



Kaspersky Mail Gateway

- Bankverbindung: Bank Austria-Creditanstalt, Konto-Nr. 0957-38605/00, BLZ: 12000
- UID-Nr: ATU16091903 • FB-Nr: 79576z • FB-Gericht: Handelsgericht Wien

© MSB Software - All trademarks and registered trademarks are the property of their respective owners.

Kaspersky[®] Mail Gateway

Kaspersky Mail Gateway ist eine universelle Lösung für Mailprogramme zum komplexen Schutz vor Viren und Spam.

Installiert zwischen Firmennetzwerk und Internet, überprüft die Anwendung die elektronische Post auf Viren, durchsucht den elektronischen Postverkehr an zentraler Stelle nach Spam und schützt auch den Mailserver des Unternehmens vor unbefugter Benutzung.

Aufgrund seiner Autonomie ist Kaspersky Mail Gateway in praktisch jeder beliebigen Umgebung einsetzbar und lässt sich leicht mit Antivirenprogrammen anderer Hersteller kombinieren, die an den übrigen Knotenpunkten des Netzwerkes installiert sind. Installation und Konfiguration der Anwendung erfordern keine große Erfahrung mit Linux-Betriebssystemen.

Funktionen

Umfassender Schutz vor Viren und Spam

Virenschutz. Das Programm sucht und entfernt Malware aller Art in allen Elementen des ein- und ausgehenden elektronischen Postverkehrs, Dateianhänge eingeschlossen.

Spamfilter. Die Anwendung prüft den Nachrichtenstrom auf das Vorhandensein von Spam, sowohl auf Grund formaler Merkmale als auch mit Hilfe künstlicher Intelligenz, die den Inhalt der Nachrichten und Anhänge analysiert. Dazu zählen auch spezielle grafische Signaturen zur Identifizierung von Spam in Form von Abbildungen.

Benachrichtigung der Anwender. Bei Auffinden eines verdächtigen oder infizierten Objekts erhalten der Administrator, der Sender und der Empfänger der betreffenden E-Mail eine Benachrichtigung, deren Inhalt, Format und Sprache vom Systemadministrator bestimmt werden. Die als Spam qualifizierte Nachricht kann blockiert, in einen Quarantäneordner verschoben oder dem Empfänger mit einer speziellen Markierung im Mailheader zugestellt werden.

Quarantäne. Infizierte und verdächtige Objekte, aber auch als Spam identifizierte Nachrichten können in ein Quarantäneverzeichnis verschoben werden, wo der Administrator sie einsehen, entfernen oder an den eigentlichen Adressaten weiterleiten kann.

Sicherheitskopien. Kopien infizierter E-Mails können vor ihrer Reparatur gespeichert werden, was die Wiederherstellung wichtiger Informationen im Falle einer inkorrekten Desinfizierung ermöglicht.

Kaspersky[®] Mail Gateway

Zusätzliche Möglichkeiten der Nachrichtenfilterung

Nach Art der Anhänge. Die Filterung des E-Mail-Verkehrs kann nach Namen und Typ der Anhänge organisiert werden. So können Objekte, die mit hoher Wahrscheinlichkeit infiziert sind, sofort isoliert werden.

Nach Benutzergruppen. Der Administrator kann für die verschiedenen Benutzergruppen des Mail-Programms jeweils bestimmte Regeln zur Nachrichten-Bearbeitung erstellen, indem er je nach Sicherheitspolitik des Unternehmens und je nach Aufgabenbereich der Mitarbeiter unterschiedliche Einschränkungen festlegt.

Schutz des Servers vor unbefugter Benutzung

Kaspersky Mail Gateway wehrt sowohl DoS-Attacken als auch den Missbrauch des Servers durch Dritte zum unbefugten Versand von Massenmails ab. Das kann zu einer höheren Bearbeitungsgeschwindigkeit des E-Mail-Traffics beitragen.

Flexible Steuerung und Administration

Remote-Steuerung. Kaspersky Mail Gateway kann entweder wie gewohnt mit Hilfe der Konfigurationsdatei oder über das Web-Interface des Programms Webmin konfiguriert werden.

Optimale Performance. Der Administrator kann die Leistungsfähigkeit der Anwendung verändern – von maximaler Effektivität einerseits bis hin zum maximalen Anwenderschutz andererseits ist alles möglich. Ebenso können folgende Einstellungen vorgenommen werden: Zeitbegrenzungen beim Empfang und/oder Versand von E-Mails, Schrittfolge in der Vorgehensweise des Programms, Anzahl der gleichzeitig im Hintergrundmodus zu überprüfenden Objekte.

Einstellung des Aktualisierungsrhythmus. Die Aktualisierung der Virendatenbank erfolgt auf Anforderung oder automatisch per Zeiteinstellung von den Kaspersky-Lab-Servern bzw. von lokalen Updateservern. Einige Module der Antivirus-Engine und des linguistischen Analysetools können dabei ebenfalls aktualisiert werden.

Grafische Auswertung. Das Programm Webmin bietet die Möglichkeit, die Virenaktivität innerhalb eines bestimmten Zeitraums grafisch darzustellen. Zudem werden Detailinformationen zu den gefundenen Virustypen angezeigt.

Systemanforderungen

Hardwareanforderungen

- Intel Pentium Prozessor (Pentium III oder Pentium IV empfohlen)
- mindestens 256 MB freier Arbeitsspeicher
- mindestens 100 MB freier Festplattenspeicher zur Installation der Anwendung
- mindestens 500 MB freier Speicher im Dateisystem/tmp

Softwareanforderungen

Eines der folgenden Betriebssysteme:

- Red Hat Enterprise Linux Advanced Server 4
- Red Hat Linux 9.0
- Fedora Core 4
- SuSE Linux Enterprise Server 9.0 (SP3)
- SuSE Linux Professional 10.0
- Debian GNU/Linux 3.1r1
- Mandriva 2006
- FreeBSD 4.11/5.4/6.0

Perl ab Version 5.0
(www.perl.org)

Webmin ab Version 1.070
(www.webmin.com), wenn Remote-Steuerung beabsichtigt ist

Produktversion: 5.5

Sprache: Englisch

Kaspersky Labs GmbH
Steinheilstr. 13, 85053 Ingolstadt
www.kaspersky.de
Email: info@kaspersky.de
Tel.: +49 (0) 841 98 189 0
Fax: +49 (0) 841 98 189 100

© 2007 Kaspersky Lab, Ltd.
Kaspersky Lab ist das eingetragene
Warenzeichen von Kaspersky Lab.
Alle anderen Namen sind Warenzeichen Ihrer
Eigentümer.

KASPERSKY^{lab}
www.kaspersky.de