



Sehr geehrter Benutzer,

vielen Dank, dass Sie sich für unser Produkt entschieden haben. Wir hoffen, dass Ihnen dieses Dokument bei der Arbeit hilft und den Großteil der auftauchenden Fragen beantwortet.

Achtung! Die Rechte an diesem Dokument sind Eigentum der Kaspersky Lab ZAO (nachfolgend Kaspersky Lab) und durch russisches Urheberrecht und internationale Verträge geschützt. Die widerrechtliche Vervielfältigung und Verbreitung des Dokuments oder einzelner Teile daraus kann zivilrechtlich, verwaltungsrechtlich und strafrechtlich verfolgt werden.

Das Vervielfältigen, Weiterverbreiten und Übersetzen der Unterlagen ist nur nach vorheriger schriftlicher Genehmigung von Kaspersky Lab zulässig.

Das Dokument sowie dessen grafische Darstellungen dürfen nur zu Informationszwecken für den persönlichen Gebrauch genutzt werden. Eine kommerzielle Nutzung ist nicht gestattet.

Änderungen vorbehalten. Die neueste Version finden Sie auf der Seite von Kaspersky Lab unter der Adresse <http://www.kaspersky.de/docs>.

Kaspersky Lab übernimmt keine Haftung für den Inhalt, die Qualität, die Aktualität und Richtigkeit der im Dokument verwendeten Unterlagen, die das Eigentum anderer Rechtsinhaber sind, sowie für den möglichen Schaden durch die Nutzung dieser Unterlagen.

Redaktionsdatum: 09/04/2012

© Kaspersky Lab ZAO, 2012

[www.kaspersky.de](http://www.kaspersky.de)  
<http://support.kaspersky.com/de/>

# INHALT

ÜBER DIESES HANDBUCH.....	6
In diesem Dokument.....	6
Symbole und Stilkonventionen .....	7
WEITERE INFORMATIONSQUELLEN.....	9
Selbständige Informationssuche.....	9
Diskussion von Kaspersky-Lab-Programmen im Webforum.....	10
Nachricht an das Redaktionsteam für Benutzerdokumentation .....	10
KASPERSKY SECURITY 8.0 FÜR MICROSOFT EXCHANGE SERVER.....	11
Lieferumfang.....	12
Hardware- und Softwarevoraussetzungen .....	12
PROGRAMMARCHITEKTUR .....	15
Programmkomponenten und ihre Funktion.....	15
Architektur des Sicherheitsservers .....	16
TYPISCHER VERLAUF DER PROGRAMMINSTALLATION.....	17
Rollen in Microsoft Exchange Server und zugehörige Konfiguration für den Virenschutz .....	17
Installationsverlauf für den Sicherheitsserver .....	17
Installation des Programms auf einem Servercluster .....	18
Verteilung des Programms unter Microsoft Exchange DAG .....	19
PROGRAMM INSTALLIEREN UND DEINSTALLIEREN .....	20
Programminstallation vorbereiten .....	20
Aktualisierung von Vorgängerversionen .....	21
Vorgehen bei der Installation .....	22
Schritt 1. Erforderliche Komponenten installieren .....	22
Schritt 2. Begrüßung und Lizenzvertrag.....	23
Schritt 3. Installationstyp auswählen .....	23
Schritt 4. Programmkomponenten auswählen .....	23
Schritt 5. Verbindung zum Microsoft SQL Server konfigurieren .....	24
Schritt 6. Dateien kopieren.....	25
Programmbetrieb vorbereiten.....	25
Hinzufügen des Schlüssels.....	26
Schutz für den Server anpassen.....	26
Aktivieren KSN.....	27
Konfiguration des Proxyserver .....	27
Benachrichtigungen anpassen.....	27
Programmfunktionen überprüfen .....	28
Programm wiederherstellen.....	30
Programm löschen .....	30
LIZENZIERUNG DES PROGRAMMS.....	32
Über den Lizenzvertrag .....	32
Über die Lizenz.....	32
Über die Schlüsseldatei.....	33
Über Schlüssel .....	33
Anzeigen von Informationen zu hinzugefügten Schlüsseln.....	34

Hinzufügen des Schlüssels.....	35
Löschen des Schlüssels .....	35
Warnmeldung bei Ablauf der Lizenz.....	36
Liste geschützter Postfächer und Verzeichnisse anlegen .....	36
PROGRAMMOBERFLÄCHE .....	37
Hauptfenster.....	37
Kontextmenü .....	39
PROGRAMM STARTEN UND ANHALTEN .....	40
SCHUTZSTATUS DES SERVERS .....	42
Über den Schutzstatus des Servers .....	42
Anzeigen der Meldungen zum Schutzstatus des Servers.....	45
STANDARDMÄßIGER VIRENSCHUTZSTATUS FÜR MICROSOFT EXCHANGE SERVER.....	47
ERSTE SCHRITTE .....	48
Management-Konsole starten.....	48
Liste geschützter Microsoft Exchange-Server erstellen .....	48
Management-Konsole mit dem Sicherheitsserver verbinden.....	50
REGELMÄßIGES UPDATE DER ANTI-VIREN- UND ANTI-SPAM-DATENBANKEN .....	51
Manuelles Update.....	52
Automatisches Update .....	53
Updatequelle auswählen .....	54
Verbindungseinstellungen anpassen.....	54
VIRENSCHUTZ.....	56
Virenschutz für den Server aktivieren und deaktivieren.....	57
Verarbeitungsregeln für Objekte erstellen .....	58
Dateianhänge in Archiven und Container prüfen .....	59
Schutzeinstellungen für Postfächer einrichten.....	60
Einstellung der Ausnahmen für die Anti-Virenprüfung .....	60
Einstellung der Ausnahmen nach Dateinamensmasken.....	61
Einstellung der Ausnahmen nach Empfängeradressen .....	61
Prüfung im Hintergrund.....	63
SPAMSCHUTZ .....	65
Einstellungen für die Spamprüfung anpassen .....	67
Einstellung der "Whitelist" und "Blacklist" der Absender.....	69
Einstellung der "Whitelist" für E-Mail-Empfänger.....	70
Konfigurierung der Einstellungen zur Ermittlung des Spam-Ratings .....	72
Externe Dienste zur Spamverarbeitung nutzen .....	73
Einstellungen für Anti-Spam-Berichte anpassen .....	74
BACKUP .....	76
Backup-Ordner anzeigen.....	77
Eigenschaften von Objekten im Backup-Ordner anzeigen .....	79
Einstellung der Backup-Ordner-Filter .....	80
Objekte aus dem Backup-Ordner wiederherstellen.....	81
Objekt aus dem Backup an die Empfänger versenden.....	81
Entsendung des Objektes aus dem Backup-Ordner zur Untersuchung .....	82
Objekte aus dem Backup-Ordner wiederherstellen .....	82

Einstellungen für Backup-Ordner anpassen .....	83
BENACHRICHTIGUNGEN.....	84
Benachrichtigungseinstellungen anpassen.....	84
Versandeneinstellungen für Benachrichtigungen anpassen .....	85
BERICHTE .....	86
Die Schnellerstellung eines Berichts .....	86
Einstellungen für Anti-Virus-Berichte anpassen.....	87
Einstellungen für Anti-Spam-Berichte anpassen .....	88
Fertige Berichte anzeigen.....	90
EREIGNISJOURNALE DES PROGRAMMS .....	94
Diagnosetiefe anpassen .....	94
Journaleinstellungen anpassen .....	95
KONFIGURATIONSVERWALTUNG .....	96
Konfiguration exportieren.....	96
Konfiguration importieren.....	97
HÄUFIG GESTELLTE FRAGEN .....	98
KONTAKTAUFNAHME MIT DEM TECHNISCHEM SUPPORT .....	100
GLOSSAR .....	101
KASPERSKY LAB ZAO .....	105
INFORMATIONEN ZU VERWENDETEM FREMDCODE .....	106
HINWEISE ZU MARKENZEICHEN.....	107
INDEX .....	108

# ÜBER DIESES HANDBUCH

Dieses Dokument ist das Administratorhandbuch zu Kaspersky Security 8.0 für Microsoft® Exchange Server (weiter Kaspersky Security oder Programm).

Das Handbuch wendet sich an technische Fachkräfte, zu deren Pflichten die Installation und das Administrieren von Kaspersky Security bzw. der Support von Organisationen, die Kaspersky Security verwenden, gehört.

Das Handbuch erfüllt folgende Zwecke:

- Hilfe für die Einstellung und Anwendung von Kaspersky Security.
- Gewährleistung der schnellen Suche nach Informationen zu Fragen, die mit der Arbeit von Kaspersky Security verbunden sind.
- Benennung weiterer Informationsquellen zum Programm und technischen Support.

## IN DIESEM ABSCHNITT

---

In diesem Dokument .....	<a href="#">6</a>
Symbole und Stilkonventionen .....	<a href="#">7</a>

## IN DIESEM DOKUMENT

Das Administratorhandbuch zu Kaspersky Security 8.0 für Microsoft Exchange Server besteht aus folgenden Abschnitten:

- Über dieses Handbuch. In diesem Kapitel werden das Ziel und die Struktur des Administratorhandbuchs beschrieben.
- Weitere Informationsquellen (s. S. [9](#)). In dieser Abschnitt werden verschiedene Informationsquellen zu Erwerb, Installation und Verwendung von Kaspersky Security beschrieben.
- Kaspersky Security 8.0 für Microsoft Exchange Server (s. S. [11](#)). Dieser Abschnitt beschreibt die wesentlichen Programmfunktionen.
- Programmarchitektur (s. S. [15](#)). Dieser Abschnitt beschreibt die Programmkomponenten und die Möglichkeiten ihrer Zusammenarbeit.
- Typischer Installationsverlauf (s. S. [17](#)). Dieser Abschnitt beschreibt die Rollen von Microsoft Exchange Server und den Installationsverlauf des Serverschutzes.
- Programm installieren (s. S. [20](#)). Dieser Abschnitt beschreibt detailliert die Schritte zur Installation von Kaspersky Security.
- Lizenzverwaltung (s. S. [32](#)). Dieses Kapitel beschreibt die verschiedenen Lizenztypen sowie die Schritte zur Installation und zur Löschung von Lizenzen.
- Programmoberfläche (s. S. [37](#)). Dieses Kapitel beschreibt die Benutzeroberfläche von Kaspersky Security.
- Programm starten und anhalten (s. S. [40](#)). Dieses Kapitel beschreibt, wie das Programm gestartet und vorübergehend angehalten wird.
- Standardmäßiger Virenschutzstatus für Microsoft Exchange Server (s. S. [47](#)). Dieses Kapitel beschreibt die Besonderheiten beim Verwenden der Standardeinstellungen für Kaspersky Security.

- Erste Schritte (s. S. [48](#)). Dieses Kapitel beschreibt die ersten Schritte zur Verwendung von Kaspersky Security, das Aktivieren des Schutzes für E-Mail-Server und das Erstellen der Liste geschützter Server.
- Regelmäßiges Update der Naiveren- und Anti-Spam-Datenbanken (s. S. [51](#)). Dieses Kapitel beschreibt das Anpassen der Updateeinstellungen für Kaspersky Security.
- Virenschutz (s. S. [56](#)). Dieses Kapitel beschreibt das Einrichten des Virenschutzes für E-Mail-Server.
- Spamschutz (s. S. [65](#)). Dieses Kapitel beschreibt die Programmfunktionen für den Schutz von Mailservern vor Spammnachrichten.
- Backup (s. S. [76](#)). Dieses Kapitel beschreibt die Funktionen des Backup-Ordners, die Möglichkeiten zur Wiederherstellung von Objekten aus dem Backup-Ordner sowie das Anpassen der Einstellungen für den Backup-Ordner.
- Benachrichtigungen (s. S. [84](#)). Das Kapitel beschreibt Verfahren zum Erhalten von Benachrichtigungen über Ereignisse von Kaspersky Security.
- (s. S. [86](#)). Dieses Kapitel beschreibt, wie Sie Berichte in Kaspersky Security erstellen, anzeigen und per E-Mail versenden können.
- Ereignisjournal (s. S. [94](#)). In diesem Kapitel wird die Einstellung der Parameter für die Ereignisjournale beschrieben, die bei der Arbeit von Anti-Virus- und Anti-Spam-Programmen sowie anderen Kaspersky-Security-Ereignissen erzeugt werden.
- Häufig gestellte Fragen (s. S. [98](#)). Dieses Kapitel gibt Antwort auf die von Nutzern am häufigsten gestellten Fragen.
- Kontaktaufnahme mit dem technischen Support (s. S. [100](#)). Dieses Kapitel beschreibt, wie und wo sie technische Unterstützung zum Programm bekommen können.
- Terminologieglossar (s. S. [104](#)). In diesem Kapitel werden die im Programm vorkommenden Begriffe kurz erläutert.
- Kaspersky Lab" (s. S. [105](#)). Das Kapitel enthält kurze Informationen über das Unternehmen.
- Informationen zu verwendetem Fremdcode (s. S. [106](#)). Dieses Kapitel enthält Informationen zu verwendeten Quellcodes anderer Hersteller in Kaspersky Security.

## SYMBOLS UND STILKONVENTIONEN

Der Text des Dokumentes wird von den Bedeutungselementen begleitet, auf die wir Ihnen empfehlen zuzuwenden, - die Warnungen, die Räte, den Beispielen.

Für die Absonderung der Bedeutungselemente werden die bedingten Bezeichnungen verwendet. Die bedingten Bezeichnungen und die Beispiele ihrer Nutzung sind in der Tabelle niedriger gebracht.

Tabella 1. Symbole und Stilkonventionen

TEXTBEISPIEL	BESCHREIBUNG
Beachten Sie, dass...	Die Warnungen sind von der roten Farbe gewählt und sind in den Rahmen geschlossen. Warnungen informieren darüber, dass unerwünschte Aktionen möglich sind, die zu Datenverlust oder zu Störungen bei der Arbeit der Software oder des Betriebssystems führen können.
Wir empfehlen,... zu verwenden	Die Anmerkungen sind in den Rahmen geschlossen. Hinweise können nützliche Tipps, Empfehlungen und spezielle Parameterwerte enthalten oder sich auf wichtige Sonderfälle bei der Arbeit mit dem Programm beziehen.

TEXTBEISPIEL	BESCHREIBUNG
<p><b>Beispiel:</b></p> <p>...</p>	<p>Die Beispiele sind in den Blöcken auf dem gelben Hintergrund unter dem Titel "Beispiel" gebracht.</p>
<p><i>Updates</i> sind...</p> <p>Es entsteht das Ereignis <i>veraltete Datenbanken</i>.</p>	<p>Von der Kursivschrift sind die folgenden Bedeutungselemente des Textes gewählt:</p> <ul style="list-style-type: none"> <li>• die neuen Termini;</li> <li>• die Titel der Status und der Ereignisse des Programms.</li> </ul>
<p>Betätigen Sie die Schaltfläche <b>ENTER</b>.</p> <p>Betätigen Sie die Kombination der Schaltflächen <b>ALT+F4</b>.</p>	<p>Bezeichnungen von Tasten sind halbfett und in Großbuchstaben geschrieben.</p> <p>Die Titel der Schaltfläche, der vom Zeichen + (Plus) verbunden ist, bedeuten die Kombination der Schaltfläche. Solche Schaltfläche muss man gleichzeitig drücken.</p>
<p>Betätigen die Schaltfläche <b>Aktivieren</b>.</p>	<p>Die Titel der Interfaceelemente des Programms, zum Beispiel, der Eingabefelder, der Punkte des Menüs, der Knöpfe, sind von der halbfettigen Schrift gewählt.</p>
<p>➡ <i>Um den Zeitplan zur Ausführung des Tasks einzurichten, gehen Sie wie folgt vor:</i></p>	<p>Die einführenden Phrasen der Instruktionen sind auch durch Abzeichen "Pfeil" und Kursiv hervorgehoben.</p>
<p>In der Kommandozeile geben Sie den Text <code>help</code> ein</p> <p>Es wird die folgende Mitteilung erscheinen:</p> <p>Bezeichnen Sie das Datum im Format <code>TT:MM:JJ</code>.</p>	<p>Vom speziellen Stil sind die folgenden Typen des Textes gewählt:</p> <ul style="list-style-type: none"> <li>• Text der Kommandozeile;</li> <li>• Text der Mitteilungen, die vom Programm auf den Bildschirm herausgeführt werden;</li> <li>• Daten, die der Benutzer eingeben muss.</li> </ul>
<p>&lt;Benutzername&gt;</p>	<p>Variablen stehen in spitzen Klammern. Anstelle der Variablen muss ihr entsprechender Wert ohne spitze Klammern eingesetzt werden.</p>

# WEITERE INFORMATIONSQUELLEN

Hier erhalten Sie schnelle Antworten auf mögliche Fragen zu Auswahl, Erwerb, Installation und Verwendung von Kaspersky Security.

Kaspersky Lab bietet zu diesem Zweck unterschiedliche Informationsquellen zu dem Programm an. Sie können je nach Dringlichkeit und Wichtigkeit Ihrer Frage eine passende Quelle wählen.

## IN DIESEM ABSCHNITT

---

Selbständige Informationssuche .....	<a href="#">9</a>
Diskussion von Kaspersky-Lab-Programmen im Webforum .....	<a href="#">10</a>
Nachricht an das Redaktionsteam für Benutzerdokumentation.....	<a href="#">10</a>

## SELBSTÄNDIGE INFORMATIONSSUCHE

Bei Fragen über die Anwendung stehen folgende Informationsquellen zur Verfügung:

- Seite über das Programm auf der Webseite von Kaspersky Lab
- Seite über das Programm auf der Webseite des Technischen Supports (in der Wissensdatenbank).
- Elektronisches Hilfesystem
- Dokumentation

### Seite auf der Webseite von Kaspersky Lab

[http://www.kaspersky.de/business\\_products](http://www.kaspersky.de/business_products)

Auf dieser Website finden Sie allgemeine Informationen zu Kaspersky Security und zur Verwendung des Programms.

### Seite auf der Webseite des Technischen Supports (Wissensdatenbank)

<http://support.kaspersky.com/de/exchange>

Auf dieser Seite finden Sie Artikel, die von Spezialisten des Technischen Supports veröffentlicht wurden.

