zum Schutz des internen Netzwerks



Regeln
Quarantäne für eingehende und ausgehende verdächtige Anhänge
Virenkontrolle für eingehende, ausgehende und interne Mitteilungen
Aktivierung der Exploit-Engine und HTML-Threats-Engine sowie des Trojan & Executable Scanner *optional

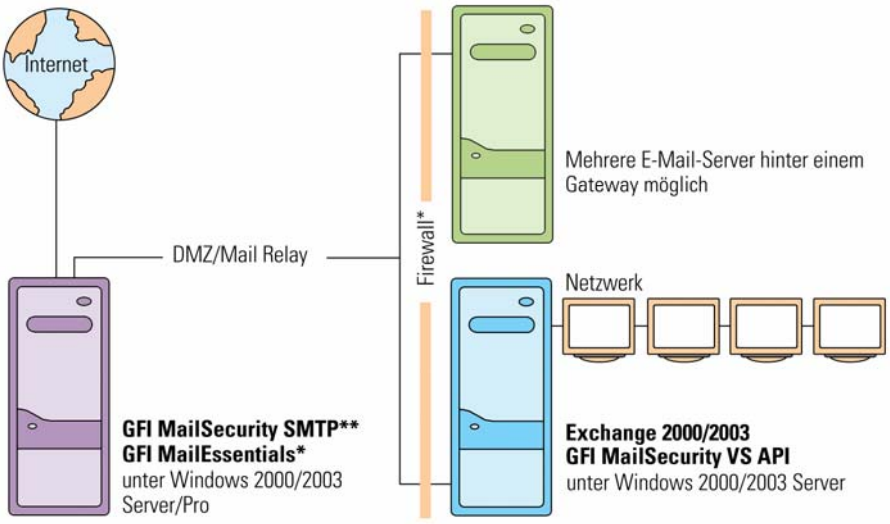
Installationsoption 3

Bei größeren Netzwerken mit einem oder mehreren Exchange 2000/2003-Servern ist zu empfehlen, dass GFI MailSecurity auf dem Exchange 2000/2003-Rechner im VS API-Modus und am Netzwerk-Perimeter im SMTP-Gateway-Modus betrieben wird. Bei dieser idealen Installa-tionsart profitieren Sie vor allem davon, dass Sie für ein- und ausgehende Mails strenge Regeln definieren, bei internen E-Mails jedoch weniger restriktive Richtlinien festlegen können.

Größere Netzwerke mit Windows 2000/2003

Die Optimal-Lösung: Einsatz beider Modi

1. Einsatz des Gateway für die DMZ zur Gefahrenabwehr am Gateway und zur Kontrolle der ausgehenden Daten
2. Einsatz von VS API zur Kontrolle interner Virenausbrüche



Regeln
Quarantäne für eingehende und ausgehende verdächtige Anhänge
Virenkontrolle für eingehende, ausgehende und interne Mitteilungen
Aktivierung der Exploit-Engine und HTML-Threats-Engine
sowie des Trojan & Executable Scanner

Regeln
Interne Virenkontrolle

*optional
**Wartungsmehrkosten in Höhe von 30% aufgrund der Lizenz für zusätzliche Anti-Viren-Engine

Gemeinsamer Einsatz von GFI MailEssentials und GFI MailSecurity auf einem Rechner

GFI MailEssentials und GFI MailSecurity sind Schwesterprodukte und eignen sich daher perfekt für den gemeinsamen Einsatz auf demselben Rechner. GFI MailEssentials erweitert die Funktionalität von Exchange Server mit wichtigen E-Mail-Tools wie POP3-Downloader, Server-basierte Auto-Replies, E-Mail-Archivierung, Internet-Mail-Berichterstellung und Disclaimer.

Beide Produkte können auch als kostengünstiges Bundle erworben werden.

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.