WHITE PAPER

Trojaner – E-Mail-basierte Gefahren für Unternehmen

Wie Sie Ihr Netzwerk vor Spionen schützen können

Dieses White Paper informiert über die Funktionsweise von Trojanern und welche Bedrohung sie für Unternehmensnetzwerke darstellen. Es wird erläutert, warum Netzwerke vor Trojanern geschützt werden müssen und welche Abwehrmethoden verfügbar sind.

Einführung

Dieses White Paper informiert über die Funktionsweise von Trojanern und welche Gefahr sie für Unternehmensnetzwerke darstellen. Bereits im Jahr 2001 wurde in einem Artikel des Magazins *eWeek* vom Trojaner-Befall zehntausender Computer berichtet. Und die Zahlen steigen, wie von InternetWeek.com im Januar 2004 bestätigt wurde. Mit Hilfe von Trojanern können mittlerweile Kreditkarten-Informationen, Passwörter und andere vertrauliche Informationen ausspioniert oder gezielte elektronische Angriffe gegen Unternehmen gestartet werden. In diesem White Paper wird erläutert, warum neben einem Viren-Scanner auch ein auf Mail-Server-Ebene eingesetzter Trojaner- und Executable-Scanner dringend erforderlich ist, um Netzwerke noch umfassender schützen zu können.

Was ist ein Trojanisches Pferd?

Ein Trojanisches Pferd im IT-Bereich bezeichnet ein Programm, das unbemerkt auf einem Rechner installiert wird und seinem Programmierer uneingeschränkten Zugriff auf die auf darauf gespeicherten Daten verschafft und somit großen Schaden verursachen kann. Ein Trojaner kann als einzelnes Programm versteckt auf einem Rechner gestartet werden, ohne dass ein Anwender es bemerkt. Ebenso ist es möglich, Trojaner als geheime Funktion in legitime Programme zu "integrieren". (Ein Überblick über die Funktionsweise von Trojanern steht unter http://kbase.gfi.com/showarticle.asp?id=KBID001671 zur Verfügung.)

Begehrte Ziele von Angreifern

Trojaner können eingesetzt werden, um an vertrauliche Informationen zu gelangen oder Schäden zu verursachen. Bei Netzwerken dienen Trojaner vornehmlich der Ausspionierung und dem Diebstahl privater und vertraulicher Informationen (Industriespionage). Unter anderem sind Angreifer an folgenden Informationen interessiert:

- Kreditkarten-Daten (werden oft für Domänenregistrierungen oder Internet-Einkäufe verwendet)
- Kontoinformationen aller Art (E-Mail-Passwörter, DFÜ-Anmeldedaten, Passwörter für Web-Dienste usw.)
- Vertrauliche Dokumente

- E-Mail-Adressen (z. B. von Kunden)
- Vertrauliche Entwürfe oder Bildmaterial
- Kalenderinformationen mit Angaben zum Aufenthaltsort/zu Terminen des Anwenders
- Missbrauch von Rechnern für illegale Zwecke, z. B. Hacken, Scannen, DoS-Angriffe oder Infiltrieren anderer Computer im Netzwerk oder Internet.

Verschiedene Arten von Trojanern

Es gibt viele verschiedene Arten von Trojanern, die in sieben Hauptkategorien unterteilt werden können. Im Allgemeinen ist es jedoch schwierig, einen Trojaner einer bestimmten Gruppe zuzuweisen, da diese Schädlinge oftmals Merkmale besitzen, anhand derer sie sich gleich mehreren verschiedenen Kategorien zuordnen lassen. Folgende Kategorien informieren über die wichtigsten Ziele, die mit Trojanern verfolgt werden:

Remote-Access-Trojaner für Fernzugriff auf Rechner

Diese Art Trojaner werden in den Medien wohl am häufigsten erwähnt, da sie Angreifern die uneingeschränkte Kontrolle über einen infizierten Rechner ermöglichen. Einige Beispiele sind die Trojaner Back Orifice und NetBus. Mit diesen Schädlingen wird beabsichtigt, zunächst die vollständige Kontrolle über einen infizierten Rechner zu erhalten, um dann ungehindert Zugriff auf darauf gespeicherte Dateien, private Korrespondenz, Kontodaten usw. nehmen zu können.