Diese Artikel enthalten nützliche Informationen, Empfehlungen und Antworten auf häufig gestellte Fragen zur Verwendung von Kaspersky Security.

### Elektronisches Hilfesystem

In der elektronischen Hilfe finden Sie Informationen zum Einrichten der Programmkomponenten und Hinweise zur Programmverwaltung.

Um die elektronische Hilfe aufzurufen, wählen Sie **Hilfe** im Menü **Aktion** der Management-Konsole.

Bei Fragen zu den einzelnen Programmfenstern oder Registerkarten von Kaspersky Security können Sie die Kontexthilfe aufrufen.

Zum Aufrufen der Kontexthilfe öffnen Sie das gewünschte Programmfenster bzw. die Registerkarte, und betätigen Sie die Schaltfläche **F1**.

## Dokumentation

Dieses Administratorhandbuch für Kaspersky Security enthält sämtliche erforderlichen Informationen zur Arbeit mit dem Programm und ist im Lieferumfang enthalten.

## DISKUSSION VON KASPERSKY-LAB-PROGRAMMEN IM WEBFORUM

Wenn Ihre Frage keine dringende Antwort erfordert, können Sie sie mit den Spezialisten von Kaspersky Lab und mit anderen Anwendern in unserem Forum unter der Adresse <http://forum.kaspersky.com> diskutieren.

Im Forum können Sie bereits veröffentlichte Themen nachlesen, eigene Kommentare verfassen, neue Themen eröffnen und die Suchfunktion verwenden.

## NACHRICHT AN DAS REDAKTIONSTEAM FÜR BENUTZERDOKUMENTATION

Bei Fragen und Anmerkungen zur Programmdokumentation, oder falls Sie Fehler entdecken, können Sie sich direkt an unser Redaktionsteam wenden.

Über den link **Feedback schreiben** abgeben rechts oben im Hilfefenster können Sie das E-Mail-Programm Ihres Computers direkt aufrufen. Es wird eine neue E-Mail-Nachricht geöffnet. In der Adresszeile erscheint für den Empfänger automatisch die E-Mail-Adresse unseres Redaktionsteams – [docfeedback@kaspersky.com](mailto:docfeedback@kaspersky.com), in der Betreffzeile – "Kaspersky Help Feedback: Kaspersky Security". Im Textkörper der E-Mail können Sie Ihre Nachricht direkt eingeben. Bitte ändern Sie nicht die automatisch erzeugte Betreffzeile.

# KASPERSKY SECURITY 8.0 FÜR MICROSOFT EXCHANGE SERVER

Kaspersky Security 8.0 für Microsoft Exchange Server ist ein Programm zum Schutz von E-Mail-Servern unter Microsoft Exchange Server vor Viren, Trojanern, Würmern und anderen Bedrohungen, die über eingehenden E-Mails auf den Computer gelangen können.

Schädliche Anwendungen wie diese können erheblichen Schaden verursachen: Sie werden mit dem Ziel geschrieben, auf Computern gespeicherte Daten zu stehlen, zu blockieren, zu manipulieren oder unbrauchbar zu machen, um die ordnungsgemäße Funktion von Computern und Netzwerken zu stören. In Massen versandt, können sich Viren schnell über das gesamte Firmennetzwerk ausbreiten, die Server des Unternehmens und die Computer Ihrer Mitarbeiter lahmlegen, was erhebliche Ausfallzeiten und somit Verluste für das Unternehmen bedeuten kann. Außerdem können Virusattacken zu Datenverlusten führen und dadurch sowohl Ihr Unternehmen als auch Ihre Geschäftspartner schädigen.

Kaspersky Security schützt die E-Mail-Server Ihres Unternehmens vor Spam. Unerwünschte E-Mails müssen so nicht mehr von jedem Mitarbeiter individuell und von Hand gelöscht werden.

Kaspersky Security schützt E-Mail-Postfächer, öffentliche Ordner und den gesamten E-Mail-Verkehr unter Microsoft Exchange Server vor schädlichen Programmen und Spam-Mails. Hierbei wird der gesamte durchlaufende E-Mail-Verkehr auf Servern unter Microsoft Exchange Server überwacht.

Kaspersky Security bietet Ihnen folgende Möglichkeiten:

- Prüfung eingehender, ausgehender und auf dem Microsoft Exchange Server gespeicherter E-Mails (auch in öffentlichen Ordnern) auf schädliche Objekte. Bei der Prüfung wird nicht nur die Nachricht selbst, sondern auch alle Anlagen bearbeitet. Je nach den gewählten Programmeinstellungen werden die gefundenen schädlichen Objekte desinfiziert oder gelöscht, und der Benutzer erhält eine entsprechende Meldung.
- Filtern des E-Mail-Verkehrs auf unerwünschte E-Mails (Spam). Durch das Anti-Spam-Modul wird der gesamte E-Mail-Verkehr auf unerwünschte E-Mails hin geprüft. Mit Anti-Spam können Sie außerdem "Whitelists" und "Blacklists" für E-Mail-Absenderadressen anlegen sowie unterschiedlich hohe Sicherheitsstufen zur Spamprüfung von E-Mails einstellen.
- Speichern von Kopien infizierter und verdächtiger Objekte (E-Mail-Nachrichten und Anlagen) sowie Spam-Nachrichten im Backup-Ordner vor dem Desinfizieren bzw. Löschen, um sie später wiederherstellen zu können, was Informationsverluste ausschließt. Schnelle Suche nach Kopien der Ursprungsdateien über benutzerdefinierte Filter.
- Benachrichtigung von Absendern, Empfängern und Virenschutzadministratoren über infizierte E-Mail-Nachrichten.
- Führen von Ereignisjournalen, Statistiken und periodische Berichterstattung zur Funktion des Programms. Berichte können nach voreingestellten Zeitplänen oder ad-hoc auf Benutzeranfrage erstellt werden.
- Programmeinstellungen können individuell je nach Menge und Art des durchlaufenden E-Mail-Verkehrs konfiguriert werden, z.B. durch Timeouts für Verbindungen zur Effizienzsteigerung bei der Überprüfung.
- Wahlmöglichkeit zwischen automatischen und manuellen Programmupdates für Kaspersky Security. Als Updatequellen können die FTP- und HTTP-Updateserver von Kaspersky Lab über das Internet, lokale bzw. Netzwerkordner mit den aktuellen Updates oder auch benutzerdefinierte FTP- und HTTP-Server dienen.
- Prüfung älterer (bereits früher geprüfter) E-Mail-Nachrichten auf neuere Viren anhand voreingestellter Zeitpläne durchführen. Diese Prüfung wird im Hintergrund ausgeführt und beeinträchtigt die Performance des E-Mail-Servers nur geringfügig.
- Virenschutz auf Ordner Ebene aufgrund der erstellten Liste der zu schützenden Speicherordner ausführen.

**IN DIESEM ABSCHNITT**

Lieferumfang .....	<a href="#">12</a>
Hardware- und Softwarevoraussetzungen .....	<a href="#">12</a>

**LIEFERUMFANG**

Kaspersky Security kann bei unseren Vertriebspartnern oder in einem Online-Shop (z.B. <http://www.kaspersky.com/de>, Abschnitt E-Store) erworben werden. Kaspersky Security wird wie der Teil Kaspersky Security für E-Mail Server geliefert, und auch Kaspersky Open Space Security als Teil Kaspersky Enterprise Space Security und Kaspersky Total Space Security. Nach dem Erwerb einer Lizenz für Kaspersky Security erhalten Sie per E-Mail einen Link für den Download des Programms und des Aktivierungsschlüssels von unserer Homepage, oder wir senden Ihnen das Installationspaket auf CD zu. Lesen Sie bitte vor dem Öffnen des Umschlags mit der CD den Lizenzvertrag sorgfältig durch.

**HARDWARE- UND SOFTWAREVORAUSSETZUNGEN****Hardwarevoraussetzungen**

Die Hardwarevoraussetzungen für Kaspersky Security sind dieselben wie auch für die Installation von Microsoft Exchange Server. Je nach gewählter Programmkonfiguration und Funktionsmodus kann es sein, dass sehr viel Speicherplatz auf dem lokalen Datenträger für den Backup-Ordner und andere Hilfsverzeichnisse benötigt wird (bei Verwendung der standardmäßigen Voreinstellungen kann der Backup-Ordner bis zu 5120 MB belegen).

Es gelten folgende Hardwarevoraussetzungen für die Management-Konsole, die zusammen mit dem Programm installiert werden muss:

- Prozessor Intel® Pentium® 400 MHz oder höher (empfohlen werden 1000 MHz);
- 256 MB Arbeitsspeicher;
- 500 MB freier Speicherplatz auf dem lokalen Datenträger für die Installation.

**Softwarevoraussetzungen**

Für die Installation von Kaspersky Security ist eines der folgenden Betriebssysteme erforderlich:

- Microsoft Small Business Server 2011;
- Microsoft Small Business Server 2008 Standard x64;
- Microsoft Small Business Server 2008 Premium x64;
- Microsoft Essential Business Server 2008 Standard x64;
- Microsoft Essential Business Server 2008 Premium x64;
- Microsoft Windows Server 2008 x64 R2 Enterprise Edition Service Pack 1;
- Microsoft Windows Server 2008 x64 R2 Standard Edition Service Pack 1;
- Microsoft Windows Server 2008 x64 Enterprise Edition Service Pack 2;
- Microsoft Windows Server 2008 x64 Standard Edition Service Pack 2;

- Microsoft Windows Server 2003 x64 R2 Enterprise Edition Service Pack 2;
- Microsoft Windows Server 2003 x64 R2 Standard Edition Service Pack 2;
- Microsoft Windows Server 2003 x64 Enterprise Edition Service Pack 2;
- Microsoft Windows Server 2003 x64 Standard Edition Service Pack 2.

Für die Installation von Kaspersky Security ist folgende Software erforderlich:

- Microsoft Exchange Server 2007 x64 Service Pack 3 oder Microsoft Exchange Server 2010 Service Pack 1, eine der folgenden Rollen installiert ist: Hub Transport, Mailbox oder Cross Border Server;
- Eine der folgenden Datenbankbetriebssysteme: Microsoft SQL Server® 2005 Express Edition, Microsoft SQL Server 2005 Standard Edition, Microsoft SQL Server 2005 Enterprise Edition, Microsoft SQL Server 2008 Express Edition, Microsoft SQL Server 2008 Standard Edition, Microsoft SQL Server 2008 Enterprise Edition, Microsoft SQL Server 2008 R2 Express Edition, Microsoft SQL Server 2008 R2 Standard Edition, Microsoft SQL Server 2008 R2 Enterprise Edition;
- Microsoft .NET Framework 3.5 Service Pack 1.

Für die Installation der Management-Konsole ist eines der folgenden Betriebssysteme erforderlich:

- Microsoft Small Business Server 2011;
- Microsoft Small Business Server 2008 Standard;
- Microsoft Small Business Server 2008 Premium;
- Microsoft Essential Business Server 2008 Standard;
- Microsoft Essential Business Server 2008 Premium;
- Microsoft Windows Server 2008 x64 R2 Enterprise Edition Service Pack 1;
- Microsoft Windows Server 2008 x64 R2 Standard Edition Service Pack 1;
- Microsoft Windows Server 2008 x64 Enterprise Edition Service Pack 2;
- Microsoft Windows Server 2008 x64 Standard Edition Service Pack 2;
- Microsoft Windows Server 2008 Enterprise Edition Service Pack 2;
- Microsoft Windows Server 2008 Standard Edition Service Pack 2;
- Microsoft Windows Server 2003 x64 Service Pack 2;
- Microsoft Windows Server 2003 x64 R2 Standard Edition;
- Microsoft Windows Server 2003 x64 R2 Enterprise Edition;
- Microsoft Windows® XP x64 Service Pack 2;
- Microsoft Windows Vista x64;
- Microsoft Windows Server 2003 R2 Standard Edition;
- Microsoft Windows Server 2003 R2 Enterprise Edition;
- Microsoft Windows Vista;

- Microsoft Windows Server 2003 Service Pack 2;
- Microsoft Windows XP Service Pack 3;
- Microsoft Windows 7 Professional;
- Microsoft Windows 7 Professional x64;
- Microsoft Windows 7 Enterprise;
- Microsoft Windows 7 Enterprise x64;
- Microsoft Windows 7 Ultimate;
- Microsoft Windows 7 Ultimate x64.

Für die Installation der Konsole ist folgende Software erforderlich:

- Microsoft Management Console 3.0;
- Microsoft .NET Framework 3.5 Service Pack 1.

# PROGRAMMARCHITEKTUR

Kaspersky Security überprüft eingehende, ausgehende und auf dem Server gespeicherte E-Mails auf Viren und filtert Spammitteilungen heraus. Das Programm prüft sowohl den Textkörper der E-Mails als auch Dateianhänge in beliebigen Formaten. Schädliche Programme und Spam werden anhand der Datenbankeinträge von Kaspersky Security gesucht und identifiziert. Die Datenbanken werden durch Kaspersky Lab laufend aktualisiert und stehen auf den Updateservern zum Download per Internet zur Verfügung.

Weiterhin erfolgt eine Prüfung durch ein besonderes Verfahren "Heuristische Analyse", um auch neue, unbekannte Viren aufzuspüren. Die Spamprüfung erfolgt durch die Komponente Anti-Spam, die mehrere verschiedene Verfahren zur Identifizierung und Bekämpfung von Spam verwendet. Die Prüfung der auf dem Server eingehenden Objekte erfolgt in Echtzeit. Der Inhalt neu eingehender Nachrichten kann erst angezeigt werden, nachdem diese überprüft wurden. Jedes einzelne Objekt wird entsprechend den vom Administrator eingestellten Aktionen für den jeweiligen Objekttyp behandelt. Sie können Regeln der Verarbeitung von bösartigen Objekten (s. Abschnitt "Verarbeitungsregeln für Objekte erstellen" auf S. [58](#)) und Spam (s. Abschnitt "Einstellungen für die Spamprüfung anpassen" auf S. [67](#)) erstellen.

Vor dem Ändern von Objekten können diese vom Programm in einem speziellen Backup-Ordner gespeichert werden, um sie später wiederherstellen zu können oder zur Untersuchung an Kaspersky Lab einzusenden. Das Programm kann Benachrichtigungen zu Ereignissen an den für den Virenschutz verantwortlichen Administrator sowie die Empfänger und Absender der betreffenden Nachrichten versenden oder auch entsprechende Einträge im Ereignisjournal von Kaspersky Security sowie im Microsoft-Windows-Ereignisjournal vornehmen.

## IN DIESEM ABSCHNITT

---

Programmkomponenten und ihre Funktion .....	<a href="#">15</a>
Architektur des Sicherheitsservers .....	<a href="#">16</a>

## PROGRAMMKOMPONENTEN UND IHRE FUNKTION

Das Programm besteht aus folgenden Hauptkomponenten:

- **Sicherheitsserver.** Dieser wird auf einen Microsoft Exchange-Server installiert. Er filtert den gesamten E-Mail-Verkehr auf Spamobjekte und gewährleistet den Schutz vor Viren. Der Sicherheitsserver fängt unter Microsoft Exchange Server eingehende E-Mails ab und prüft diese durch das Anti-Viren- und Anti-Spam-Modul auf Viren bzw. Spam. Werden in eingehenden E-Mails Viren oder Spam gefunden, können die betroffenen Objekte entweder im Backup-Ordner gespeichert oder sofort gelöscht werden - je nachdem, welche Einstellungen für Anti-Virus und Anti-Spam festgelegt wurden.
- **Die Management-Konsole** ist ein spezielles autonomes Tool unter Verwendung der MMC 3.0. Die Management-Konsole kann auf dem gleichen Server wie Microsoft Exchange aber auch auf einem Remoteserver zur Remoteüberwachung der Sicherheit auf dem Microsoft Exchange-Server installiert werden. Über die Management-Konsole können Sie Listen von geschützten Servern unter Microsoft Exchange anlegen und den Sicherheitsserver verwalten.

# ARCHITEKTUR DES SICHERHEITSSERVERS

Die Serverkomponente des Programms – der Sicherheitsserver – besteht aus folgenden Subsystemen:

- Das Abfangmodul für E-Mails. Fängt in den Microsoft Exchange Server eingehende E-Mails ab und prüft diese durch das Anti-Viren- und Anti-Spam-Modul. Diese Komponente wird mithilfe der VSAPI 2.6-Technologie oder der Transport-Agents-Technologie in die Prozesse von Microsoft Exchange Server integriert, je nachdem, für welche Rolle Microsoft Exchange Server installiert ist.
- Anti-Virus-Modul. Prüft Objekte auf vorhandene Viren. Beinhaltet den Anti-Viruskern und ein Verzeichnis, in dem temporäre Objekte zur Prüfung im Arbeitsspeicher aufbewahrt werden. Es ist dies das Hilfsverzeichnis Store.

Der Ordner Store wird im Installationsordner des Programms (standardmäßig <Installdir>/data) angelegt und muss in den im Firmennetzwerk installierten Virenschutzprogrammen von der Überprüfung ausgeschlossen werden. Ansonsten kann es zu Funktionsfehlern bei der Ausführung des Programms kommen.

- Anti-Spam. Filtert unerwünschte E-Mail-Nachrichten aus. Nach dem Abfangen der E-Mail übergibt das Abfangmodul für E-Mails die Mitteilung an Anti-Spam zur Kontrolle. Kopien gelöschter Objekte können im Backup-Ordner aufbewahrt werden.
- Das Modul zur internen Programmsteuerung und Überwachung der Unversehrtheit. Dies ist ein Dienstprogramm von Microsoft Windows, das Kaspersky Security 8.0 für Microsoft Exchange Server genannt wird. Es wird automatisch beim Durchlaufen der ersten E-Mail, beim Verbindungsaufbau der Management-Konsole zum Sicherheitsserver sowie nach Abschluss des Installationsassistenten gestartet. Das Dienstprogramm funktioniert unabhängig vom Status des Microsoft Exchange Server, das Programm kann auch konfiguriert werden, wenn der Microsoft Exchange Server angehalten wurde. Im Modus "Prüfung im Hintergrund" empfängt das interne Programmsteuerungsmodul in Abhängigkeit der gewählten Einstellungen von Microsoft Exchange Server sämtliche in öffentlichen Ordnern und zu schützenden Verzeichnissen gespeicherte E-Mail-Nachrichten. Wurde zur Prüfung von Nachrichten nicht die aktuellste Version der Programmdateibanken verwendet, übergibt das Programm die Nachrichten an die Komponente Anti-Virus. Die Verbreitung von Objekten im Hintergrundmodus läuft genau so ab, wie bei der Überwachung des E-Mail-Verkehrs. Damit das Programm korrekt funktioniert, muss das interne Steuerungsmodul stets aktiviert sein. Wir empfehlen, den Dienst nicht manuell zu stoppen.

