



# Kaspersky® Anti-Spam

Mit Kaspersky Anti-Spam sind Mail-Server von Unternehmen und Internet-Providern optimal vor unerwünschten Spam-Mails und unberechtigtem Massenversand geschützt.

Jeder der heute E-Mail nutzt, muss damit rechnen, dass seine Adresse früher oder später in den Datenbanken von Spammern gelistet wird - die Folge ist eine Flut unerwünschter Werbemails. Der Schaden für Unternehmen ist dabei oft enorm: Die Mitarbeiter müssen während ihrer Arbeitszeit dutzende Spam-Mails löschen, außerdem entstehen zusätzliche Traffic-Kosten. Gleichzeitig kann das Mailsystem überlastet werden und es besteht das Risiko, Opfer von Virusepidemien und Erpresser-Attacken zu werden.

Dank innovativer Technologien zur Spam-Erkennung und der langjährigen Erfahrung im Schutz großer Mail-Systeme, hilft Ihnen Kaspersky Anti-Spam, sich von unerwünschten Spam-Mails zu befreien.

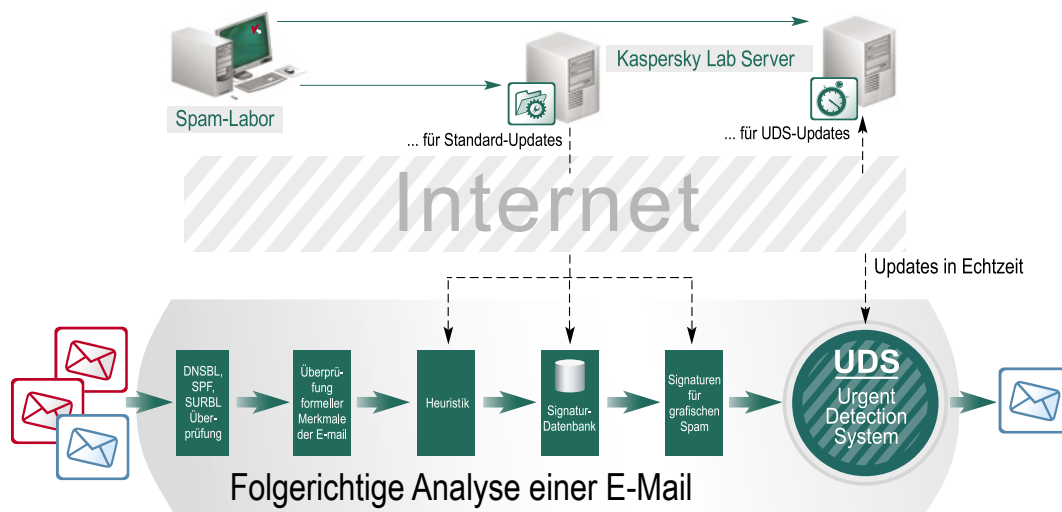
## Die Vorteile

**Fortschrittliche Technologien zum Schutz vor Spam.** Kaspersky Anti-Spam nutzt die intelligente SpamTest-Technologie zur Erkennung unerwünschter Mails: Absender werden mit Schwarzlisten verglichen, E-Mails auf formelle Merkmale geprüft, die linguistische Heuristik erkennt bestimmte Schlüsselwörter und auch Bild-Spams können blockiert werden.

**Schnelle Reaktion auf neue Spam-Mails.** Die Spam-Analysiker bei Kaspersky Lab arbeiten rund um die Uhr, im Minutentakt werden neue Spam-Muster und Tricks zum Umgehen der Anti-Spam-Filter in den Datenbanken ergänzt. Die UDS-Technologie (Urgent Detection System) erlaubt zudem den Empfang von Informationen über die letzten Spam-Versandaktionen – innerhalb weniger Sekunden nach deren Entdeckung und ohne dabei großen Traffic zu verursachen.

**Komfortable Administration.** Das neue, intuitive Web-Interface von Kaspersky Anti-Spam erlaubt dem Administrator die zentrale Steuerung und Einstellung des Programms. Über das erweiterte Statistik-Modul kann der Status der Spam-Blockierung jederzeit überprüft werden.

**Leistungsfähig und flexibel.** Der neue Spam-Filter von Kaspersky Lab verbraucht 4 bis 5 Mal weniger System-Ressourcen als die Vorgängerversion, die Größe der Datenbank-Updates wurde ebenfalls reduziert. Das Programm schützt kleine und große Unternehmen optimal vor unerwünschten Spam-Mails – selbst Mail-Provider wie Mail.Ru, über deren Server täglich bis zu 70 Millionen Nachrichten mit einer Größe von bis zu 500 GByte laufen, vertrauen auf den Spam-Schutz von Kaspersky Lab.



## Funktionen Schutz vor Spam

**Filterung nach Listen.** Das Programm vergleicht die Mail- und IP-Adressen der Absender mit Schwarzslisten (der so genannten DNSBL – DNS-based Blackhole List) der Provider und nicht kommerzieller Unternehmen, so dass eine hohe Erkennungsrate ermöglicht wird. Der Administrator kann zudem Weißlisten erstellen mit Absendern, deren E-Mails auf jeden Fall angenommen werden („Freundes-Liste“).