Der Bugbear-Virus, der das Internet im September 2003 überflutete, hat beispielsweise einen Trojaner auf Rechnern installiert, über den Angreifer per Fernzugriff Zugang zu vertraulichen Daten erlangen konnten.

Bislang haben Trojaner die Rolle eines Servers übernommen und Ports abgehört, der für Internet-Angreifer verfügbar sein musste. Mittlerweile können Angreifer jedoch auch mit Hilfe einer Reverse-Verbindung mit dem mit einer Hintertür versehenen Host kommunizieren, sodass sie den Server selbst dann erreichen können, wenn er durch eine Firewall geschützt ist. Einige Trojaner können auch automatisch eine IRC-Verbindung herstellen und beinahe unerkannt über IRC-Befehle gesteuert werden – eine echte TCP/IP-Verbindung zwischen Angreifer und Opfer wird somit erst gar nicht aufgebaut.

Mail- und Keylogger- Trojaner (für Passwörter, Tastatureingaben usw.)

Ziel dieser Trojaner ist es, vertrauliche Anmeldeinformationen an den Hacker zurück zu schicken, z. B. Passwörter (ICQ, IRC, FTP, HTTP) oder andere sensible Daten wie Kreditkarteninformationen, Chat-Protokolle, Adressenlisten usw. Hierfür sucht der Trojaner in bestimmten Verzeichnissen nach einzelnen Daten oder installiert einen Keylogger, mit dem alle Tasteneingaben protokolliert und an den Hacker geleitet werden, der dann die Passwörter aus den Daten herausfiltert.

Der E-Mail-Virus Badtrans.B, erstmals gesichtet im Dezember 2001, ist z. B. ein Trojaner, der

alle Tastatureingaben des befallenen Rechners aufgezeichnet hat.

Erfasste Daten können an eine E-Mail-Adresse des Angreifers geschickt werden, die meistens anonym bei einem Web-basierten Free-Mail-Anbieter eingerichtet wurde. Eine weitere Übertragungsmethode besteht auch darin, die Daten per Web-Formular über eine mit der Web-Site des Hackers aufgebaute Verbindung zu übermitteln, die womöglich ebenfalls von einem kostenfreien Webseiten-Provider gehostet wird. Beide Methoden werden vom betroffenen Anwender nicht bemerkt und können für jeden Netzwerk-Rechner angewandt werden, der an das Internet angebunden ist und über einen E-Mail-Zugang verfügt.

Sowohl interne als auch externe Trojaner können Mail-Trojaner einsetzen, um an vertrauliche Informationen über ein Unternehmen zu gelangen.

Trojaner mit zerstörerischer Wirkung

Die einzige Funktion dieses Trojaner-Typs ist die Zerstörung und das Löschen von Dateien. Dadurch ist er auch sehr einfach einzusetzen. Ein solcher Trojaner kann sämtliche wichtigen Systemdateien auf einem Rechner automatisch löschen (z. B. Dateien der Formate .dll, .ini oder .exe sowie u. U. auch andere). Eine Aktivierung des Trojaners erfolgt entweder über den Angreifer oder zeitgesteuert an einem bestimmten Tag zu einer festgelegten Uhrzeit.

Zerstörerische Trojaner sind eine Gefahr für jedes Computer-Netzwerk und ähneln in vielerlei Hinsicht einem Virus. Sie werden jedoch entwickelt, um gezielt einen Schaden auf dem Anwenderrechner anzurichten und sind oftmals nicht von Anti-Viren-Software aufzuspüren.