# TYPISCHER VERLAUF DER PROGRAMMINSTALLATION

Kaspersky Security wird auf demselben Server installiert wie auch Microsoft Exchange. Die Auswahl der verfügbaren Komponenten für die Installation richtet sich danach, für welche Rolle Microsoft Exchange Server installiert ist. Kaspersky Security kann auch auf einem Servercluster und auf Gruppe des Zugriffs der Datenbanken Microsoft Exchange installiert werden. Wir empfehlen Ihnen, dieses Kapitel genau zu lesen, um die für Sie geeignete Installationsvariante zu finden.

## IN DIESEM ABSCHNITT

---

Rollen in Microsoft Exchange Server und zugehörige Konfiguration für den Virenschutz .....	<a href="#">17</a>
Installationsverlauf für den Sicherheitsserver .....	<a href="#">17</a>
Installation des Programms auf einem Servercluster .....	<a href="#">18</a>
Verteilung des Programms unter Microsoft Exchange DAG.....	<a href="#">19</a>

## ROLLEN IN MICROSOFT EXCHANGE SERVER UND ZUGEHÖRIGE KONFIGURATION FÜR DEN VIRENSCHUTZ

Damit Kaspersky Security ordnungsgemäß funktioniert, muss der geschützte Microsoft Exchange-Server für mindestens eine der folgenden Rollen installiert sein:

- Mailbox
- Hub Transport
- Edge Transport.

Ist Microsoft Exchange Server für die Rolle Mailbox installiert, verwendet Kaspersky Security für die Verbindung den Standard VSAPI 2.6. In allen anderen Fällen wird die Transport-Agent-Technologie verwendet. Dabei werden für die Hub Transport Rolle die Objekte zuerst durch Kaspersky Security und anschließend durch die Transportassistenten von Microsoft Exchange verarbeitet. Für die Edge Transport Rolle ist der Ablauf genau umgekehrt – die Objekte werden zuerst durch die Transportassistenten von Microsoft Exchange und anschließend durch Kaspersky Security verarbeitet.

## INSTALLATIONSVERLAUF FÜR DEN SICHERHEITSSERVER

Der Schutz für E-Mail Server wird wie folgt installiert:

1. Die Komponente Sicherheitsserver wird auf allen zu schützenden Microsoft Exchange-Servern im Netz installiert. Dabei ist das Installationspaket auf jedem einzelnen Server separat auszuführen.
2. Gemeinsam mit der Komponente Sicherheitsserver wird die Management-Konsole installiert, über die Sie als Administrator Zugriff auf alle unter Kaspersky Security installierten Sicherheitsserver haben. Falls erforderlich, installieren Sie die Management-Konsole auf einem separaten Computer innerhalb des Firmennetzwerkes. Falls mehrere Administratoren das Programm gemeinsam verwalten, muss die Management-Konsole auf jedem ihrer Computer installiert sein.

3. Es wird die Liste der gesteuerten Server erstellt (s. Abschnitt "Liste geschützter Microsoft Exchange-Server erstellen" auf S. [48](#)).
4. Verwaltungskonsole verbindet sich mit dem Sicherheitsserver (s. Abschnitt "Management-Konsole mit dem Sicherheitsserver verbinden" auf S. [50](#)).

## INSTALLATION DES PROGRAMMS AUF EINEM SERVERCLUSTER

Kaspersky Security unterstützt folgende Clustertypen:

- Cluster mit nur einem Speicherverzeichnis (Single Copy Clusters, SCC);
- Cluster mit permanenter Replikation (Cluster Continuous Replication, CCR).

Während der Installation wird das Servercluster automatisch vom Programm erkannt. Die Reihenfolge der Programminstallation auf den Clusterknoten spielt dabei keine Rolle. Das Vorgehen bei der Installation von Kaspersky Security auf einem Servercluster unterscheidet sich wie folgt von der üblichen Installation:

- Bevor die Installation von Kaspersky Security auf allen Clusterknoten abgeschlossen ist, können Sie die Clusterserver für die Postfächer (CMS) nicht zwischen den einzelnen Node verschieben.
- Für die korrekte Arbeit des Backup-Ordners und der Statistik-Komponente ist es nötig, eine einheitliche Datenbank für alle Cluster-Nodes zu verwenden. Dazu muss diese Datenbank bei der Installation von Kaspersky Security auf allen Cluster-Nodes angegeben werden.
- Das für die Installation verwendete Benutzerkonto muss eine Schreibberechtigung für den Konfigurationsbereich von Active Directory® besitzen.

Wenn im Cluster eine Firewall aktiviert ist, muss der Kaspersky-Security-Dienst in die Liste vertrauenswürdiger Applikationen auf jedem Cluster-Node eingetragen werden. Das ist für die korrekte Zusammenarbeit von Kaspersky Security mit dem Backup notwendig.

Nach der Installation auf einem Servercluster wird ein großer Teil der Programmeinstellungen im Active Directory gespeichert, und alle Nodes in einem Cluster verwenden diese Einstellungen. Kaspersky Security erkennt automatisch die aktiven Clusterknoten und verteilt die Konfigurationseinstellungen aus Active Directory.

Das Vorgehen beim Deinstallieren von Kaspersky Security aus einem Servercluster unterscheidet sich wie folgt vom üblichen Deinstallationsvorgang:

- Bevor der Deinstallationsvorgang für Kaspersky Security abgeschlossen ist, können Sie die Clusterserver für die Postfächer (CMS) nicht zwischen den einzelnen Node verschieben.
- Beim Deinstallieren des Programms von einem aktiven Clusterknoten werden die Clusterressource vom Typ Microsoft Exchange Information Store und alle mit ihr verknüpften Ressourcen vom Typ Microsoft Exchange Database Instance gestoppt. Der Ausgangsstatus der Clusterressourcen wird nach Abschluss des Löschvorgangs wiederhergestellt.
- Nach der Deinstallation des Programms bleibt die Cluster-Konfiguration im Active Directory erhalten und kann ggf. für eine nochmalige Installation des Programms verwendet werden.

# VERTEILUNG DES PROGRAMMS UNTER MICROSOFT EXCHANGE DAG

Das Kaspersky-Security-Programm kann auf Servern installiert werden, die der Microsoft Exchange *Database Availability Group* (DAG) angehören.

Während der Installation wird die Microsoft Exchange Database Availability Group (im folgenden als Database Availability Group oder DAG bezeichnet) vom Programm automatisch erkannt. Die Reihenfolge der Programminstallation auf den DAG-Nodes spielt dabei keine Rolle. Das Vorgehen bei der Installation von Kaspersky Security auf DAG unterscheidet sich wie folgt von der üblichen Installation:

- Für die korrekte Arbeit des Backup-Ordners und der Statistik-Komponente ist es nötig, eine einheitliche Datenbank für alle Cluster-Nodes zu verwenden. Dazu muss diese Datenbank bei der Installation von Kaspersky Security auf allen DAG-Nodes angegeben werden.
- Das für die Installation verwendete Benutzerkonto muss eine Schreibberechtigung für den Konfigurationsbereich von Active Directory besitzen.

Wenn auf den Servern, die DAG angehören, eine Firewall aktiviert ist, muss der Kaspersky-Security-Dienst in die Liste vertrauenswürdiger Applikationen auf jedem DAG-Server aufgenommen werden. Das ist für die korrekte Zusammenarbeit von Kaspersky Security mit dem Backup notwendig.

Nach der Installation auf einem Servercluster wird ein großer Teil der Programmeinstellungen im Active Directory gespeichert, und alle Nodes in einem Cluster verwenden diese Einstellungen. Kaspersky Security erkennt automatisch die aktiven Server und übernimmt für sie die Konfigurationseinstellungen aus Active Directory.

Nach der Deinstallation des Programms bleibt die Cluster-Konfiguration im Active Directory erhalten und kann ggf. für eine nochmalige Installation des Programms verwendet werden.

# PROGRAMM INSTALLIEREN UND DEINSTALLIEREN

Kaspersky Security besteht aus zwei Hauptkomponenten: Sicherheitsserver und Management-Konsole. Der Sicherheitsserver wird immer gemeinsam mit der Management-Konsole installiert. Die Management-Konsole kann separat auf einem anderen Computer installiert werden, um eine Remote-Steuerung des Sicherheitsservers zu ermöglichen. In Abhängigkeit von der Serverarchitektur in Ihrem Unternehmen können Sie sich für eine der drei folgenden Installationsvarianten entscheiden:

- Der Sicherheitsserver wird auf demselben Computer installiert wie Microsoft Exchange Server. Auf diesen Computer wird auch die Management-Konsole installiert.
- Der Sicherheitsserver und die Management-Konsole werden auf demselben Computer installiert wie Microsoft Exchange Server. Die Management-Konsole wird auf einem beliebigen Computer im Unternehmensnetzwerk installiert, um eine Remote-Steuerung des Sicherheitsservers zu ermöglichen.
- Der Sicherheitsserver wird auf einem Cluster installiert, auf dem auch Microsoft Exchange Server installiert ist. Bei dieser Variante werden der Sicherheitsserver und die Management-Konsole auf jedem Clusterknoten gemeinsam installiert. Die Management-Konsole wird auf einem beliebigen Computer im Unternehmensnetzwerk installiert, um eine Remote-Steuerung der Sicherheitsserver zu ermöglichen.
- Der Sicherheitsserver wird auf Gruppe des Zugriffs der Datenbanken Microsoft Exchange installiert. Bei dieser Variante werden der Sicherheitsserver und die Management-Konsole gemeinsam auf jedem Server, der sich in diese Gruppe des Zugriffs der Datenbanken befindet, installiert. Die Management-Konsole wird auf einem beliebigen Computer im Unternehmensnetzwerk installiert, um eine Remote-Steuerung der Sicherheitsserver zu ermöglichen.

Nach der Installation von Kaspersky Security müssen Sie einige Dienste von Microsoft Exchange Server neu starten. Der Neustart der Dienste von Microsoft Exchange Server wird automatisch ohne zusätzliche Anfragen durchgeführt.

## IN DIESEM ABSCHNITT

Programminstallation vorbereiten.....	<a href="#">20</a>
Aktualisierung von Vorgängerversionen.....	<a href="#">21</a>
Vorgehen bei der Installation.....	<a href="#">22</a>
Programmbetrieb vorbereiten.....	<a href="#">25</a>
Programm wiederherstellen .....	<a href="#">30</a>
Programm löschen .....	<a href="#">30</a>

## PROGRAMMINSTALLATION VORBEREITEN

Um Kaspersky Security zu installieren, benötigen Sie Rechte als Domain-Administrator. Folgende Komponenten sind außerdem für die Installation unbedingt erforderlich:

- .Net Framework 3.5 SP1;
- Microsoft Management Console 3.0;

Für die ordnungsgemäße Arbeit von Kaspersky Security ist der Exemplare des SQL-Servers Microsoft SQL Server 2005 / 2008 / 2008 R2 (Standard, Express, Enterprise), der auf einem der Netz-PC installiert ist, erforderlich. Es wird zugelassen, den SQL-Server auf einen Computer mit Kaspersky Security festzustellen. Wir empfehlen, für Kaspersky Security einen neu installierten SQL-Server zu verwenden.

Zum Anlegen der SQL-Serverdatenbank benötigen Sie die Anmeldeberechtigung als lokaler Benutzer für den Computer, auf dem Kaspersky Security installiert werden soll, sowie Administratorenrechte für den SQL-Server. Befindet sich der SQL-Server auf dem Domaincontroller, müssen Sie als Mitglied der Administratorengruppe auf Unternehmensebene / Domänebene eingetragen sein.

## AKTUALISIERUNG VON VORGÄNGERVERSIONEN

Kaspersky Security unterstützt die Aktualisierung der Vorgängerversion 8.0 Planmäßiges Update 1 auf die aktuelle Version des Programms. Das Update der früheren Versionen des Programms wird nicht unterstützt.

Es wird empfohlen, das Programmupdate auf Servern, die in der Konfiguration mit DAG arbeiten, in so kurzer Zeit wie möglich auszuführen. Es wird dringend davon abgeraten, eine Verbindung mit diesen Servern über die Management-Konsole aufzubauen und die Programmeinstellungen anzupassen, solange das Update nicht auf allen DAG-Servern abgeschlossen ist. Andernfalls könnte das Update fehlerhaft beendet werden, was zu Unterbrechungen im Programmbetrieb führen kann. Wenn eine Verbindung während des Updates unvermeidlich ist, müssen Sie zunächst sicherstellen, dass die Version des Administrationsservers und die der Administrationskonsole, über die die Verbindung hergestellt wird, identisch sind.

Es wird dringend davon abgeraten, das Programm auf den Servern zu aktualisieren, die im Bestand der SCC- und CCR-Cluster arbeiten, da dies die Migration der Daten aus der alten Version des Programms in die neue wesentlich erschwert. Vor der Installation der aktuellen Version muss die frühere Version des Programms gelöscht werden.

Der SQL-Server, auf dem sich die Datenbank des Programms befindet, muss während der Aktualisierung zugänglich sein. Andernfalls wird die Aktualisierung mit dem Fehler enden.

Die Bedeutungen der Parameter und die Daten der vorhergehenden Version des Programms werden bei der Aktualisierung zur neuen Version auf folgende Weise verlegt:

- Die Gültigkeit der Lizenz für die Vorgängerversion des Programms erstreckt sich auch auf die neue Version. Das Anfangsdatum der Nutzung der Lizenz bleibt ohne Veränderungen erhalten.
- Parameterwerte des Programms, die in der vorhergehenden Version konfiguriert wurden, werden unverändert den entsprechenden Parametern der neuen Programmversion zugewiesen.
- Die Listen der Ausnahmen von der Untersuchung durch Anti-Virus und die "Blacklist" und "Whitelist" der Absender und der Empfänger in Anti-Spam werden in die neue Version übertragen. Die Einträge aus Active Directory, die in die Liste der Anti-Virus-Ausnahmen und in die "Whitelist" der Absender hinzugefügt wurden, werden aber nicht mehr automatisch aktualisiert.
- Die Struktur der Datenbank bei der Aktualisierung des Programms wird auch aktualisiert. Die Daten des Backup-Ordners und der Statistik bleiben erhalten.
- Fertige Berichte werden im Interface der neuen Programmversion nicht dargestellt, aber im Berichtsordner gespeichert (<Ordner zur Programminstallation>/data/statistics/reports).

Beenden Sie vor dem Update die Management-Konsole, wenn sie gestartet war.

Während der Ausführung des Updates vergrößert sich der vom Backup-Ordner eingenommene Speicherplatz (<Installdir>\data) auf das Doppelte. Vor dem Start des Updates müssen Sie sicherstellen, dass genügend freier Speicherplatz für die Unterbringung dieses Ordners vorhanden ist. Nach der Beendigung des Updates verringert sich der Umfang des Backup-Ordners auf den früheren Wert.

➤ Um Kaspersky Security bis zur aktuellen Version zu aktualisieren, erfüllen Sie die folgenden Handlungen:

1. Starten Sie die Installationsdatei (Datei mit Erweiterung exe) der aktuellen Programmversion auf einem Computer mit der installierten Programmversion 8.0 Maintenance Pack 1.
2. Starten Sie das Update des Programms mit einem Klick auf **Kaspersky Security 8.0 für Microsoft Exchange Servers**.
3. Im sich öffnenden Fenster der Begrüßung des Installationsassistenten betätigen Sie die Schaltfläche **Installieren**.  
  
Der Installationsassistent führt das Update automatisch aus.
4. Nach Abschluss der Erneuerung betätigen Sie die Schaltfläche **Fertig**, um das Fenster des Installationsassistenten zu schließen.

## VORGEHEN BEI DER INSTALLATION

Der Installationsvorgang von Kaspersky Security erfolgt mithilfe eines Assistenten, der Sie durch die Installation führt. Mithilfe der Schaltflächen **Zurück** und **Weiter** können Sie während der Installation jederzeit zwischen den einzelnen Fenstern (Schritten) navigieren. Schaltfläche **Abbrechen** dient für den Ausgang aus dem Installationsprogramm.

- Um die Installation von Kaspersky Security zu starten, müssen Sie die Installationsdatei des Programms ausführen (Datei mit Endung exe).

### IN DIESEM ABSCHNITT

Schritt 1. Erforderliche Komponenten installieren .....	<a href="#">22</a>
Schritt 2. Begrüßung und Lizenzvertrag .....	<a href="#">23</a>
Schritt 3. Installationstyp auswählen .....	<a href="#">23</a>
Schritt 4. Programmkomponenten auswählen.....	<a href="#">23</a>
Schritt 5. Verbindung zum Microsoft SQL Server konfigurieren .....	<a href="#">24</a>
Schritt 6. Dateien kopieren .....	<a href="#">25</a>

## SCHRITT 1. ERFORDERLICHE KOMPONENTEN INSTALLIEREN

Überzeugen Sie sich an dieser Stelle, dass auf dem Computer folgende Komponenten installiert sind:

- .Net Framework 3.5 SP1. Sie können diese Komponente erforderlichenfalls über die Schaltfläche **.Net Framework 3.5 SP1 installieren** hinzufügen.

Nach der Installation von .Net Framework 3.5 SP1 müssen Sie den Computer neu starten! Wenn Sie die Installation ohne Neustart fortsetzen, können im Folgenden Funktionsstörungen von Kaspersky Security auftreten.

- Microsoft Management Console 3.0 (MMC 3.0). Microsoft Management Console 3.0 (MMC 3.0) ist Bestandteil des Betriebssystems Microsoft Windows Server 2003 ab R2. Zur Installation des Programms auf eine ältere Version von Microsoft Windows Server müssen Sie die Komponente MMC auf Version 3.0 aktualisieren. Klicken Sie hierzu auf die Schaltfläche **MMC 3,0 installieren**.