**SPF und SURBL.** Während des Filterprozesses kann die Autorisierung des Absenders nach der SPF-Technologie (Sender Policy Framework) erfolgen. In Ergänzung zu DNSBL, welche die Spam IP-Adressen blockiert, wird die SURBL-Technologie (Spam URL Realtime Block List) verwendet, welche die Spammer-URL im Nachrichten-Body herausfiltert.

**Analyse der E-Mails.** Alle ankommenden E-Mails werden auf typische Spam-Merkmale geprüft: Unter anderem auf die Modifizierung des Absenders, das Fehlen eines Empfängers beziehungsweise eine große Anzahl Empfänger sowie das Fehlen der IP-Adresse. Außerdem werden auch die Größe und das Format der E-Mails analysiert.

**Linguistische Heuristik.** Die Anwendung überprüft E-Mails auf eine bestimmte Auswahl und Verteilung von Aussagen im Text sowie besondere Schlüsselworte. Dabei scannt der Filter nicht nur den E-Mail-Text, sondern auch die Anhänge.

**Signatur-Analyse.** Für jede Spam-Mail wird automatisch eine Signatur erstellt, die auch die Erkennung modifizierter Varianten der Spam-Mail ermöglicht. Die Datenbanken werden täglich um zehntausende neue Signaturen ergänzt.

**Erkennen von Bild-Spam.** Dank der grafischen Signaturen werden auch Bild-Spams in den Mails selbst sowie den Anhängen erkannt und deren Empfang abgelehnt.

**UDS-Anfragen in Echtzeit.** Kann eine E-Mail nicht eindeutig bewertet werden, schickt das Programm eine Anfrage an den UDS-Server (Urgent Detection System), der Informationen über die letzten Massenversand-Aktionen enthält: Die Daten neuer Spam-Mails werden sofort in die lokale Datenbank des Anwenders übernommen.

## Administration

**Einstellung.** Der Administrator kann die Sicherheits-Stufe des Filters individuell einstellen, eigene Schwarz- und Weißlisten erzeugen, verschiedene Filterregeln wählen und Mails bestimmter Sprachen automatisch blockieren lassen.

**Anwender-Gruppen.** Auch verschiedene Anwender-Gruppen können vom Administrator festgelegt werden – entweder über eine Adressliste oder mit Domain-Masken (etwa \*@???.domain.com). Für jede Gruppe können verschiedene Einstellungen und Filterregeln sowie eine unterschiedliche Bearbeitung der E-Mails eingestellt werden.

**Filter-Logik.** Werden Spam-Mails entdeckt, kann das Programm verschiedene Aktionen durchführen: Die Mail kann automatisch gelöscht, dem Absender eine Ablehnung geschickt und die E-Mail oder eine Kopie davon in einen Quarantäne-Ordner verschoben werden. Außerdem ist es möglich, die Mail mit einer vom Administrator vorgegebenen Kennzeichnung an den Empfänger weiterzuleiten – die Filterung erfolgt dann auf Ebene des E-Mail-Clients.

**Aktualisierung der Datenbanken.** Die Datenbanken werden nach einem vom Administrator festgelegten Zeitplan aktualisiert, als Standard ist die Aktualisierung alle 20 Minuten eingestellt. Werden verdächtige E-Mails entdeckt, die nicht eindeutig als Spam bewertet werden können, wendet sich das Programm in Echtzeit an den UDS-Server.

**Ausführliche Berichte.** Der Administrator kann die Arbeit des Programms, den Schutz-Status und die Lizenz kontrollieren. Dafür stehen anschauliche HTML-Berichte sowie die Log-Dateien von Linux zur Verfügung. Die Berichte können auch in Excel- und CSV-Dateien exportiert werden. Zudem sind Berichte über den gesamten E-Mail-Traffic und den entdeckten Spam-Anteil für einen festgelegten Zeitraum erhältlich.

### System-Anforderungen

#### Hardware

- Intel Pentium III Prozessor 500 MHz oder höher (Intel Pentium IV 2,4 MHz empfohlen)
- mindestens 512 MB freier Arbeitsspeicher (1 GB empfohlen)

#### Software

##### Mail-Server:

- Sendmail 8.13.5 mit Milter API
- Postfix 2.2.2
- Qmail 1.03
- Exim 4.50
- CommuniGate Pro 4.3.7

##### Betriebssysteme:

- RedHat Linux 9.0
- RedHat Fedora Core 3
- RedHat Enterprise Linux Advanced Server 3
- SuSe Linux Enterprise Server 9.0
- SuSe Linux Professional 9.2
- Mandrake Linux version 10.1
- Debian GNU/Linux version 3.1
- FreeBSD version 4.10
- FreeBSD version 5.4

Erforderlich sind die installierten Utilities bzip2, which sowie ein Perl-Interpreter

Sprachen: Englisch, Russisch  
(nur Dokumentation)

Version: 3.0

### Weitere Informationen:

Steinheilstr. 13  
85053 Ingolstadt  
Deutschland

www.kaspersky.de  
www.viruslist.de

Email: info@kaspersky.de

Tel.: +49 (0) 841 98 189 0

Fax: +49 (0) 841 98 189 100

©2006 Kaspersky Lab Ltd. Kaspersky Security ist das eingetragene Warenzeichen von Kaspersky Lab. Alle anderen Namen sind die Warenzeichen ihrer Eigentümer.