Denial-of-Service-Trojaner (DoS)

Diese Trojaner erlauben es einem Angreifer, einen Distributed Denial of Service-Angriff (DDoS) zu starten, wenn er die Kontrolle eine ausreichende Anzahl von Rechnern erlangt hat. Das Prinzip dieses Angriffs besteht darin, dass dieser z. B. von 200 infizierten Rechnern, die über eine schnelle Breitband-Anbindung verfügen, gleichzeitig ausgeht – mit dem Effekt, dass die Bandbreite der Internet-Verbindung des Opfers in den meisten Fällen übermäßig strapaziert, der attackierte Server durch eine große Anzahl sinnloser Anfragen in die Knie gezwungen und ein Internet-Zugriff unmöglich wird.

WinTrinoo ist beispielsweise ein DDoS-Tool, das sich gerade in letzter Zeit einer großen Beliebtheit erfreut. Mit seiner Hilfe kann ein Angreifer, der die Rechner vieler Breitband-Anwender unter seiner Kontrolle hat, Internet-Sites zusammenbrechen lassen. Erste Auswirkungen dieser Vorgehensweise waren bereits im Februar 2000 sichtbar, als eine Reihe bekannter E-Commerce-Seiten wie Amazon, CNN, E*Trade, Yahoo und eBay attackiert wurde.

Eine weitere Variante eines DoS-Trojaners ist der Mail-Bomben-Trojaner, der versucht, so viele Rechner wie möglich zu infizieren. Dabei werden gleichzeitig bestimmte E-Mail-Adressen mit beliebigen Betreffangaben und Inhalten überschwemmt, die nicht abgewehrt werden können.

Auch hier gilt, dass ein DoS-Trojaner einem Virus ähnelt, der DoS-Trojaner aber ebenso erstellt werden kann, um Anwender gezielt anzugreifen, ohne dass sich dieser Angriff mit Hilfe einer Anti-Viren-Lösung entdecken und abwehren lässt.

Proxy-Trojaner

Diese Trojaner verwandeln einen infizierten Rechner in einen Proxy-Server, der dann von Anwendern aus der ganzen Welt oder nur vom Angreifer allein für verschiedenste Machenschaften missbraucht werden kann. Hierzu zählen unter anderem anonyme Telnet-, ICQ- und IRC-Sitzungen, um Käufe mit gestohlenen Kreditkarten zu tätigen oder andere illegale Aktivitäten zu starten. Der Rechner eines Anwenders kann somit als Quelle für alle Arten von Aktionen eingesetzt werden, ohne dass der wahre Urheber dabei Gefahr läuft, entdeckt zu werden – auch nicht bei Angriffen auf andere Rechner oder Netzwerke, die über den Proxy-Trojaner gestartet werden:

Wird der Missbrauch entdeckt und nach dem Verursacher gesucht, führt die Spur nur zum für die Angriffe missbrauchten Rechner zurück, nicht jedoch zum eigentlichen Verursacher, dem Hacker. Die rechtlichen Folgen hat dann der Anwender dieses Rechners zu tragen. Jede Organisation ist für ihr Netzwerk selbst verantwortlich und somit auch für sämtliche Angriffe, die von ihm ausgehen.

FTP-Trojaner

Diese Trojaner öffnen einen FTP-Server auf dem Rechner des Opfers, auf dem Software-Raubkopien und/oder vertrauliche Dateien zur Weiterverbreitung gespeichert werden könnten. Angreifern wird eine FTP-Verbindung mit dem befallenen Rechner ermöglicht.

Trojaner zur Deaktivierung von Sicherheits-Software

Bei diesen Trojanern handelt es sich um spezielle Varianten, die extra darauf abzielen, Sicherheitsprogramme wie Anti-Viren-Software, Firewalls usw. zu deaktivieren oder sogar zu zerstören. Sind diese Programme außer Gefecht gesetzt, können Hacker den Rechner umso leichter angreifen.