Durch Klicken auf den Link **Kaspersky Security 8.0 für Microsoft Exchange Server** gelangen Sie zum nächsten Schritt der Installation.

Über die Schaltfläche **Installationshandbuch** können Sie zusätzlich das Installationshandbuch downloaden und lokal installieren.

## SCHRITT 2. BEGRÜßUNG UND LIZENZVERTRAG

Im Begrüßungsfenster erhalten Sie die Meldung, dass die Installation von Kaspersky Security gestartet wurde. Über die Schaltfläche **Weiter** wechseln Sie zum Anzeigefenster für den Lizenzvertrag.

Der Lizenzvertrag wird zwischen dem Nutzer und Kaspersky Lab abgeschlossen. Mit dem Häkchen **Ich akzeptiere die Bedingungen des Lizenzvertrages** bestätigen Sie, dass Sie den Lizenzvertrag gelesen haben und mit dessen Bedingungen einverstanden sind. Wenn Sie die Bedingung des Lizenzabkommens nicht übernehmen werden, können Sie Kaspersky Security nicht feststellen.

## SCHRITT 3. INSTALLATIONSTYP AUSWÄHLEN

Im Auswahlfenster für den Installationstyp haben Sie zwei Schaltflächen zur Auswahl:

- **Standard.** Klicken Sie auf diese Schaltfläche, werden die Standardkomponenten installiert, die von den Meisten Anwendern üblicherweise verwendet werden. Weiter s. Schritt 5.
- **Benutzerdefiniert.** Klicken Sie auf diese Schaltfläche, können Sie die zu installierenden Komponenten und Programme individuell auswählen. Eine benutzerdefinierte Installation wird nur für erfahrene Anwender empfohlen.

Nachdem Sie den Installationstyp gewählt haben, wechselt der Installationsassistent zum nächsten Schritt.

## SCHRITT 4. PROGRAMMKOMPONENTEN AUSWÄHLEN

Wenn Sie im vorigen Schritt **Benutzerdefiniert** gewählt haben, schlägt Ihnen das Installationsprogramm nun die zu installierenden Komponenten zur Auswahl vor. Je nachdem, ob und für welche Rolle Microsoft Exchange Server auf dem Computer installiert ist, werden unterschiedliche Sets von Komponenten für die Installation vorgeschlagen.

Wenn Microsoft Exchange Server sowohl für die Mailbox Role als auch für die Hub Transport Role installiert ist, werden folgende Komponenten zur Auswahl für die Installation vorgeschlagen:

- Management-Konsole;
- Schutzmodul gegen Spam;
- Antivirus für Mailbox Role;
- Anti-Virus für Hub Transportation Role und Cross-Border Transportation Role.

Wenn Microsoft Exchange Server nur für die Role Hub Transport und Edge Transport installiert ist, werden folgende Komponenten zur Auswahl für die Installation vorgeschlagen:

- Management-Konsole;
- Schutzmodul gegen Spam;
- Anti-Virus für Hub Transportation Role und Cross-Border Transportation Role.

Wenn Microsoft Exchange Server nur für die Mailbox Role installiert ist, zur Auswahl für die Installation vorgeschlagen:

- Management-Konsole;
- Antivirus für Mailbox Role.

In allen anderen Fällen ist nur die Management-Konsole zur Installation verfügbar.

Im unteren Teil des Fensters wird der Weg zum Ordner der Installation als Voreinstellung dargestellt. Um einen anderen Ordner für die Installation zu wählen, klicken Sie auf die Schaltfläche **Durchsuchen**. Niedriger wird der Weg zum Ordner der Datenspeicherung dargestellt. Der Datenspeicherordner enthält folgende Elemente:

- die Antiviren-Datenbanken;
- die Anti-Spam-Datenbanken;
- die in die Quarantäne verschobenen Objekte.

Falls Sie für den Ordner mehr Speicherplatz vorsehen möchten, als auf dem aktuell gewählten Datenträger verfügbar, können Sie über die Schaltfläche **Durchsuchen** einen anderen Pfad für den Speicherordner vorgeben.

Über die Schaltfläche **Verwerfen** können Sie die getroffene Auswahl der Komponenten verwerfen und zur voreingestellten Standardauswahl zurückkehren.

Über die Schaltfläche **Datenträger** können Sie ein Dialogfenster mit Angaben zu vorhandenem Speicherplatz für die Installation auf den lokalen Datenträgern öffnen.

## SCHRITT 5. VERBINDUNG ZUM MICROSOFT SQL SERVER KONFIGURIEREN

An dieser Stelle werden die Parameter für die Verbindung zum Microsoft SQL Server eingerichtet.

### Parameter für die Verbindung zum Microsoft SQL Server anpassen

Geben Sie im Feld **SQL-Servername** den Namen (oder die IP-Adresse) des Computers und der Installation des SQL-Servers ein, z.B. MYCOMPUTER\SQLEXPRESS. Über die Schaltfläche **Durchsuchen**, die diesem Feld gegenüberliegt, können Sie einen SQL-Server im aktuellen Netzwerksegment wählen.

Geben Sie im Feld **Datenbankname** den Namen der Datenbank ein, die zur Speicherung der Backup-Ordner-Daten und der Statistikdaten genutzt wird. Ist die Datenbank mit dem angegebenen Namen auf dem SQL-Server nicht vorhanden, wird sie erstellt.

Wenn Sie die Nutzung eines zentralen Backups sowie der zentralen Speicherung der statistischen Daten mehrerer Sicherheitsserver planen, müssen die Namen des SQL-Servers und der Datenbank für alle Sicherheitsserver übereinstimmen. Wenn kein zentrales Backup vorgesehen ist, kann jeder Sicherheitsserver jeweils eine servereigene Datenbank nutzen.

Wenn Sie Kaspersky Security über einen Cluster oder Microsoft Exchange DAG Server verteilen, ist es dringend empfehlenswert, eine einheitliche Datenbank für alle Sicherheitsserver zu verwenden.

Zum Anlegen der SQL-Serverdatenbank müssen Sie das Benutzerkonto auswählen, über das die SQL-Datenbank angelegt werden soll. Sie haben folgende Auswahlmöglichkeiten:

- **Aktuelles Benutzerkonto.** In diesem Fall wird das Benutzerkonto des aktuellen Benutzers verwendet.
- **Anderes Benutzerkonto.** In diesem Fall werden Benutzerkonto und Passwort eines anderen Benutzers verwendet. Die Auswahl des Benutzerkontos erfolgt über die Schaltfläche **Durchsuchen**.

Sie müssen den Browser des SQL-Servers auf dem Computer starten, auf dem sich der SQL-Server befindet. Ansonsten können Sie die benötigte SQL-Serverinstallation nicht finden. Wird Kaspersky Security auf Edge Transport installiert, und gehört der SQL-Server zur Domain, kann keine Verbindung zum SQL-Server hergestellt werden. In diesem Fall müssen Sie eine lokale SQL-Serverinstallation verwenden.

Zum Anlegen der SQL-Serverdatenbank benötigen Sie die Anmeldeberechtigung als lokaler Benutzer für den Computer, auf dem Kaspersky Security installiert werden soll, sowie Administratorrechte für den SQL-Server. Befindet sich der SQL-Server auf dem Domaincontroller, müssen Sie als Mitglied der Administratorengruppe auf Unternehmensebene / Domänebene eingetragen sein. Für Remoteverbindungen zum SQL-Server müssen Sie die TCP/IP-Unterstützung im SQL Server Configuration Manager aktivieren.

### Benutzerkonto für die Ausführung des Dienstprogramms auswählen

Im nächsten Fenster können Sie das Benutzerkonto auswählen, das für den Start des Programmdienstes und für die Verbindung zum SQL-Server benutzt wird. Sie haben folgende Auswahlmöglichkeiten:

- **Benutzerkonto Local System.** In diesem Fall werden der Programmdienst und die Verbindung mit dem SQL-Server durch das Benutzerkonto des lokalen Systems gestartet.
- **Anderes Benutzerkonto.** In diesem Fall werden der Name und das Passwort des Benutzerkontos angegeben. Die Auswahl des Benutzerkontos erfolgt über die Schaltfläche **Durchsuchen**.

Für die Arbeit mit der aktuellen Datenbank muss das ausgewählte Benutzerkonto über folgende Zugriffsrechte verfügen:

Tabella 2. Zugriffsrechte zur Datenbank

DIE ZU SCHÜTZENDE GRUNDLEGENDE ENTITÄT	ERLAUBNIS	BESCHREIBUNG
DATABASE	CREATE TABLE	Recht auf Hinzufügen von Tabellen in die ausgewählte Datenbank
DATABASE	CREATE XML SCHEMA COLLECTION	Recht auf Erstellung von Sammlungen von XML-Strukturen in der ausgewählten Datenbank
SCHEMA	CONTROL	Recht auf Überprüfung der dbo-Struktur in der ausgewählten Datenbank

Wenn eine neue Datenbank erstellt wird, wird das Programm diese Zugriffsrechte dem ausgewählten Benutzerkonto automatisch zuweisen.

Wenn ein in der Domain eingetragenes Benutzerkonto ausgewählt wurde, ist es notwendig, dieses Benutzerkonto der Domaingruppe Exchange View-Only Administrators hinzuzufügen. Nach dem Hinzufügen muss der Programmdienst auf allen Rechnern, auf denen er im Namen dieses Benutzers ausgeführt wird, neu gestartet werden. Das ist notwendig, damit die in den Domaingruppen vorgenommenen Änderungen wirksam werden.

## SCHRITT 6. DATEIEN KOPIEREN

Um die Installation fortzusetzen, klicken Sie im Fenster für den Installationsassistenten auf die Schaltfläche **Installieren**. Dadurch werden Programmdateien auf den Computer kopiert, Programmkomponenten im System registriert, die SQL-Serverdatenbank angelegt und einige Dienste von Microsoft Exchange Server neu gestartet.

Neuer Start der Dienste Microsoft Exchange Server wird automatisch ohne zusätzliche Anfragen durchgeführt.

## PROGRAMMBETRIEB VORBEREITEN

Nach Abschluss des Kopiervorgangs und der Registrierung der Komponenten im System erscheint im Installationsassistenten die Meldung, dass die Installation des Programms abgeschlossen ist. Über die Schaltfläche **Weiter** im Installationsassistenten wechseln Sie zum Konfigurationsassistenten des Programms. Der Konfigurationsassistent hilft Ihnen, die Update- und Benachrichtigungseinstellungen einzurichten, die Lizenz zu installieren und die ordnungsgemäße Funktion des Programms zu überprüfen. Um den Einrichtungsassistenten zu starten, klicken Sie auf die Schaltfläche **Weiter**.

**IN DIESEM ABSCHNITT**

Hinzufügen des Schlüssels .....	<a href="#">26</a>
Schutz für den Server anpassen .....	<a href="#">26</a>
Aktivieren KSN .....	<a href="#">27</a>
Konfiguration des Proxyservers .....	<a href="#">27</a>
Benachrichtigungen anpassen .....	<a href="#">27</a>
Programmfunktionen überprüfen.....	<a href="#">28</a>

**HINZUFÜGEN DES SCHLÜSSELS**

Im Fenster **Lizenz** des Konfigurationsassistenten können Sie einen Schlüssel hinzufügen, der den Bedingungen der Lizenz zur Verwendung von Kaspersky Security entspricht.

Wenn Sie Kaspersky Security auf DAG der Server Microsoft Exchange installieren, genügt es, den Schlüssel einmal bei der Installation des Programms auf jedem der DAG-Server hinzuzufügen. Im Folgenden findet der Konfigurationsassistent bei der Installation des Programms auf anderen Servern, die zu dieser DAG gehören, den hinzugefügten Schlüssel automatisch. In diesem Fall ist es nicht nötig, Schlüssel auf anderen Servern hinzuzufügen.

➤ *Gehen Sie folgendermaßen vor, um einen Schlüssel hinzuzufügen:*

1. Klicken Sie auf die Schaltfläche **Hinzufügen**.
2. Geben Sie in dem sich öffnenden Fenster im Feld **Dateiname** den Pfad der Schlüsseldatei ein (Dateierweiterung \*.key) und klicken auf **Öffnen**.

Der Schlüssel wird als aktiver Schlüssel hinzugefügt. Der aktive Schlüssel ermöglicht es, Kaspersky Security während des im Schlüssel festgelegten Zeitraums unter den in der Lizenz bestimmten Bedingungen zu nutzen (s. S. [32](#)).

➤ *Um den Schlüssel zu löschen,*

klicken Sie auf die Schaltfläche **Löschen**.

**SCHUTZ FÜR DEN SERVER ANPASSEN**

Im Fenster **Schutzparameter** des Konfigurationsassistenten können Sie die Parameter des Schutzes durch die Anti-Virus- und Anti-Spam-Programme einstellen. Standardmäßig ist der Schutz durch die Anti-Virus- und Anti-Spam-Programme aktiviert.

➤ *Um die Schutzeinstellungen anzupassen, gehen Sie folgendermaßen vor:*

1. Lassen Sie das Häkchen im Feld **Virenschutz aktivieren**, damit der Virenschutz gleich nach dem Programmstart die Arbeit aufnimmt.
2. Lassen Sie das Häkchen im Feld **Spam-Schutz aktivieren**, damit der Spam-Schutz gleich nach dem Programmstart die Arbeit aufnimmt.

Wenn Sie nicht wollen, dass der Virenschutz sowie der Spam-Schutz die Arbeit gleich nach dem Programmstart aufnehmen, entfernen Sie die entsprechenden Häkchen. Sie können den Schutz später über die Management-Konsole aktivieren.

3. Setzen Sie das Häkchen im Feld **Enforced Anti-Spam Updates Service aktivieren**, wenn Sie die Nutzung des Schnell-Update-Service der Anti-Spam-Datenbanken aktivieren wollen. Folgende Bedingungen müssen auch noch befriedigt werden, die für die Funktion von Enforced Anti-Spam Updates Service notwendig sind:
  - eine ständige Internet-Verbindung des Computers, auf dem der Sicherheitsserver installiert ist.
  - ein regelmäßiges Update der Anti-Spam-Datenbanken (empfohlen wird ein Update alle fünf Minuten).
4. Lassen Sie das Häkchen im Feld **Automatisches Datenbank-Update aktivieren**, damit die Anti-Spam- und Anti-Virus-Datenbanken nach dem Programmstart automatisch von den Kaspersky Lab Update-Servern aktualisiert werden.

## AKTIVIEREN KSN

Im Fenster **Einstellungen KSN** des Konfigurationsassistenten können Sie die Nutzung von KSN für Spambearbeitung. Die Nutzung des Services KSN lässt zu, die Reaktion Kaspersky Security auf die neuen Arten der Spams-Mitteilungen zu beschleunigen und, das Niveau der falschen Abnutzungen der Anti-Spam zu minimisieren. Dieses Fenster erscheint, nur wenn Sie für die Installation der Komponenten das Modul des Spam-Schutzes gewählt haben.

Die Nutzung des Services KSN wird unter Bedingungen der speziellen KSN-Vereinbarung erlaubt.

➤ *Um die Nutzung des Services KSN zu aktivieren,*

lesen Sie die KSN-Vereinbarung und setzen Sie das Häkchen **Ich übernehme das KSN-Vereinbarung und ich möchte KSN verwenden**. Um den vollen Text der KSN-Vereinbarung im abgesonderten Fenster zu öffnen, betätigen Sie die Schaltfläche **KSN-Vereinbarung anzeigen**.

## KONFIGURATION DES PROXYSERVERS

Im Fenster **Proxyserver-Einstellungen** des Konfigurationsassistenten können Sie die Einstellungen des Proxyserver konfigurieren. Diese Parameter werden für das Anschließen des Programms zu den Update-Servern bei der Ausführung der Aktualisierung der Datenbanken, sowie für das Anschließen zu den Servern "Kaspersky Lab" bei der Arbeit der äußerlichen Anti-Spam-Services verwendet.

➤ *Um die Parameter des Proxy-Servers zu konfigurieren, erfüllen Sie die folgenden Handlungen:*

1. Damit wurde das Programm an die Server Kaspersky Lab durch den Proxyserver angeschlossen, stellen Sie das Häkchen **Verwenden Proxyserver fest**.
2. Geben Sie die Proxyserver-Adresse im Feld **Proxyserver-Adresse** ein.
3. Wählen Sie im Eingabefeld über die Scroll-down-Liste den gewünschten Proxyserver-Port. Standardmäßig wird Port **8080** verwendet.
4. Um die Authentifizierung für den gewählten Proxyserver zu verwenden, markieren Sie das Kontrollkästchen **Authentifizierung verwenden** und geben Sie in den Feldern **Benutzerkonto** und **Passwort**. Um ein existierendes Benutzerkonto zu wählen, betätigen Sie auf die Schaltfläche
5. Soll der Download von Updates von einem lokalen Server ihres Firmennetzwerkes ohne Verwendung eines Proxyserver erfolgen, markieren Sie das Kontrollkästchen **Keinen Proxyserver für lokale Adressen verwenden**.

## BENACHRICHTIGUNGEN ANPASSEN

Im Fenster **Benachrichtigungseinstellungen** können Sie die Einstellungen für die vom System versandten E-Mail-Benachrichtigungen anpassen. Durch diese Benachrichtigungen werden Sie über sämtliche Programmereignisse unter Kaspersky Security informiert.

➤ *Zum Einrichten der Benachrichtigungseinstellungen gehen Sie wie folgt vor:*

1. Geben Sie im Feld **Webserviceadresse** die Adresse für den verwendeten Webservice zum E-Mail-Versand über Microsoft Exchange Server ein.

Standardmäßig ist dies in Microsoft Exchange Server folgende Adresse:

`https://<Server_name_für_Kunden_zugriff>/ews/exchange.asmx`

2. Geben Sie im Feld **Benutzerkonto** ein beliebiges gewünschtes Benutzerkonto für ein unter Microsoft Exchange Server registriertes Postfach ein.

Klicken Sie hierzu auf die Schaltfläche **Durchsuchen**, oder geben Sie das Benutzerkonto manuell ein.

