



## Kaspersky Anti-Virus für Proxy Server

- 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<sup>®</sup> **Anti-Virus** für Proxy-Server

Kaspersky Anti-Virus für Proxy-Server ist eine Lösung zum Schutz des Webtraffics (HTTP/FTP) auf Proxy-Servern.

Die Anwendung ermöglicht sicheres Surfen und Arbeiten im Internet und schützt die User vor den meisten Würmern, die über Instant-Messaging-Programme verbreitet werden.

## Funktionen

### Schutz vor Viren, Trojanern und Spyware

**Schutz des Webtraffics in Echtzeit.** Das Programm durchsucht den Datenstrom auf dem Proxy-Server nach Viren aller Art, nach Trojanern und anderen schädlichen Programmen und löscht diese anschließend.

**Individuelle Filterkonfiguration.** Eine große Auswahl an Filter-Parametern, wie etwa die Filterung nach IP- und URL-Adresse, MIME-Typen und nach Dateigröße, ermöglicht die Konfiguration individueller Filterregeln für verschiedene Anwendergruppen.

**Überprüfung von Archivdateien.** Kaspersky Anti-Virus gewährleistet eine hohe Erkennungsqualität und die Desinfizierung von Viren in allen Datei- und Anhangstypen. Die Anwendung unterstützt nahezu alle Archiv- und Packerformate.

**Erkennen potentiell gefährlicher Programme.** Im erweiterten Schutzmodus erkennt und löscht die Anwendung nicht nur eindeutig schädliche, sondern auch potentiell gefährliche Software wie z.B. Spyware.

# Kaspersky® Anti-Virus für Proxy-Server

## Flexible Steuerung

**Remote-Steuerung.** Kaspersky Anti-Virus für Proxy-Server kann sowohl auf traditionelle Weise über die Konfigurationsdatei als auch über das Web-Interface des Programms Webmin gesteuert werden.

**Gruppen-Sicherheits-Policy.** Der Administrator kann individuelle Traffic-Filterregeln für einzelne Anwendergruppen festlegen und diese so der Sicherheits-Policy und den Bedürfnissen der Mitarbeiter anpassen.

**Benachrichtigung der Anwender.** Bei Entdeckung eines infizierten Objekts wird dieses blockiert, und der Anwender erhält eine Benachrichtigung in Form einer HTML-Seite, deren Inhalt, Format und Sprache vom Administrator festgelegt wird.

**Berichte und Statistiken.** Die Anwendung ermöglicht das Erstellen von Statistiken, auf Grund derer der Administrator die Virusaktivität verfolgen und die Funktion der Anwendung überwachen kann.

**Einstellung des Aktualisierungsrhythmus.** Die Aktualisierung der Virendatenbank und der Programmmodule erfolgt auf Anforderung oder automatisch per Zeiteinstellung von den Kaspersky-Lab-Servern bzw. von lokalen Updateservern.

**Zuverlässigkeit.** Der Schutz vor Speicherlecks, Hardwarefehlern, Eingabe-Ausgabe-Fehlern und vor unbearbeiteten Systemabstürzen gewährleistet eine stabile Funktionsfähigkeit und eine hohe Performance der Anwendung.

## Systemanforderungen

### Hardwareanforderungen

#### Mindestkonfiguration:

Mindestens 10 Anwender, Belastung von mindestens 20 Anfragen pro Minute bei einer durchschnittlichen Größe der Anfragen von 15 KB:

- Intel Pentium-Prozessor
- mindestens 64 MB Arbeitsspeicher
- mindestens 200 MB freier Festplattenspeicher zur Speicherung temporärer Dateien und mindestens 50 MB für die Installation

#### Empfohlene Konfiguration:

Mindestens 50 Anwender, Traffic bis 256 MB pro Tag, mittlere Belastung von 20 Anfragen pro Minute, maximale Belastung von 900 Anfragen pro Minute, erforderlicher Speicher bei Spitzenbelastung bis 64 MB:

- Pentium-Prozessor II 300
- mindestens 128 MB Arbeitsspeicher
- mindestens 512 MB freier Festplattenspeicher zur Speicherung temporärer Dateien und 50 MB für die Installation

Mindestens 250 Anwender, Traffic bis 1 GB pro Tag, mittlere Belastung von 150 Anfragen pro Minute, maximale Belastung von 1300 Anfragen pro Minute, erforderlicher Speicher bei Spitzenbelastung bis 512 MB:

- Pentium-Prozessor IV
- mindestens 512 MB Arbeitsspeicher
- mindestens 1 GB freier Festplattenspeicher zur Speicherung temporärer Dateien und mindestens 50 MB für die Installation

### Softwareanforderungen

#### 32-Bit-Plattformen:

- Red Hat Enterprise Linux Advanced Server 4 Update4
- Fedora Core 6
- SUSE Linux Enterprise Server 10
- openSUSE Linux 10.2
- Debian GNU/Linux 3.1 updated (r4)
- Mandriva 2007
- FreeBSD 5.5/6.2

#### 64-Bit-Plattformen:

- Red Hat Enterprise Linux AS/ES 4
- Fedora Core 6
- SUSE Linux Enterprise Server 10
- openSUSE Linux 10.2
- FreeBSD 6.2

#### Einer der folgenden Proxy-Server:

- Squid 2.6, 3.0 (mit Unterstützung des Protokolls ICAP)
- Blue Coat SG Appliance
- NetApp/Blue Coat NetCache
- Cisco ACNS Content Engine

**Webmin ab Version 1.070** ([www.webmin.com](http://www.webmin.com)) zur Remote-Steuerung (optional)

**Perl ab Version 5.0** ([www.perl.org](http://www.perl.org))

Produktversion: 5.7  
Sprache: Englisch

**Kaspersky Labs GmbH**  
Steinheilstr. 13, 85053 Ingolstadt  
[www.kaspersky.de](http://www.kaspersky.de)  
Email: [info@kaspersky.de](mailto: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