Der Bugbear-Virus hat z. B. einen Trojaner auf infizierten Rechnern installiert und dafür gesorgt, dass Anti-Viren-Software und Firewalls deaktiviert wurden. Der zerstörerische Wurm Goner vom Dezember 2001 ist ein weiteres Beispiel für einen Schädling, der einen Trojaner enthielt, mit dem Dateien von Anti-Viren-Programmen gelöscht werden sollten.

Trojaner zur Deaktivierung von Sicherheits-Software zielen vornehmlich darauf ab, bestimmte Endanwender-Software wie Desktop-Firewalls zu manipulieren und richten sich daher weniger gegen Unternehmensnetzwerke.

Welche Infizierungswege gibt es?

Bei Netzwerk-Anwendern, die durch eine Firewall geschützt und deren ICQ- und IRC-Verbindungen deaktiviert sind, werden Trojaner vor allem per E-Mail-Anhang oder Software-Download von einer Web-Site eingeschleppt.

Viele Anwender behaupten, dass sie niemals unbekannte Anhänge öffnen oder Software von einer ihnen nicht geläufigen Web-Site herunterladen würden. Aber auch diese User sind nicht vor schlauen Social-Engineering-Techniken gefeit, mit deren Hilfe Hacker die meisten Anwender dazu bringen, arglos einen infizierten Anhang zu öffnen oder böswillige Software herunterzuladen.

Ein Beispiel für einen Trojaner, der sich das Social Engineering zu Nutze gemacht hat, ist Septer.troj, der im Oktober 2001 per E-Mail übertragen wurde. Er erschlich sich wichtige Daten, indem er als Spendenaufruf für das amerikanische Rote Kreuz getarnt Empfänger darum bat, ein Formular auszufüllen, in dem auch Kreditkarten-Daten angegeben werden sollten. Diese Angaben wurden vom Trojaner verschlüsselt und an die Web-Site des Angreifers geschickt.

Infizierung per E-Mail-Anhang

Es ist erstaunlich, wie viele Anwender ihren Rechner mit einem Virus infizieren, weil sie einen Anhang öffnen, der an ihre E-Mail-Adresse geschickt wurde. Folgendes Szenario spielt sich dabei sehr häufig ab: Eine Person, die einen Angriff auf einen Anwender plant, weiß, dass dieser einen Bekannten hat und, mit dem er per E-Mail korrespondiert. Zudem besitzt er die E-Mail-Adresse des Bekannten. Nun versteckt der Angreifer einfach einen Trojaner in einer Datei mit interessantem Inhalt, z. B. in einer Flash-Animation, und schickt sie im Namen des Bekannten an das Opfer. Diese Manipulation ist sehr einfach zu bewerkstelligen: Der Angreifer nutzt einen ungeschützten Mail-Relay-Server, um das VON-Feld der E-Mail zu fälschen und es so aussehen zu lassen, als wäre der Bekannte der Absender. Die E-Mail-Adresse des Bekannten lautet z. B. alex@beispiel.com, und das Absenderfeld des Angreifers wird nun einfach in eben diese Adresse umgeändert. Das Opfer erhält dann eine Mitteilung von dieser Adresse, denkt, dass sie von seinem Bekannten stammt und öffnet den Dateianhang, ohne darüber nachzudenken, dass es sich dabei um eine böswilligen Angriff handeln könnte – ein Freund würde doch wohl kaum gefährliche Dateien verschicken…

Wissen ist Macht: In diesem Beispiel besitzt der Angreifer lediglich die Informationen zum Bekannten des Opfers und kann mit großer Sicherheit davon ausgehen, dass ein von dieser Person verschickter Anhang geöffnet wird – und der Schädling wird ohne große Mühe eingeschleust.

Neben diesem Szenario sind noch viele andere denkbar. Der entscheidende Punkt dabei ist, dass nur EIN Netzwerk-Benutzer eine solche Nachricht empfangen und öffnen braucht, und das gesamte Netzwerk wird infiziert.