3. Geben Sie im Feld **Passwort** das Passwort für das gewählte Benutzerkonto ein.
4. Geben Sie im Feld **Adresse Administrator** die Empfängeradresse für Benachrichtigungen ein, z.B., Ihr E-mail.
5. Klicken Sie auf die Schaltfläche **Test**, um eine Testnachricht zu versenden.

Kommt die Testnachricht im gewählten Postfach an, sind die Einstellungen für Benachrichtigungen korrekt.

6. Klicken Sie auf **Weiter**, um das Einrichten der Programmeinstellungen abzuschließen.

7. Klicken Sie im letzten Fenster auf die Schaltfläche **Fertig**, um den Installationsassistenten abzuschließen.

Wenn Sie das Kontrollkästchen **Nach Abschluss des Assistenten Management-Konsole starten** als markiert beibehalten haben, wird automatisch die Management-Konsole gestartet.

## PROGRAMMFUNKTIONEN ÜBERPRÜFEN

Nach Installation und Einrichten von Kaspersky Security sollten Sie die Richtigkeit der gewählten Einstellungen und die ordnungsgemäße Funktion der Anwendung mithilfe des mitgelieferten Testvirus und seiner Modifikationen überprüfen.

Dieser Testvirus wurde vom EICAR-Institut (The European Institute for Computer Anti-Virus Research) speziell zum Überprüfen der Funktion von Virenschutzprogrammen entwickelt. Der Testvirus ist kein Schädlingsprogramm und enthält keine Programmcodes, die Schäden an Ihrem Computer verursachen könnten. Von den meisten Virenschutzprogrammen wird er jedoch als Virus erkannt und eingestuft.

Der Testvirus kann von der offiziellen Homepage des EICAR-Instituts heruntergeladen werden:  
[http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

### Funktion von Anti-Virus überprüfen

➤ *Um eine Nachricht zu versenden, die den Testvirus enthält, gehen Sie wie folgt vor:*

1. Erstellen Sie eine neue E-Mail, die den Testvirus EICAR als Anlage enthält.
2. Versenden Sie diese Nachricht über Microsoft Exchange Server, während Kaspersky Security installiert ist und eine Verbindung zum Sicherheitsserver besteht.
3. Überzeugen Sie sich davon, dass die zugestellte Nachricht keine Viren enthält. Wird für die Mailbox Rolle ein Virus festgestellt, so wird der gelöschte Virus durch eine Textnachricht ersetzt. Wird ein Virus für die Hub Transport Rolle festgestellt, wird in die Überschrift der Nachricht zusätzlich folgendes Präfix hinzugefügt:  
`Malicious object deleted.`

Nach den Ergebnissen der Virusentdeckung wird an die E-Mail-Adresse, die Sie in Benachrichtigungseinstellungen (s. Abschnitt "Benachrichtigungen anpassen" auf S. 27) vom Assistenten zur eingegeben haben, eine Mitteilung über ein entdecktes Virus gesendet.

➤ *Um der Bericht zu Virenfunden im Programm anzuzeigen, gehen Sie wie folgt vor:*

1. Starten Sie Kaspersky Security über **Start** → **Programme** → **Kaspersky Security 8.0 für Microsoft Exchange Server** → **Management-Konsole**.
2. Klappen Sie links im Konsolenbaum den Node für den Server auf, über den die infizierte E-Mail versandt wurde.
3. Wählen Sie den Node **Berichte**.
4. Setzen Sie im Detailfenster im Einstellungsblock **Schnelle Berichte** gehen Sie wie folgt vor:
  - a. In der Liste **Typ** wählen Sie den gewünschten Bericht **Anti-Virus für Mailbox Role** oder **Anti-Virus für Hub Transport Role** (abhängig von installierter Konfiguration).
  - b. Betätigen Sie die Schaltfläche **Bericht erstellen**.
5. Im Einstellungsblock **Fertige Berichte** können Sie den neu erstellten Bericht einsehen. Hierzu öffnen Sie das gewünschte Bericht per Doppelklick.

Enthält der Bericht die Information, dass der Virus EICAR gefunden wurde, sind die Programmeinstellungen korrekt eingerichtet.

➤ *Um die Berichte automatisch an eine bestimmte E-Mail-Adresse zu versenden, gehen Sie wie folgt vor:*

1. Setzen Sie im Detailfenster im Einstellungsblock **Detaillierter Anti-Virus-Bericht für das Postfach** und **Anti-Virus-Bericht für Hub Transport Role** das Häkchen bei **Administrator**. Der Versand erfolgt an die Adresse, welche Sie unter Benachrichtigungseinstellungen (s. Abschnitt "Benachrichtigungen anpassen" auf S. 27) des Einrichtungsassistenten angegeben haben.

Falls Sie keine E-Mail-Adresse im Konfigurationsassistenten eingegeben haben, können Sie diese unter dem Link **Einstellungen für den E-Mail-Versand** anpassen (s. Abschnitt "Benachrichtigungen anpassen" auf S. 27).

2. Um sicherzugehen, dass die Berichte tatsächlich an die gewünschte Adresse versandt werden, klicken Sie auf die Schaltfläche **Test** zum Versand einer Testnachricht.

Standardmäßig wird eine Kopie des Infizierten Objektes im Backup-Ordner gespeichert.


➤ *Um zu überprüfen, ob tatsächlich eine Kopie des infizierten Objektes im Backup-Ordner gespeichert wurde, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Node **Backup**.
2. Überzeugen Sie sich davon, dass das infizierte Objekt (E-Mail mit dem Virus als Anhang) im Detailfenster angezeigt wird.

### Funktionsprüfung für Anti-Spam

➤ *Um die Korrektheit der Arbeit von der Anti-Spam Komponente zu überprüfen, gehen Sie folgendermaßen vor:*

1. Starten Sie Kaspersky Security über **Start** → **Programme** → **Kaspersky Security 8.0 für Microsoft Exchange Server** → **Management-Konsole**.
2. Klappen Sie links im Konsolenbaum den Node für den Server auf, über den die Testnachricht versandt werden soll.
3. Wählen Sie den Node **Serverschutz**.
4. Wählen Sie im Detailfenster die Registerkarte **Schutz für Hub Transport Role**.
5. Öffnen Sie den Block **Einstellungen der "Whitelist" und "Blacklist"**.

6. Setzen Sie das Häkchen **Absenderadresse in Blacklist übernehmen**.
7. Geben Sie in der Eingabezeile die Adresse E-Mail eines beliebigen Briefkastens, zu der Sie den Zugang haben, ein.
8. Klicken Sie auf die Schaltfläche Hinzufügen  rechts neben dem Feld.
9. Klappen Sie die Gruppe **Untersuchungseinstellungen** auf.
10. Wählen Sie im Feld **In "Blacklist" enthalten** den Wert **Überspringen**.
11. Aktivieren Sie im selben Feld das Kontrollkästchen **Kennzeichen hinzufügen**.
12. Senden Sie eine Nachricht aus gezeigtem Postfach an die E-Mail-Adresse des Administrators über einen geschützten E-Mail-Server.

Enthält diese Nachricht im Eingang das Kennzeichen **[Blacklisted]** in der Überschrift, funktioniert Anti-Spam ordnungsgemäß.

## PROGRAMM WIEDERHERSTELLEN

Treten im laufenden Betrieb Funktionsstörungen (z.B. mit ausgeführten Programmdateien) auf, kann das Problem durch die Wiederherstellung eventuell gelöst werden. Hierbei werden die gewählten Programmeinstellungen und die benutzerdefinierte Konfiguration einschließlich Benachrichtigungen, Pfad für den Quarantäneordner usw. durch das Installationsprogramm gespeichert.

➤ *Um Kaspersky Security wiederherzustellen, gehen Sie wie folgt vor:*

1. Starten Sie die Datei setup\_de.exe.
2. Starten Sie den Installationsassistenten über den Link **Kaspersky Security 8.0 für Microsoft Exchange Servers** und klicken Sie auf die Schaltfläche **Weiter**.
3. Klicken Sie im Begrüßungsfenster des Installationsassistenten auf die Schaltfläche **Weiter**.
4. Klicken Sie im Fenster **Programm ändern, wiederherstellen oder löschen** auf die Schaltfläche **Wiederherstellen**.
5. Klicken Sie im Fenster **Wiederherstellen** auf die Schaltfläche **Reparieren**.

Falls die Konfigurationsdateien beschädigt sind, kann das Programm nicht wiederhergestellt werden. In diesem Fall empfehlen wir, das Programm zu löschen und neu zu installieren.

## PROGRAMM LÖSCHEN

➤ *Um Kaspersky Security von Ihrem Computer zu löschen, gehen Sie wie folgt vor:*

1. Starten Sie die Datei setup\_de.exe.
2. Starten Sie den Installationsassistenten über den Link **Kaspersky Security 8.0 für Microsoft Exchange Servers** und klicken Sie auf die Schaltfläche **Weiter**.
3. Klicken Sie im Fenster **Programm ändern, wiederherstellen oder löschen** auf die Schaltfläche **Löschen**.
4. Klicken Sie im Fenster **Löschen** auf die Schaltfläche **Löschen**.

5. Im Fenster **Datenbank löschen** gehen Sie wie folgt vor:

- Wenn Sie möchten, dass die Datenbank vom SQL-Server bei der Entfernung des Programms gelöscht ist, klicken Sie auf die Schaltfläche **Ja**.
- Wenn Sie möchten nicht, dass die Datenbank vom SQL-Server bei der Entfernung des Programms gelöscht ist, klicken Sie auf die Schaltfläche **Nein**. Aus der Datenbank werden die Daten des Backup-Ordners, die vom Programm beigefügt sind, gelöscht sein. Die statistische Daten, die vom Programm beigefügt sind, werden nicht gelöscht.

Ebenso können Sie das Programm aber auch über die Standardfunktionen zum Installieren und Deinstallieren von Programmen unter Microsoft Windows entfernen.

Während des Löschens von Kaspersky Security müssen einige Dienstprogramme von Microsoft Exchange Server neu gestartet werden. Neuer Start der Dienste Microsoft Exchange Server wird automatisch ohne zusätzliche Anfragen durchgeführt.

# LIZENZIERUNG DES PROGRAMMS

Dieser Abschnitt informiert über die Grundlagen der Programmlizenzierung: Lizenzvereinbarung, Lizenztypen, Schlüsseldateien und Verlängerung der Gültigkeitsdauer der Lizenz. In diesem Abschnitt finden Sie ebenso Anleitungen zur Verwendung von Schlüsseln, zur Einrichtung von Benachrichtigungen über den Ablauf der Lizenz und zum Erstellen einer Liste geschützter E-Mail-Postfächer und Backups.

## IN DIESEM ABSCHNITT

Über den Lizenzvertrag .....	<a href="#">32</a>
Über die Lizenz .....	<a href="#">32</a>
Über die Schlüsseldatei.....	<a href="#">33</a>
Über Schlüssel .....	<a href="#">33</a>
Anzeigen von Informationen zu hinzugefügten Schlüsseln .....	<a href="#">34</a>
Hinzufügen des Schlüssels .....	<a href="#">35</a>
Löschen des Schlüssels .....	<a href="#">35</a>
Warnmeldung bei Ablauf der Lizenz .....	<a href="#">36</a>
Liste geschützter Postfächer und Verzeichnisse anlegen .....	<a href="#">36</a>

## ÜBER DEN LIZENZVERTRAG

Der Lizenzvertrag ist ein rechtsgültiger Vertrag zwischen Ihnen und Kaspersky Lab ZAO. Er bestimmt die Nutzungsbedingungen für das Programm.

**Lesen Sie den Lizenzvertrag sorgfältig, bevor Sie beginnen, mit dem Programm zu arbeiten.**

Die Bedingungen des Lizenzvertrags können Sie während der Installation des Kaspersky-Lab-Programms einsehen.

Wenn Sie bei der Programminstallation den Lizenzbedingungen zustimmen, gilt Ihr Einverständnis mit den Lizenzbedingungen als erteilt. Falls Sie dem Lizenzvertrag nicht zustimmen, müssen Sie die Programminstallation abbrechen.

## ÜBER DIE LIZENZ

Eine *Lizenz* begründet ein zeitlich begrenztes Nutzungsrecht für ein Programm, das Ihnen auf Basis eines Lizenzvertrags überlassen wird.

Die Lizenz enthält die Berechtigung zur Nutzung folgender Leistungen:

- Verwendung des Programms zum Schutz einer bestimmten Anzahl von E-Mail-Postfächern
- Kontaktaufnahme mit dem Technischen Support von Kaspersky Lab
- Nutzung sonstiger von Kaspersky Lab oder den Vertriebspartnern angebotenen Leistungen während der Gültigkeitsdauer der Lizenz

Der Umfang der verfügbaren Leistungen und die Nutzungsdauer für das Programm sind vom Lizenztyp abhängig.

Es sind folgende Lizenztypen vorgesehen:

- *Testlizenz* – kostenlose Lizenz zum Testen des Programms.

Eine Testlizenz hat üblicherweise nur eine kurze Gültigkeitsdauer. Nach Ablauf der Testlizenz stellt Kaspersky Security alle Funktionen ein. Es muss eine kommerzielle Lizenz gekauft werden, um das Programm weiterhin zu verwenden.

- *Kommerzielle Lizenz* – kostenpflichtige Lizenz mit beschränkter Gültigkeitsdauer, die beim Kauf zusammen mit dem Programm erworben wird.

Nach Ablauf der kommerziellen Lizenz funktioniert das Programm auch weiterhin, jedoch lediglich mit eingeschränktem Funktionsumfang. Sie können weiterhin alle Programmkomponenten verwenden, allerdings nur mit den Datenbanken, die beim Ablauf der Lizenz installiert waren. Um Kaspersky Security weiterhin mit der vollen Funktionalität zu verwenden, muss die kommerzielle Lizenz verlängert werden.

Es wird empfohlen, die Gültigkeitsdauer einer Lizenz spätestens dann zu verlängern, wenn die aktive Lizenz abläuft. Nur so lässt sich ein optimaler Antiviren- und Spam-Schutz für Ihren Computer gewährleisten.

## ÜBER DIE SCHLÜSSELDATEI

Die *Schlüsseldatei* ist eine Datei des Typs „xxxxxxx.key“. Sie können das Programm nur bei Vorhandensein von der Schlüsseldatei verwenden. Die Schlüsseldatei enthält einen Schlüssel, mit dessen Hilfe die Bedingungen der gültigen Lizenz realisiert werden.

Die Schlüsseldatei enthält folgende Informationen:

- Schlüssel – eine einzigartige Folge von Buchstaben und Ziffern. Der Schlüssel wird, beispielsweise, für den Erhalt von technischer Unterstützung durch Kaspersky Lab verwendet.
- Einschränkung – die maximale Anzahl der Postfächer, die das Programm mit diesem Schlüssel schützen kann.
- Erstellungsdatum der Schlüsseldatei.
- Gültigkeitsdauer der Lizenz – die Gültigkeitsdauer des Programms, die im Lizenzvertrag genannt wird und die mit der Hinzufügung dieses Schlüssels in der Programmoberfläche beginnt. Beispielsweise 1 Jahr.

**Die Gültigkeitsdauer der Lizenz endet nicht später als die Gültigkeitsdauer der Schlüsseldatei, mit der das Programm gemäß der aktuellen Lizenz aktiviert wurde.**

- Gültigkeitsdauer der Schlüsseldatei – bestimmter Zeitraum ab Erstellung der Schlüsseldatei. Die Gültigkeitsdauer der Datei kann mehrere Jahre betragen. Die Verwendung des Programms mithilfe dieser Schlüsseldatei ist nur innerhalb dieses Zeitraums möglich.

## ÜBER SCHLÜSSEL

Der Schlüssel ist eine individuelle Abfolge von Buchstaben und Ziffern, mit deren Hilfe die Lizenzbedingungen realisiert werden. Schlüssel sowie zusätzliche Schlüsselinformationen werden in Schlüsseldateien gespeichert.

Um das Programm verwenden zu können, müssen Sie den Schlüssel in der Programmoberfläche hinzufügen.

**Kaspersky Security funktioniert nicht ohne Schlüssel!**

Man unterscheidet zwischen dem aktiven und dem Reserveschlüssel.

## Aktiver Schlüssel

Der Schlüssel, mit dessen Hilfe die Bedingungen der gültigen Lizenz realisiert werden, wird aktiv genannt. Als aktiver Schlüssel kann der Schlüssel einer Testlizenz oder einer kommerziellen Lizenz hinzugefügt werden.

In jedem Schlüssel ist eine Beschränkung der Zahl der geschützten Postfächer installiert. Die Anzahl von geschützten E-Mail-Postfächern kann man durch Ausnahme der Überprüfung (s. Abschnitt "Liste geschützter Postfächer und Verzeichnisse anlegen" auf S. 36), Postfächer die nicht überprüft werden sollen, einstellen. Wir empfehlen Ihnen, einen Schlüssel für sämtliche Postfächer zu erwerben, da sich durch nicht geschützte Postfächer die Gefahr des Eindringens von Viren über E-Mail deutlich erhöht.

Standardmäßig beginnt das Programm 15 Tage vor Ablauf der Gültigkeitsdauer der Lizenz, entsprechende Warnmeldungen zu versenden. Diese Meldungen enthalten das Ablaufdatum der aktuellen Lizenz und informieren Sie über die Möglichkeiten, die Lizenz zu verlängern. Sie können auch die Frist der Benachrichtigungserhaltung ändern (s. Abschnitt "Warnmeldung bei Ablauf der Lizenz" auf S. 36) sowie die E-Mail-Adresse eingeben, an die die Benachrichtigung gesendet wird.

## Reservelizenz

Wenn Sie keinen Schlüssel für die kommerzielle Lizenz hinzugefügt haben, können Sie einen Reserveschlüssel hinzufügen. Nach Ablauf der Gültigkeit der Lizenz, die vom aktiven Schlüssel gewährt wurde, wird der Reserveschlüssel automatisch zum aktiven Schlüssel. Dadurch wird der permanente Virenschutz für die E-Mail Server Ihres Unternehmens gewährleistet. Über die Oberfläche von Kaspersky Security kann nur ein Reserveschlüssel hinzugefügt werden.