Ein weiteres Risiko besteht darin, dass sich Anhänge sogar automatisch öffnen könnten, wenn keine Sicherheits-Software eingesetzt wird, die die dafür entwickelten Exploits erkennt. Ein Hacker kann ein System bereits infizieren, indem er einen Trojaner als Anhang verschickt, und dieser wird dann ohne Zutun des Opfers geöffnet.

Infizierung durch Datei-Downloads von einer Web-Site

Trojaner werden auch über Web-Sites verbreitet. So kann ein Anwender per E-Mail einen Link zu einer angeblich interessanten Site zugeschickt bekommen. Der Anwender besucht daraufhin die Site, lädt einige Dateien herunter, die ihm wichtig oder hilfreich erscheinen, und damit installiert er jedoch ohne sein Wissen einen Trojaner, der seinem Programmierer Tür und Tor öffnet. Bestes Beispiel aus der jüngeren Vergangenheit ist der Trojaner ZeroPopUp, der in einer Spam-Mitteilung als Pop-Up-Blocker angepriesen wurde. Anwender wurden dazu verleitet, auf den Download-Link zu klicken, und schon wurde der Trojaner heruntergeladen. Nach seiner Installierung hat der Trojaner eine E-Mail an alle im Adressbuch des Opfers verzeichneten Kontakte verschickt, die über den vermeintlichen Pop-Up-Blocker informiert und die Download-URL des Trojaners enthält. Empfänger sind somit Freunde oder Kollegen, die aufgrund des ihnen bekannten Absenders arglos davon ausgehen, dass die URL und Software für sie harmlos sind.

Als weitere Gefahr stehen über Anbieter von kostenfreiem Web-Space, wie Xoom, Tripod, Geocities und anderen, Tausende von “Hacking/Security“ Archiven bereit. Über diese Archive gelangt man an viele Hacker-Tools, Scanner, Mail-Bomben, Flooder-Tools und andere Spionage-Werkzeuge. Oftmals sind selbst einige dieser Programme vom Autor der Site manipuliert worden.

Im Januar 2003 wurde von TruSecure, dem Unternehmen für Risiko-Management und Eigentümer der ICSA Labs sowie des InfoSecurity Magazine, die Warnung herausgegeben, dass Malware-Autoren Remote-Access-Trojaner als Einwahlprogramme für den Zugang zu weiteren Sites der “Erwachsenen-Unterhaltung“ deklarieren und auf Seiten mit pornografischen Inhalten oder in Newsgroups anbieten.

Der Trojaner Migmaf (“migrant Mafia”) vom Juli 2003 hat ungefähr 2000 Windows-Rechner, die über einen High-Speed-Anbindung an das Internet verfügten, für seine Zwecke eingespannt, um mit ihrer Hilfe Spam-Mitteilungen mit pornografischem Inhalt zu verschicken. Hier kam zudem das bereits weiter oben beschriebene Prinzip des Proxy-Servers zum Einsatz, bei dem Migmaf den Rechner seines Opfers als eine Art Verteilerstelle oder Mittler missbraucht hat. Die Links in den verschickten Spam-Mails verwiesen dabei nicht direkt auf den Web-Server mit den beworbenen Inhalten, sondern auf einen der infizierten PCs, von denen der Trojaner den Zugriff dann weitergeleitet hat.

Wie sich Netzwerke gegen Trojaner absichern lassen

Um sich vor der Gefahr schützen zu können, die von Trojanern ausgeht, sind verschiedene

Maßnahmen zu ergreifen. Eine häufige Fehleinschätzung ist, dass Netzwerke durch den Einsatz von Anti-Viren-Software bereits umfassend abgesichert sind. Diese Annahme ist deswegen trügerisch, weil Anti-Viren-Lösungen nur einen bedingten Schutz bieten. Sie erkennen längst nicht alle bekannten Trojaner und sind geben erst recht keinen Alarm bei unbekannten Trojanern.

Der Grund: Anti-Viren-Software soll Schutz vor Trojanern bieten, indem sie vorrangig nach den “Signaturen” dieser Schädlinge sucht. Da Angreifern der Quell-Code vieler Trojaner jedoch öffentlich zugänglich ist, können erfahrenere Hacker eine neue Version eines Trojaners programmieren, deren Signatur KEINEM Viren-Scanner zur Verfügung steht.

Findet ein Angreifer heraus, welche Anti-Viren-Software sein potenzielles Opfer einsetzt, beispielsweise durch den automatischen Disclaimer, mit dem einige Sicherheits-Engines ausgehende Mitteilungen versehen, kann er einen Trojaner so konzipieren, dass der Viren-Scanner umgangen wird.

Hinzu kommt, dass viele Viren-Scanner nicht sämtliche bereits bekannten Trojaner identifizieren können. Viele Anti-Viren-Hersteller suchen nicht aktiv nach neuen Trojanern, zudem haben Untersuchungen gezeigt, dass die einzelnen Viren-Engines oftmals immer nur eine bestimmte Trojaner-Art erkennen. Um die Erkennungsrate von bekannten Trojanern zu erhöhen, müssen somit mehrere Viren-Scanner eingesetzt werden.

Für einen effektiven Schutz von Netzwerken vor Trojanern ist eine mehrstufige Sicherheitsstrategie zu verfolgen:

1. Bereits am Netzwerk-Perimeter muss ein Gateway-Virenscanner zum Einsatz kommen und eine Inhaltskontrolle stattfinden, um E-Mails sowie HTTP- und FTP-Verbindungen zu überprüfen. E-Mail-Virenschutz allein reicht somit nicht aus, wenn Anwender immer noch die Möglichkeit haben, einen Trojaner von einer Web-Site herunterzuladen, mit dem das Netzwerk infiziert werden kann.
2. Ein umfassender Gateway-Schutz erfordert mehrere Anti-Viren-Engines. Obwohl eine gute Anti-Viren-Lösung so gut wie alle bekannten Viren abfängt, hat die Verwendung mehrerer Engines den Vorteil, dass eine weitaus größere Anzahl von Trojanern entdeckt werden kann als mit einer einzigen Engine.
3. Ausführbare Dateien, die per E-Mail und Web/FTP ins Netzwerk gelangen können, müssen bereits am Gateway unter Quarantäne gestellt bzw. überprüft werden. Es muss analysiert werden, welche Auswirkungen das Starten einer exe-Datei hat.

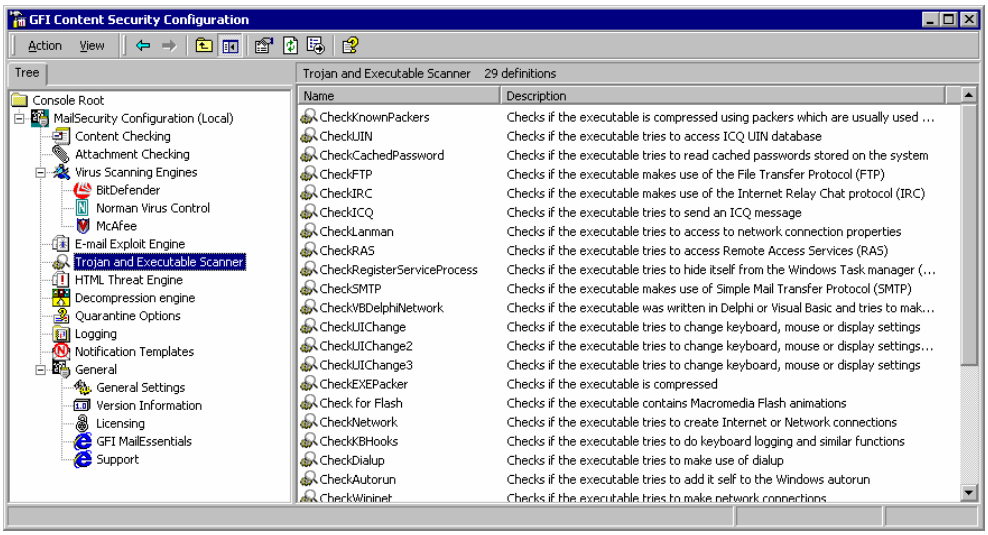
Für diese unfangreichen Sicherheitsüberprüfungen stehen bereits Tools zur Verfügung, die die Kontrollen automatisieren und für Anwender eine große Arbeitserleichterung bedeuten.