Der Schlüssel einer Testlizenz kann nicht als Reserveschlüssel verwendet werden.

## Lizenzierungsschemen

Je nachdem, welche Variante für die Programminstallation verwendet wurde, müssen Sie die Schlüssel gemäß den Lizenzierungsschemen hinzufügen:

- Wenn das Programm auf einzelnen Servern von Microsoft Exchange Server verwendet wird, muss auf jedem Server ein separater Schlüssel hinzugefügt werden.
- Wenn das Programm auf einem Server-Cluster von Microsoft Exchange Server verwendet wird, genügt die Installation eines einzigen Schlüssels, der sich auf den gesamten Cluster erstreckt.
- Wenn das Programm auf DAG-Servern von Microsoft Exchange Server verwendet wird, genügt es, einen einzigen Schlüssel zu installieren, der sich auf die gesamte DAG erstreckt.

# ANZEIGEN VON INFORMATIONEN ZU HINZUGEFÜGTEN SCHLÜSSELN

➤ *Gehen Sie folgendermaßen vor, um Informationen zu den hinzugefügten Schlüsseln anzuzeigen:*

1. Starten Sie die Management-Konsole.
2. Wählen Sie im Konsolenbaum auf dem gewünschten Serverknoten den Knoten **Lizenzierung**.

Im Ergebnisfenster werden Informationen zu den hinzugefügten Schlüsseln angezeigt. Es werden folgende Informationen angezeigt:

- **Lizenztyp.** Lizenztyp (Test, kommerziell).
- **Vertreter des Nutzers.** Die Person oder das Unternehmen, auf deren Namen die Lizenz ausgestellt ist.
- **Beschränkungen.** Die Zahl der Postfächer, auf die die Lizenz ausgestellt ist.

- **Ablaufdatum.** Ablauffrist für die Gültigkeit der Lizenz.
- **Schlüssel.** Individuelle Abfolge von Buchstaben und Ziffern.
- **Status.** Lizenzstatus.

## HINZUFÜGEN DES SCHLÜSSELS

Wenn Kaspersky Security in der Konfiguration mit DAG arbeitet, genügt es, einen Schlüssel für die gesamte DAG hinzuzufügen. Sie können den Schlüssel hinzufügen, indem Sie die Management-Konsole mit einem beliebigen Server dieser DAG verbinden.

➔ *Gehen Sie folgendermaßen vor, um einen Schlüssel hinzuzufügen:*

1. Wählen Sie in der Management-Konsole den Node **Lizenzierung**.
2. Klicken Sie im Ergebnisbereich im Block **Aktiver Schlüssel** auf die Schaltfläche **Hinzufügen**.
3. Geben Sie in dem sich öffnenden Fenster im Feld **Dateiname** den Pfad der Schlüsseldatei ein (Dateierweiterung \*.key) und klicken auf **Öffnen**.

Der Schlüssel wird als aktiver Schlüssel hinzugefügt. Die Informationen über den Schlüssel werden im Block **Aktiver Schlüssel** angezeigt.

Nachdem Sie den aktiven Schlüssel hinzugefügt haben, können Sie den Reserveschlüssel hinzufügen. Als Reserveschlüssel kann nur ein Schlüssel der kommerziellen Lizenz hinzugefügt werden. Der Schlüssel einer Testlizenz kann nicht als Reserveschlüssel verwendet werden.

➔ *Um den Reserveschlüssel hinzuzufügen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Management-Konsole den Node **Lizenzierung**.
2. Klicken Sie im Ergebnisbereich im Block **Reserveschlüssel** auf die Schaltfläche **Hinzufügen**.
3. Geben Sie in dem sich öffnenden Fenster im Feld **Dateiname** den Pfad der Schlüsseldatei ein (Dateierweiterung \*.key) und klicken auf **Öffnen**.

Der Schlüssel wird als Reserveschlüssel hinzugefügt. Die Informationen über den Schlüssel werden im Block **Reserveschlüssel** angezeigt.

## LÖSCHEN DES SCHLÜSSELS

➔ *Gehen Sie folgendermaßen vor, um den Reserveschlüssel zu löschen:*

1. Wählen Sie in der Management-Konsole den Node **Lizenzierung**.
2. Erfüllen Sie eine der folgenden Aktionen:
  - Wenn Sie den aktiven Schlüssel löschen möchten, betätigen Sie die Schaltfläche **Löschen** im Block **Aktiver Schlüssel**.
  - Wenn Sie den Reserveschlüssel löschen möchten, betätigen Sie die Schaltfläche **Löschen** im Block **Reserveschlüssel**.

Der gewählte Schlüssel wird gelöscht. Wenn der aktive Schlüssel gelöscht wird, wird der (evtl. vorhandene) Reserveschlüssel zum aktiven Schlüssel.

## WARNMELDUNG BEI ABLAUF DER LIZENZ

Nach jedem Update der Datenbanken prüft das Programm die aktuelle Lizenz. Wenn das Programm feststellt, dass die Gültigkeitsdauer der Lizenz bald abläuft, wird ein entsprechender Eintrag im Programmjournal gemacht und es werden Benachrichtigungen an die E-Mail-Adressen versendet, die in den Benachrichtigungseinstellungen angegeben sind (s. Abschnitt "Benachrichtigungseinstellungen anpassen" auf S. 84). Standardmäßig erfolgt die Benachrichtigung 15 Tage vor Ablauf der Gültigkeit der Lizenz. Sie können einen früheren oder einen späteren Zeitpunkt für die Benachrichtigung einstellen.

➤ *Gehen Sie folgendermaßen vor, um die Benachrichtigung zum Ablauf der Lizenz für Kaspersky Security einzurichten:*

1. Wählen Sie in der Management-Konsole den Node **Lizenzen**.
2. Wählen Sie im Detailfenster für den Parameter **Bei Ablauf der Lizenz benachrichtigen** im Eingabefeld mit der Scrollbox, wie viele Tage vorher die Benachrichtigung zum Ablauf der Lizenz an Sie versandt werden soll.
3. Klicken Sie auf die Schaltfläche **Speichern**.

## LISTE GESCHÜTZTER POSTFÄCHER UND VERZEICHNISSE ANLEGEN

Das Programm schützt maximal die im aktiven Schlüssel angegebene genannte Anzahl von E-Mail-Postfächern. Wenn diese Zahl ungenügend ist, können Sie den Schutz beim Teil der Postfächer abnehmen. Dazu können Sie die Postfächer, bei denen Sie den Schutz abnehmen wollen, in die Aufbewahrungsorte verlegen, die sich nicht verteidigen werden. Sind die Standardeinstellungen gewählt, werden auch sämtliche öffentliche Ordner auf dem E-Mail-Server geschützt. Sie können für öffentliche Ordner den Schutz deaktivieren, wenn diese Ihrer Meinung nach nicht geprüft werden müssen.

➤ *Gehen Sie folgendermaßen vor, um eine Liste der geschützten Postfächer und Backups zu erstellen:*

1. Wählen Sie in der Management-Konsole den Node **Serverschutz**.
2. Öffnen Sie in der Registerkarte **Schutz für Mailbox Role** den Einstellungsblock **Postfächer schützen**.
3. Markieren Sie im Abschnitt **Geschützte Speicherverzeichnisse** für E-Mail-Postfächer die Verzeichnisse für Postfächer, welche geschützt werden sollen.
4. Markieren Sie im Abschnitt **Geschützte Verzeichnisse für öffentliche Ordner** die Verzeichnisse für öffentliche Ordner, welche geschützt werden sollen.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu übernehmen.

In den Listen werden Ihnen sämtliche Verzeichnisse für Postfächer und öffentliche Ordner unter Microsoft Exchange angezeigt. Werden die Standardeinstellungen verwendet, sind sämtliche Verzeichnisse für Postfächer und öffentliche Ordner geschützt, die zum Zeitpunkt der Installation des Programms bereits vorhanden waren oder später hinzugefügt wurden.

# PROGRAMMOBERFLÄCHE

Die Management-Konsole enthält die Oberfläche zur Programmverwaltung. Die Benutzeroberfläche ist ein spezielles, separates Tool und Bestandteil der MMC.

## IN DIESEM ABSCHNITT

---

Hauptfenster.....	<a href="#">37</a>
Kontextmenü.....	<a href="#">39</a>

## HAUPTFENSTER

Das Hauptfenster der Management-Konsole ist in folgende Bereiche unterteilt (s. Abb. unten):

- **Werkzeugleiste.** Im oberen Bereich des Hauptfensters. Über die Schaltflächen der Werkzeugleiste können Sie einige der am häufigsten verwendeten Programmfunktionen direkt aufrufen.
- **Menü.** Über der Werkzeugleiste. Über das Menü können Sie zwischen Fenstern und Dateien navigieren und die Hilfe aufrufen.
- **Konsolenbaum.** Im linken Bereich des Hauptfensters. Im Konsolenbaum können Sie die verbundenen Sicherheitsserver und die gesetzten Einstellungen für Kaspersky Security einsehen. Die verbundenen Sicherheitsserver und die gesetzten Einstellungen für Kaspersky Security werden als Nodes angezeigt. Übergeordnete Nodes können Sie durch einen Klick auf das Symbol "Plus" expandieren. Beim Expandieren des Nodes wird das Plus- zum Minuszeichen.

- **Detailfenster.** Im rechten Bereich des Hauptfensters. Zeigt den Inhalt des gewählten Nodes an.

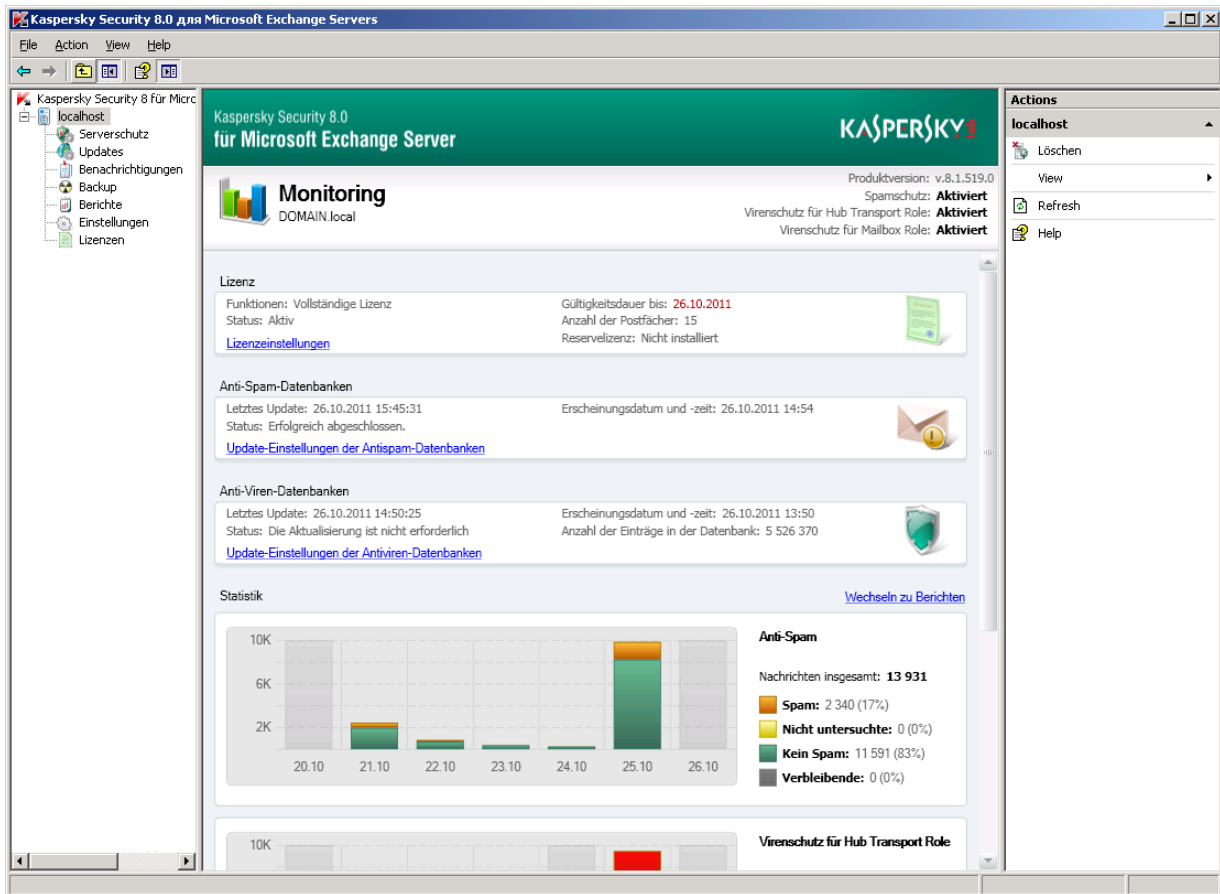


Abbildung 1. Programmhauptfenster

Der oberste Knoten im Konsolenbaum ist **Kaspersky Security 8.0 für Microsoft Exchange Server**. Durch Doppelklick auf diesen Node können Sie im Konsolenbaum die Gesamtliste der Server öffnen, auf denen Kaspersky Security installiert ist. Im Detailfenster werden außerdem die verbundenen Server und die Schaltfläche **Server hinzufügen** angezeigt.

Wenn Sie mit der linken Maustaste auf den Node für einen der angeschlossenen Server klicken, werden im Detailfenster die allgemeine Information angezeigt:

- Die Liste und der Status der Komponenten des Programms, die auf dem gewählten Server installiert sind.
- Die Informationen über die installierte Lizenz.
- Der Update-Status der Datenbanken des Anti-Virus und der Anti-Spam.
- Die Zeitpläne, die die statistischen Informationen über die Arbeit der Anti-Spams und den Anti-Virus darstellen.

Auf den Druck auf das Plus-Zeichen gegenüber dem angeschlossenen Server, im Baum der Konsole wird die Liste der angelegten Knoten, die die Parameter und die Elemente der Steuerung der Funktionen Kaspersky Security enthalten, geöffnet. Die angelegten Knoten Kaspersky Security sind für die Ausführung der folgenden Aktionen vorbestimmt:

- **Serverschutz** – Einstellungen für Anti-Viren- und Spamschutz anzeigen und anpassen.
- **Updates** – Einstellungen für Updates der Anti-Viren- und Anti-Spam-Datenbanken anzeigen und anpassen.
- **Benachrichtigungen** – Einstellungen der E-Mail-Benachrichtigungen anzeigen und anpassen.

- **Backup-Ordner** – die Durchsicht des Backup-Ordners, die Sendung und das Löschen der Objekte aus dem Backup-Ordner.
- **Berichte** – Berichtseinstellungen von Anti-Virus und Anti-Spam anzeigen und anpassen.
- **Konfiguration** – Einstellungen für den Versand von Benachrichtigungen, Backup-Ordner, Diagnosefunktionen, Berichte und Statistik anzeigen und anpassen.
- **Lizenzen** – Lizenzen installieren und löschen, Informationen zu aktuell installierten Lizenzen und Reservelizenz anzeigen.

Wenn Sie einen Programmknoten im Konsolenbaum markieren, werden im Detailfenster die Einstellungen für den Node angezeigt, welche angepasst werden können.

## KONTEXTMENÜ

Jede Gruppe von Objekten im Konsolenbaum hat ein eigenes Kontextmenü, das Sie durch einen Klick mit der rechten Maustaste aufrufen können. Dieses enthält außer den Standard-Menübefehlen der MMC auch Befehle zur Arbeit mit dem gewählten Objekt. Über das Kontextmenü können Sie folgende Aktionen aufrufen:

- Server hinzufügen. Wählen Sie im Konsolenbaum den Node **Kaspersky Security 8.0 für Microsoft Exchange Servers** und klicken Sie mit der rechten Maustaste. Wählen Sie im Kontextmenü den Punkt **Server hinzufügen**.
- Tooldiagnose aktivieren. Wählen Sie im Konsolenbaum den Node **Kaspersky Security 8.0 für Microsoft Exchange Servers** und klicken Sie mit der rechten Maustaste. Wählen Sie im Kontextmenü den Punkt **Tooldiagnose aktivieren**.
- Verbundene Server löschen. Im Baum der Management-Konsole wählen Sie den Knoten des angeschlossenen Servers und drücken Sie darauf mit der rechten Maustaste. Wählen Sie im Kontextmenü den Punkt **Löschen**.
- Anti-Viren- und Anti-Spam-Datenbanken aktualisieren. Im Baum der Management-Konsole wählen Sie den Node **Updates** und drücken Sie darauf mit der rechten Maustaste. Wählen Sie im Kontextmenü den Punkt **Anti-Viren-Datenbanken aktualisieren** bzw. **Anti-Spam-Datenbanken aktualisieren**.
- Versandeinstellungen für Benachrichtigungen anpassen. Im Baum der Management-Konsole wählen Sie den Node **Meldungen** oder **Berichte** und drücken Sie darauf mit der rechten Maustaste. Wählen Sie im Kontextmenü den Punkt **Einstellungen für den E-Mail-Versand**.

# PROGRAMM STARTEN UND ANHALTEN

Kaspersky Security wird automatisch bei Start des Microsoft Exchange Servers oder Microsoft Windows, beim Durchlauf von E-Mails auf dem Microsoft Exchange-Server und beim Verbinden der Management-Konsole mit dem Sicherheitsserver mit gestartet. Ist der Schutz für den Server aktiviert, schaltet er sich sofort nach dem Start von Microsoft Exchange Server ein.

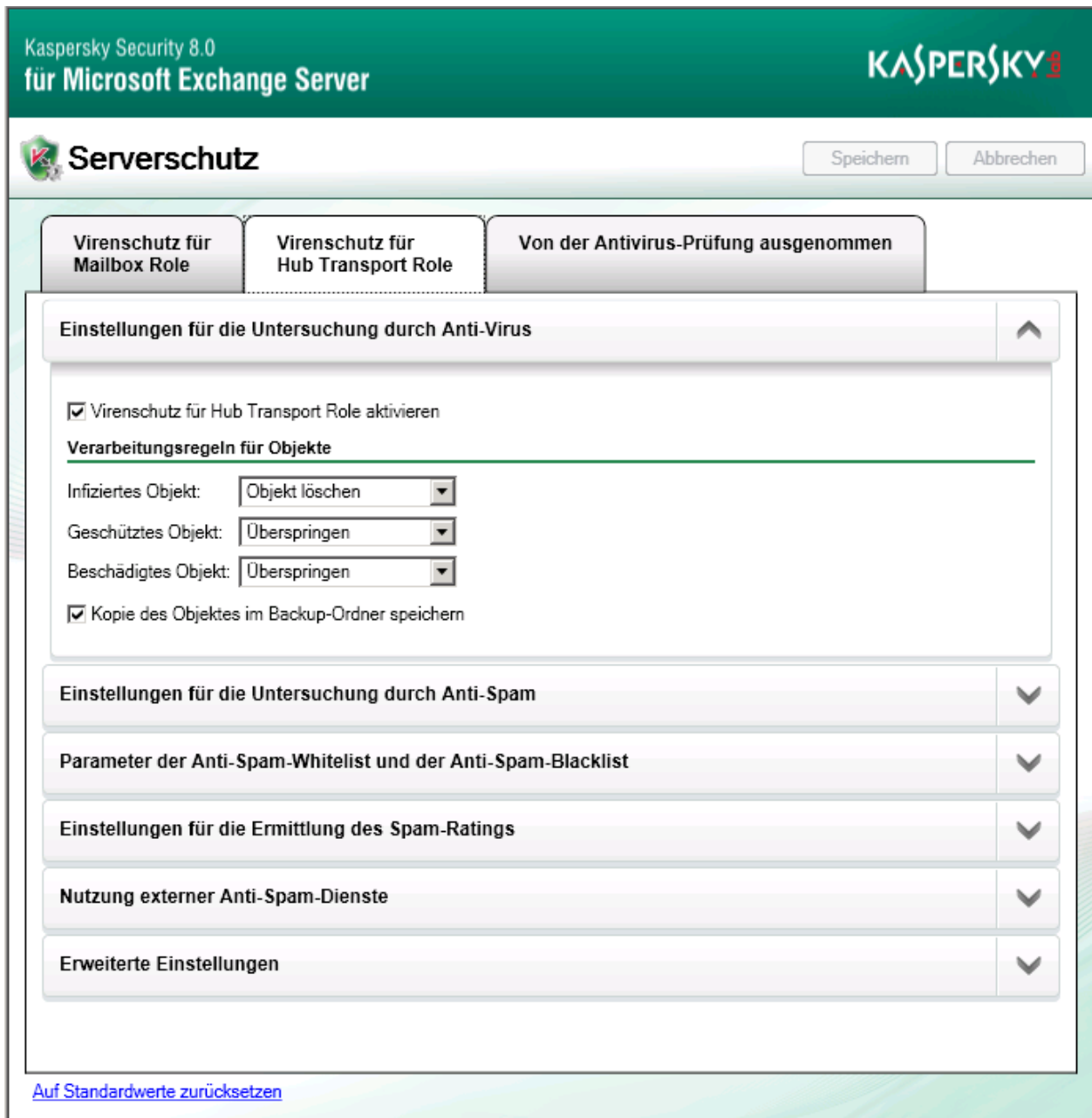


Abbildung 2. Serverschutz aktivieren

Sie können den Viren- und Spamschutz auf Hub Transport Rolle oder Mailbox Rolle abgesondert schalten und abschalten.

- *Um den Virenschutz für Mailbox Rolle einen angeschlossenen Microsoft Exchange-Server zu aktivieren, gehen Sie wie folgt vor:*
  1. Starten Sie Kaspersky Security über **Start → Programme → Kaspersky Security 8.0 für Microsoft Exchange Server → Management-Konsole**.
  2. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
  3. Wählen Sie den Node **Serverschutz**.
  4. Öffnen Sie in der Registerkarte **Virenschutz für Mailbox Role** im Einstellungsblock **Untersuchungseinstellungen von Anti-Virus** setzen Sie das Häkchen **Virenschutz für Mailbox Role aktivieren**.
  5. Klicken Sie auf die Schaltfläche **Speichern**.
- *Um den Virenschutz für Hub Transport Rolle einen angeschlossenen Microsoft Exchange-Server zu aktivieren, gehen Sie wie folgt vor:*
  1. Starten Sie Kaspersky Security über **Start → Programme → Kaspersky Security 8.0 für Microsoft Exchange Server → Management-Konsole**.
  2. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
  3. Wählen Sie den Node **Serverschutz**.
  4. Öffnen Sie in der Registerkarte **Virenschutz für Hub Transporter Role** im Einstellungsblock **Untersuchungseinstellungen von Anti-Virus** setzen Sie das Häkchen **Virenschutz für Hub Transporter Role aktivieren**.
  5. Klicken Sie auf die Schaltfläche **Speichern**.
- *Um den Spamschutz für einen angeschlossenen Microsoft Exchange-Server zu aktivieren, gehen Sie wie folgt vor:*
  1. Starten Sie Kaspersky Security über **Start → Programme → Kaspersky Security 8.0 für Microsoft Exchange Server → Management-Konsole**.
  2. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
  3. Wählen Sie den Node **Serverschutz**.
  4. Öffnen Sie in der Registerkarte **Virenschutz für Hub Transporter Role** den Bereich **Untersuchungseinstellungen von Anti-Spam**.
  5. Setzen Sie das Häkchen **Nachrichten auf Spam überprüfen**.
  6. Klicken Sie auf die Schaltfläche **Speichern**.
- *Zum Anhalten von Kaspersky Security, gehen Sie folgendermaßen vor:*
  1. Deaktivieren Sie den Viren- und Spamschutz über die Management-Konsole (s. oben).
  2. **Stoppen Sie den Dienst** von Kaspersky Security und stellen Sie als Autostarttyp – Deaktiviert ein.
- *Um das Programm nach Deaktivierung der Autostart-Option für Kaspersky Security erneut zu starten:*
  1. Überzeugen Sie sich davon, dass für Kaspersky Security der Autostarttyp – **Automatisch** eingestellt ist.
  2. Aktivieren Sie den Anti-Viren- und Anti-Spamschutz über die Management-Konsole (s. oben).

# SCHUTZSTATUS DES SERVERS

Dieser Abschnitt informiert darüber, wie Sie mithilfe der Administrationskonsole Informationen über den Zustand der Programmkomponenten, der Antiviren- und Anti-Spam-Datenbanken sowie über die Programmlicenzierung erhalten. In diesem Abschnitt erfahren Sie ebenso, wie Sie statistische Informationen zu den verarbeiteten Objekten und dem Umfang an erkannten Bedrohungen und Spam-Nachrichten einsehen können.

## IN DIESEM ABSCHNITT

---

Über den Schutzstatus des Servers .....	<a href="#">42</a>
Anzeigen der Meldungen zum Schutzstatus des Servers .....	<a href="#">45</a>

## ÜBER DEN SCHUTZSTATUS DES SERVERS

Mithilfe der Management-Konsole erhalten Sie folgende aktuelle Informationen zum Schutzstatus des angeschlossenen Servers:

- Informationen zum Server und zu den Programmkomponenten
- Lizenzinformationen
- Informationen zum Zustand der Datenbanken von Anti-Spam und Anti-Virus
- Statistische Informationen zu Objekten, die von den Programmkomponenten verarbeitet wurden

Diese Informationen werden für den gewählten Server im Ergebnisbereich der Management-Konsole angezeigt (auf der Seite **Monitoring**). Der Inhalt dieser Seite wird einmal pro Minute aktualisiert. Sie können den Inhalt der Seite **Monitoring** sofort aktualisieren, indem Sie die Taste **F5** drücken.

### Informationen zum Server und zu den Programmkomponenten

Im oberen Bereich der Seite **Monitoring** werden folgende Meldungen zum verbundenen Server und zu den Programmkomponenten angezeigt:

- **Servername.**
  - Name des physischen Servers (im Format Canonical Name), wenn die Management-Konsole mit einem einzelnen Server, einem passiven Cluster-Knoten oder einem DAG-Server verbunden ist.
  - Name des virtuellen Servers (im Format Canonical Name), wenn die Management-Konsole mit einem virtuellen Server oder mit seinem aktiven Knoten verbunden ist.
- **Informationen zum Verlauf der Programminstallation:**
  - Bezeichnung "Virtueller Server", wenn die Management-Konsole mit dem virtuellen Server oder mit seinem aktiven Knoten verbunden ist.
  - Name der DAG, wenn die Management-Konsole mit einem DAG-Server verbunden ist.
- **Version** – Informationen zur installierten Programmversion.
- **Anti-Spam-Schutz.** Status der Komponente Anti-Spam. Wird angezeigt, wenn für Microsoft Exchange Server Hub Transport Role oder Edge Transport Role installiert wurde.

- **Virenschutz für Hub Transport Role.** Status der Komponente Antivirus für Hub Transport Role. Wird angezeigt, wenn für Microsoft Exchange Server Hub Transport Role oder Edge Transport Role installiert wurde.
- **Virenschutz für Mailbox Role.** Status der Komponente Antivirus für Mailbox Role. Wird angezeigt, wenn für Microsoft Exchange Server Mailbox Role installiert wurde.

Jedes der Felder, die den Status der Programmkomponenten anzeigen, kann einen der folgenden Werte enthalten:

- **Aktiv** – die Komponente ist installiert und aktiv.
- **Deaktiviert** – die Komponente ist installiert und vorübergehend deaktiviert.
- **Nicht installiert** – die Komponente ist nicht installiert.

Die Auswahl der Felder, die den Status der Programmkomponenten anzeigen, kann je nach der Konfiguration von Microsoft Exchange Server gekürzt sein. Wenn das Feld der Komponente nicht angezeigt wird, kann diese Komponente nicht in der aktuellen Serverkonfiguration von Microsoft Exchange Server installiert werden.

## Informationen zur Lizenz

In der Einstellungsgruppe **Lizenz** werden folgende Informationen zum Zustand der gültigen Lizenz angezeigt:

- **Funktionalität** – das Funktionalitätsniveau des Programms, das von der gültigen Lizenz bestimmt wird.
- **Status** – der Zustand der gültigen Lizenz. Kann folgende Werte annehmen:
  - *Aktiv,*
  - *Die Gültigkeit der Testlizenz ist abgelaufen;*
  - *Lizenz ist abgelaufen, Update ist verboten;*
  - *Datenbanken wurden beschädigt;*
  - *Schlüssel fehlt;*
  - *Der Schlüssel wurde blockiert;*
  - *Die schwarze Schlüsselliste wurde beschädigt oder nicht gefunden:*

Wenn im Feld **Status** ein anderer Wert angezeigt wird als **Aktiv**, ist der Block **Lizenz** rot hervorgehoben. Das bedeutet, dass die Bedingungen der gültigen Lizenz verletzt wurden. In einem solchen Fall müssen Sie einen aktiven Schlüssel hinzufügen oder ihn ersetzen (s. Abschnitt "Hinzufügen des Schlüssels" auf S. [35](#)).

- **Ablaufdatum** – das Ablaufdatum für die Gültigkeit der geltenden Lizenz; Wird im Format angezeigt, das in den Einstellungen der Betriebssysteme festgelegt ist. Wenn die Gültigkeit der Lizenz abläuft, wird das Feld rot hervorgehoben. Der Zeitraum bis zum Ablauf der Gültigkeit der Lizenz, in dem das Feld rot hervorgehoben wird, kann unter **Benachrichtigung über Ablauf der Lizenz N Tage vorher** eingegeben werden. Standardmäßig beträgt dieser Zeitraum 15 Tage (s. Abschnitt "Warnmeldung bei Ablauf der Lizenz" auf S. [36](#)).
- **Anzahl von Mailboxes** – die maximale Anzahl von E-Mail-Postfächern, die gemäß den gültigen Lizenzbedingungen geschützt werden können.
- **Reserveschlüssel** – Status des Reserveschlüssels: **Hinzugefügt** oder **Fehlt**.

Mit einem Klick auf **Schlüsselverwaltung** öffnen Sie den Knoten **Lizenzierung**. Dieser Knoten erlaubt es, Schlüssel hinzuzufügen und zu entfernen (s. Abschnitt "Lizenzierung des Programms" auf S. [32](#)).

Wenn die Lizenzbedingungen verletzt wurden (z. B. der Schlüssel ist gesperrt), wird der Block **Lizenz** rot hervorgehoben.

## Informationen zum Zustand der Datenbanken

In der Einstellungsgruppe **Anti-Spam-Datenbanken** werden folgende Informationen zum Zustand der Anti-Spam-Datenbanken angezeigt:

- **Letztes Update** – das Datum des letzten Updates der Anti-Spam-Datenbanken.
- **Status** – der Status des letzten Updates der Anti-Spam-Datenbanken.
- **Herausgabedatum und -zeitpunkt** – das Datum und der Zeitpunkt der Veröffentlichung der Anti-Spam-Datenbanken. Werden im Format angezeigt, das in den Einstellungen des Betriebssystems festgelegt ist. Wenn die Anti-Spam-Datenbanken älter sind als 24 Stunden, wird der Text in diesem Feld rot hervorgehoben.

Mit einem Klick auf **Anpassen der Update-Einstellungen** öffnen Sie den Knoten **Updates**.

Wenn die letzte Aktualisierung der Anti-Spam-Datenbanken mit einem Fehler beendet wurde, wird der Block rot hervorgehoben, während im Feld **Status** eine Fehlermeldung angezeigt wird.

In der Einstellungsgruppe **Antiviren-Datenbanken** werden folgende Meldungen angezeigt:

- **Letztes Update** – das Datum des letzten Updates der Anti-Viren-Datenbanken.
- **Status** – der Status des letzten Updates der Anti-Viren-Datenbanken.
- **Herausgabedatum und -zeitpunkt** – das Datum und der Zeitpunkt der Veröffentlichung der Anti-Viren-Datenbanken. Werden im Format angezeigt, das in den Einstellungen des Betriebssystems festgelegt ist. Wenn die Antiviren-Datenbanken älter sind als 24 Stunden, wird der Text in diesem Feld rot hervorgehoben.
- **Anzahl der Datenbankeinträge** – die Anzahl der Einträge über bekannte Drohungen, die in den Anti-Viren-Datenbanken enthalten sind.

Mit einem Klick auf **Anpassen der Update-Einstellungen** öffnen Sie den Knoten **Updates**.

Wenn die letzte Aktualisierung der Antiviren-Datenbanken mit einem Fehler beendet wurde, wird der Block rot hervorgehoben, während im Feld **Status** eine Fehlermeldung angezeigt wird.

## Statistische Informationen

In der Einstellungsgruppe **Statistik** werden folgende Tabellen angezeigt, die statistische Informationen zum Betrieb der Programmkomponenten in den letzten sieben Tagen enthalten:

- **Anti-Spam.** Enthält folgende Informationen:
  - **Nachrichten gesamt.** Anzahl der bearbeiteten Nachrichten.
  - **Enthalten Spam.** Anzahl der gefundenen Spam-Nachrichten.
  - **Nicht untersucht.** Anzahl der nicht geprüften Nachrichten.
  - **Kein Spam.** Anzahl der geprüften Nachrichten, die kein Spam enthielten.
  - **Sonstige.** Anzahl der Nachrichten, die zu den folgenden Kategorien gehören:
    - Potentieller Spam.
    - Formelle Benachrichtigung.
    - Nachricht, auf die sich die Schwarze oder die Weiße Liste erstrecken.

- **Antivirus für Hub Transport Role.** Enthält folgende Informationen:
  - **Nachrichten gesamt.** Anzahl der bearbeiteten Nachrichten.
  - **Enthalten Viren.** Anzahl gefundener infizierter Nachrichten.
  - **Nicht untersucht.** Anzahl der nicht geprüften Nachrichten.
  - **Keine Viren.** Anzahl der geprüften Nachrichten, die keine Bedrohungen enthielten.
  - **Sonstige.** Anzahl der Nachrichten, die zu den folgenden Kategorien gehören:
    - Möglicherweise infiziert.
    - Geschützt.
    - Beschädigt.
  
- **Antivirus für Mailbox Role.** Enthält folgende Informationen:
  - **Servername.** Name des verbundenen Servers.
  - **Objekte insgesamt.** Anzahl der bearbeiteten Nachrichten.
  - **Enthalten Viren.** Anzahl gefundener infizierter Nachrichten.
  - **Nicht untersucht.** Anzahl der nicht geprüften Nachrichten.
  - **Keine Viren.** Anzahl der geprüften Nachrichten, die keine Bedrohungen enthielten.
  - **Sonstige.** Anzahl der Nachrichten, die zu den folgenden Kategorien gehören:
    - Möglicherweise infiziert.
    - Geschützt.
    - Beschädigt.

Die Auswahl der Tabellen kann je nach nach der Konfiguration des Programms gekürzt sein.

Mit einem Klick auf **Zu Berichten übergangen** öffnen Sie den Knoten **Berichte**, über den Sie Berichte über die Programmausführung erstellen können (s. S. [86](#)).

## ANZEIGEN DER MELDUNGEN ZUM SCHUTZSTATUS DES SERVERS

➔ *Um Meldungen über den Schutzstatus des Servers zu sehen, gehen Sie folgendermaßen vor:*

1. Starten Sie Kaspersky Security über **Start** → **Programme** → **Kaspersky Security 8.0 für Microsoft Exchange Server** → **Management-Konsole**.
2. Wählen Sie im Konsolenbaum den Knoten des angeschlossenen Servers.

Im Ergebnisbereich öffnet sich die Seite **Monitoring**, in der Meldungen über den Zustand des Serverschutzes angezeigt werden.

3. Nehmen Sie im Block **Lizenzen** folgende Handlungen vor:
  - a. Wenn der Block rot hervorgehoben ist, fügen Sie einen aktiven Schlüssel hinzu oder ersetzen Sie ihn (s. Abschnitt "Hinzufügen des Schlüssels" auf S. [35](#)).
  - b. Wenn das Feld **Gültigkeitsdauer** bis rot hervorgehoben ist, prüfen Sie, ob ein Reserveschlüssel hinzugefügt wurde, und fügen Sie ihn bei Bedarf hinzu (s. Abschnitt "Hinzufügen des Schlüssels" auf S. [35](#)).
4. Wenn der Block **Anti-Spam-Datenbanken** oder das Feld **Datum und Uhrzeit der Herausgabe** in diesem Block rot hervorgehoben sind, müssen Sie die Anti-Spam-Datenbanken aktualisieren (s. Abschnitt "Manuelles Update" auf S. [52](#)). Konfigurieren Sie bei Bedarf das Update der Anti-Spam-Datenbanken (s. Abschnitt "Automatisches Update" auf S. [53](#)).
5. Wenn der Block **Antiviren-Datenbanken** oder das Feld **Datum und Uhrzeit der Herausgabe** in diesem Block rot hervorgehoben sind, müssen Sie die Antiviren-Datenbanken aktualisieren (s. Abschnitt "Manuelles Update" auf S. [52](#)). Konfigurieren Sie bei Bedarf das Update der Antiviren-Datenbanken (s. Abschnitt "Automatisches Update" auf S. [53](#)).