Analyse böswilliger exe-Dateien per Scanner für Trojaner und ausführbare Dateien

Unbekannte Trojaner lassen sich nur aufspüren, indem eine verdächtige exe-Datei manuell überprüft oder ein spezielles Analyse-Tool zum Scannen von Trojanern und ausführbaren Dateien eingesetzt wird.

Die manuelle Kontrolle ist jedoch sehr zeitaufwändig und nur bedingt zuverlässig, da dem bei der Überprüfung Fehler unterlaufen können. Der Vorgang sollte daher teilweise automatisiert werden, um Fehler durch z. B. Unachtsamkeit auszuschließen und höhere Erkennungsraten zu erzielen. Diese Automatisierung kann durch den Einsatz eines Scanners für Trojaner und exe-Dateien erfolgen.

Ein Scanner für exe-Dateien führt eine intelligente Analyse der Prozessabläufe von ausführbaren Dateien durch und bestimmt ihren Gefährdungsgrad. Die Datei wird disassembliert, die Überprüfung der Abläufe erfolgt in Echtzeit, und vorgegebene Aktionen werden schließlich mit einer Datenbank bekannter böswilliger Aktionen abgeglichen. Dadurch lassen sich potenziell gefährliche, unbekannte oder zielgerichtet eingesetzte Trojaner erkennen. Mit Hilfe eines Scanners für Trojaner und exe-Dateien lassen sich auch Angriffe von versierten Hackern abwehren, die eigene Trojaner-Versionen erstellen, deren Signaturen nicht von Anti-Viren-Software identifiziert werden können.



Konfigurierung des Trojan & Executable Scanner

Erst die Kombination aus Gateway-Kontrolle, mehreren Anti-Viren-Engines UND einem Scanner für Trojaner und exe-Dateien bietet einen umfangreichen Trojaner-Schutz für Netzwerke.

Gateway-Schutz

Zwei Produkte, die Netzwerke bereits auf Gateway-Ebene unter anderem mit mehreren Anti-Viren-Engines und einem Scanner für Trojaner und exe-Dateien schützen, sind GFI MailSecurity und GFI DownloadSecurity.

GFI MailSecurity for Exchange/SMTP ist eine umfassende E-Mail-Sicherheitslösung und bietet mehrere Anti-Viren-Engines für Inhalts- und Anhangskontrolle mit Quarantäne-Optionen, einen Exploit-Schutz, einen Scanner für Trojaner- und exe-Dateien sowie eine HTML-Threats-Engine zum Deaktivieren von HTML-Skripten in elektronischer Post. Sämtliche schädlichen Elemente, die sich per E-Mail übertragen lassen, werden somit blockiert, bevor sie E-Mail-Anwender erreichen. Weitere Informationen und eine Testversion stehen zum Download bereit unter http://www.gfisoftware.de/de/mailsecurity.

GFI WebMonitor ist ein speziell für Microsoft ISA Server entwickeltes Utility, mit dem Administratoren überwachen können, welche Web-Sites/Dateien von Mitarbeitern besucht/heruntergeladen werden – in Echtzeit! Zudem erlaubt das Tool die Sperrung von Erwachsenen-Sites und führt für alle Downloads eine Virenüberprüfung durch. GFI WebMonitor kontrolliert die Internet-Aktivitäten von Netzwerk-Benutzern unauffällig im Hintergrund, auch um die Einhaltung gesetzlicher Vorschriften zu garantieren – und erlaubt dabei weiterhin eine produktive Nutzung des Internet! Weitere Informationen und eine Testversion stehen bereit unter http://www.gfisoftware.de/de/webmon.

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.