# STANDARDMÄßIGER VIRENSCHUTZSTATUS FÜR MICROSOFT EXCHANGE SERVER

Der Schutz für den Microsoft Exchange Server-Server vor schädlichen Programmen und Spam wird sofort nach Installation der Sicherheitsserver-Komponente aktiviert, sofern dies nicht im Konfigurationsassistenten (s. Abschnitt "Schutz für den Server anpassen" auf S. [26](#)) deaktiviert wurde. Standardmäßig wird das Programm im folgenden Modus ausgeführt:

- Die Objekte werden auf sämtliche aktuell bekannten Viren und schädlichen Programme überprüft:
  - Es werden sämtliche E-Mail-Textkörper und Anhänge in beliebigen Formaten überprüft, mit Ausnahme von Objekten in Containern mit mehr als 32-facher Verschachtelung.
  - Die maximale Dauer der Prüfung für ein einzelnes Objekt beträgt 180 Sekunden.
  - Welche Aktion beim Auffinden infizierter Objekte ausgeführt wird, richtet sich danach, in welcher Rolle des Microsoft Exchange-Servers ein Objekt gefunden wurde:
    - Beim Auffinden infizierter Objekte in der Edge Transport Rolle oder Hub Transport Rolle werden infizierte Objekte sofort automatisch gelöscht. Eine Kopie des Ursprungsobjekts wird im Backup-Ordner gespeichert und dem Betreff der Nachricht ein Präfix [Malicious object deleted] hinzugefügt.
    - Beim Auffinden infizierter Objekte in der Mailbox Rolle speichert das Programm eine Kopie des Ursprungsobjekts (Anhang oder Textkörper) im Backup und versucht, das Objekt zu desinfizieren. Falls dies nicht gelingt, wird das Objekt gelöscht und durch eine Textdatei in folgendem Format ersetzt:  
  
Schädliches Objekt gefunden <Virus\_Name>. Die Datei (<Objekt\_Name>) wurde von Kaspersky Security 8.0 für Microsoft Exchange Server gelöscht. Servername: <Server\_Name>
  - Aufgefundene geschützte oder beschädigte Objekte werden bei Verwendung der Standardeinstellungen vom Programm ignoriert. Benutzerdefiniert kann auch die Aktion Löschen für diese beiden Objektkategorien gewählt werden. Hierbei speichert das Programm eine Kopie des Ursprungsobjektes im Backup-Ordner.
  - Geschützt werden Speicherzeichnisse für öffentliche Ordner und für E-Mail-Postfächer.
- Spam-Nachrichten werden herausgefiltert. Stellen Sie mit dem Schieberegler die gewünschte Intensivitätsstufe für die Spamprüfung ein. Dies gewährleistet ein optimales Verhältnis von Performance und Gründlichkeit während der Überprüfung:
  - Für alle E-Mail-Nachrichten ist die Aktion Ignorieren voreingestellt; Nachrichten mit dem Verdikt "Spam" werden jedoch besonders gekennzeichnet [!!Spam].
  - Ist die Option **Potenzieller Spam** aktiviert, erhalten dem entsprechende Nachrichten ebenfalls ein Kennzeichen [!!Probable Spam].
  - Die maximale Dauer der Prüfung pro einzelner E-Mail beträgt 30 Sekunden.
  - Die maximale Größe für ein einzelnes zu prüfendes Objekt beträgt 300 KB.
  - Es werden folgende externe Server zur Prüfung der IP-Adressen und URL-Links verwendet: DNSBL und SURBL. Hierbei wird Spam anhand öffentlich verfügbarer "Blacklists" für IP-Adressen und URL-Links herausgefiltert.
  - Service UDS deaktiviert (s. Abschnitt "Einstellungen für die Spamprüfung anpassen" auf S. [67](#)).
- Wenn der Service KSN im Installationsassistenten aktiviert war, so nimmt dieser Service an der Arbeit Anti-Spam (s. Abschnitt "Aktivieren KSN" auf S. [27](#)) teil. Andernfalls ist Service KSN deaktiviert (s. Abschnitt "Einstellungen für die Spamprüfung anpassen" auf S. [67](#)).
- Wenn die Updatefunktion für die Datenbanken von Kaspersky Security im Konfigurationsassistenten aktiviert wurde (s. Abschnitt "Schutz für den Server anpassen" auf S. [26](#)), werden die Datenbanken regelmäßig über die Server von "Kaspersky Lab" aktualisiert.

# ERSTE SCHRITTE

Die Programmverwaltung erfolgt über den Arbeitsplatz des Administrators. Dies ist der Computer, auf dem die Management-Konsole installiert ist. Sie können eine beliebige Anzahl an Computern zur Management-Konsole hinzufügen, um sie lokal oder im Remote-Modus zu verwalten.

## IN DIESEM ABSCHNITT

Management-Konsole starten .....	<a href="#">48</a>
Liste geschützter Microsoft Exchange-Server erstellen.....	<a href="#">48</a>
Management-Konsole mit dem Sicherheitsserver verbinden .....	<a href="#">50</a>

## MANAGEMENT-KONSOLE STARTEN

➤ *Zum Starten der Management-Konsole gehen Sie wie folgt vor:*

1. Im Menü **Start** wählen Sie den Punkt **Programme**.
2. Wählen Sie **Kaspersky Security 8.0 für Microsoft Exchange Server**.
3. Klicken Sie mit der linken Maustaste auf **Management-Konsole**.

Beim Start der Management-Konsole verbindet sich ein Tool von Kaspersky Security mit der MMC. Im Konsolenbaum werden das Programmsymbol und der Knoten **Kaspersky Security 8.0 für Microsoft Exchange Server** angezeigt. Weiterhin wird im Konsolenbaum der Node für den mit der Konsole verbundenen lokalen Sicherheitsserver angezeigt (sofern dieser installiert ist).

## LISTE GESCHÜTZTER MICROSOFT EXCHANGE-SERVER ERSTELLEN

Sie können eine Liste geschützter Microsoft Exchange-Server erstellen. Dazu muss auf jedem Microsoft Exchange-Server, der geschützt werden soll, die Komponente Sicherheitsserver installiert sein. Sie können sowohl lokale Computer hinzufügen (s. Abb. unten), als auch beliebige geschützte Microsoft Exchange-Server aus Ihrem Netzwerk. Sofort nach Hinzufügen eines Servers kann sich die Management-Konsole mit Kaspersky Security verbinden.

Sie können die Microsoft Exchange Database Availability Group (DAG) nicht zur Liste der geschützten Server hinzufügen. Statt dessen können Sie jeden der Server hinzufügen, die der DAG angehören, um ihn zwecks Ausführung allgemeiner Aktionen für die DAG zu kontaktieren (wie bspw. die Anpassung der Benachrichtigungseinstellungen oder die Inhaltsanzeige des Backup-Ordners), sowie weiterhin einen konkreten Server für die Anpassung der individuellen Servereinstellungen (wie die Einstellungen für den Backup-Ordner).

➤ *Um den Sicherheitsserver für Kaspersky Security zur Liste geschützter Server hinzuzufügen, gehen Sie wie folgt vor:*

1. Starten Sie Kaspersky Security über **Start** → **Programme** → **Kaspersky Security 8.0 für Microsoft Exchange Server** → **Management-Konsole**.
2. Wählen Sie im Konsolenbaum den Knoten **Kaspersky Security 8.0 für Microsoft Exchange Server**.

3. Wählen Sie im Kontextmenü des Knotens den Befehl **Server hinzufügen** oder den gleichlautenden Punkt im Menü **Aktion**.



Abbildung 3. Sicherheitsserver hinzufügen

4. Wählen Sie eine der beiden Varianten:
- **Lokaler Computer.** In diesem Fall wird ein Sicherheitsserver hinzugefügt, der auf einem lokalen Computer installiert ist.
  - **Anderer Computer.** In diesem Fall können Sie einen Sicherheitsserver anschließen, der auf einem Microsoft Exchange-Remoteserver installiert ist. Zum Verbinden mit einem Sicherheitsserver, der auf einem Remotecomputer installiert ist, müssen Sie Kaspersky Security zur Liste vertrauenswürdiger Programme der Firewall auf dem Remotecomputer hinzufügen oder die Verbindung über RPC erlauben.
5. Haben Sie die Option **Anderer Computer** gewählt, tragen Sie den Namen des Computers im Eingabefeld ein. Sie können den Namen manuell eingeben. Geben Sie hierfür wahlweise folgendes ein:
- die IP-Adresse;
  - den vollständigen Domainnamen (im Format <Computername>.<DNS-Domainname>);
  - den Namen des Computers in Microsoft Windows (NetBIOS-Name).
- Sie können den Computer auch aus einer Liste mit Hilfe der Schaltfläche **Durchsuchen** auswählen.
6. Klicken Sie auf **OK**.

Der ausgewählte Computer wird in die Liste der geschützten Server aufgenommen.

# MANAGEMENT-KONSOLE MIT DEM SICHERHEITSSERVER VERBINDEN

Nach dem Start von Kaspersky Security stellt die Management-Konsole automatisch eine Verbindung zum lokalen Sicherheitsserver her. Der Sicherheitsserver wird hierbei im Verzeichnisbaum der Management-Konsole angezeigt. Zum Verbinden mit einem Sicherheitsserver, der auf einem Remotecomputer installiert ist, müssen Sie Kaspersky Security zur Liste vertrauenswürdiger Programme der Firewall auf dem Remotecomputer hinzufügen oder die Verbindung über RPC erlauben.

Sie können die Management-Konsole nicht in die Microsoft Exchange Database Availability Group (DAG) einschließen. Stattdessen können Sie sie an einen beliebigen Sicherheitsserver der DAG-Server anschließen, um allgemeine Aktionen für die DAG auszuführen (z. B. Anpassung der Benachrichtigungseinstellungen oder Inhaltsanzeige des Backup-Ordners), oder sie an einen Sicherheitsserver eines einzelnen Servers anschließen, um die individuellen Servereinstellungen anzupassen (z. B. Einstellungen für den Backup-Ordner).

Es wird dringend davon abgeraten, eine Verbindung mit diesen Servern über die Management-Konsole aufzubauen und die Programmeinstellungen anzupassen, solange das Update der Vorgängerversion auf die aktuelle Version auf den DAG-Servern läuft (s. Abschnitt "Aktualisierung von Vorgängerversionen" auf S. 21). Andernfalls könnte das Update fehlerhaft beendet werden, was zu Unterbrechungen im Programmbetrieb führen kann. Wenn eine Verbindung während des Updates unvermeidlich ist, müssen Sie zunächst sicherstellen, dass die Version des Administrationsservers und die der Administrationskonsole, über die die Verbindung hergestellt wird, identisch sind.

➤ Um die Management-Konsole an einen Remote-Sicherheitsserver anzuschließen, gehen Sie wie folgt vor:

1. Starten Sie Kaspersky Security über **Start → Programme → Kaspersky Security 8.0 für Microsoft Exchange Server → Management-Konsole**.
2. Wählen Sie im Konsolenbaum den Knoten **Kaspersky Security 8.0 für Microsoft Exchange Server**.
3. Wählen Sie die Option **Server hinzufügen** im Kontextmenü des Knotens oder im Menü **Aktion**. Sie können auch die Schaltfläche **Server hinzufügen** im Detailfenster verwenden.
4. Wählen Sie im geöffneten Fenster die Option **Anderer Computer** aus und geben Sie mithilfe der Schaltfläche **Durchsuchen** im Eingabefeld den Namen des Computers ein, auf dem der Sicherheitsserver installiert ist. Sie können den Computernamen auch manuell eingeben. Geben Sie dazu einen der folgenden Werte ein:
  - die IP-Adresse;
  - den vollständigen Domainnamen (im Format <Computername>.<DNS-Domainname>);
  - den Namen des Computers in Microsoft Windows (NetBIOS-Name).

Sie können den Computer auch aus einer Liste mit Hilfe der Schaltfläche **Durchsuchen** auswählen.

5. Klicken Sie auf **OK**.

Der ausgewählte Computer wird in die Liste der geschützten Server aufgenommen.

# REGELMÄßIGES UPDATE DER ANTI-VIREN- UND ANTI-SPAM-DATENBANKEN

Kunden von Kaspersky Lab erhalten regelmäßige Updates für die zur Suche nach schädlichen Programmen und Desinfektion von Dateien verwendeten Datenbanken in Kaspersky Security. Die Datenbankdateien enthalten Beschreibungen aller zum jeweiligen Zeitpunkt aktuell bekannten schädlichen Programme sowie der Möglichkeiten zur Desinfektion infizierter Objekte; außerdem Beschreibungen zu potenziell als schädlich eingestuftem Programmen.

Die Anti-Spam-Datenbanken werden ebenfalls aktualisiert. Für die maximal wirksame Filtrierung der Spam ist es empfehlenswert, die minimale Periodizität der Aktualisierung der Anti-Spam-Datenbanken festzustellen.

Es ist außerordentlich wichtig, dass die Datenbanken stets auf dem aktuellen Stand sind. Es wird empfohlen, sofort nach Installation des Programms ein Datenbankupdate auszuführen, da die im Installationspaket enthaltenen Datenbanken zum Zeitpunkt der Installation sicher veraltet sein werden. Auf den Updateservern von Kaspersky Lab werden die Anti-Viren-Datenbanken regelmäßig einmal pro Stunde aktualisiert. Die Anti-Spam-Datenbanken werden in einem Abstand von 5 Minuten aktualisiert. Es wird empfohlen, das automatische Update des Programms (s. Abschnitt "Automatisches Update" auf S. 53) mit demselben Intervall einzustellen.

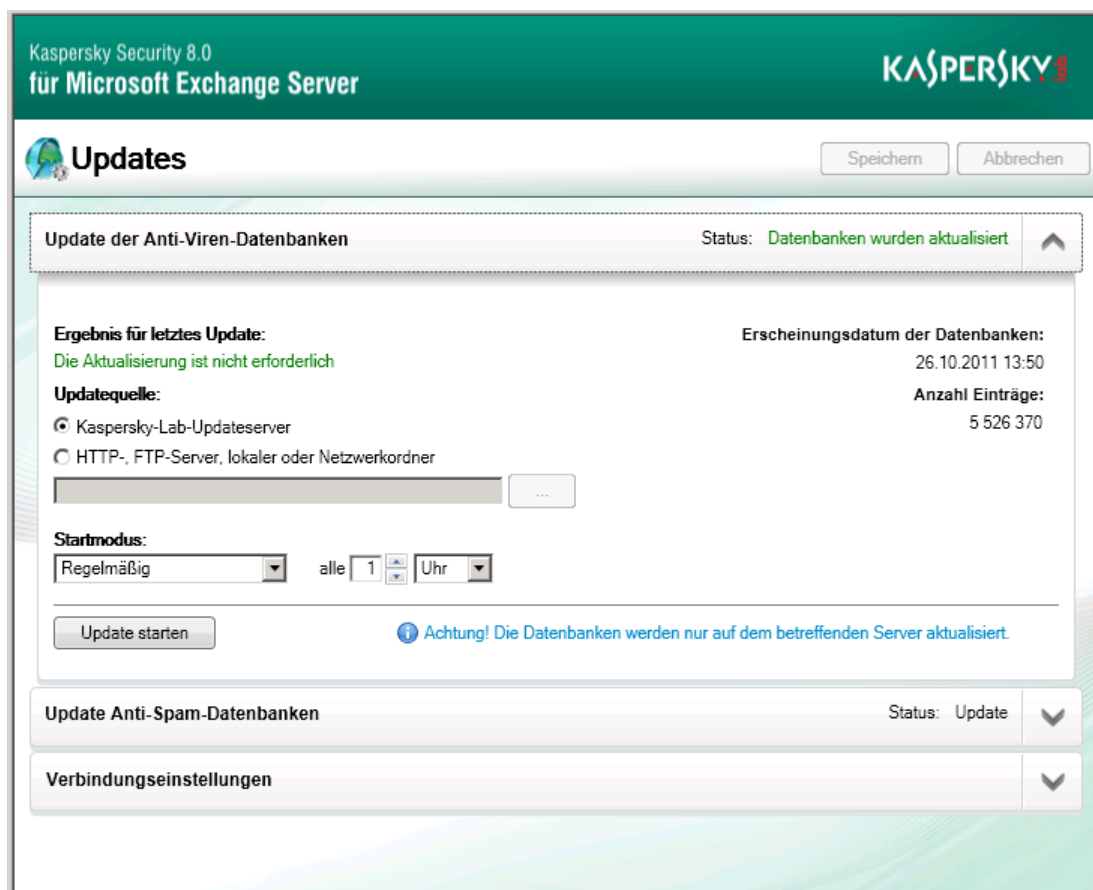


Abbildung 4. Anti-Viren-Datenbanken aktualisieren

Kaspersky Security kann das Datenbankupdate aus folgenden Quellen bekommen:

- Updateserver von Kaspersky Lab im Internet;
- lokale Update-Quellen: lokale oder Netzwerkverzeichnisse;
- andere HTTP- / FTP-Server (z.B. Ihr Intranet-Server).

Updates können manuell oder anhand eines Zeitplanes erfolgen. Nach dem Kopieren der Dateien von der ausgewählten Update-Quelle aktiviert das Programm automatisch die neuen Datenbanken.

## IN DIESEM ABSCHNITT

Manuelles Update .....	<a href="#">52</a>
Automatisches Update .....	<a href="#">53</a>
Updatequelle auswählen .....	<a href="#">54</a>
Verbindungseinstellungen anpassen .....	<a href="#">54</a>

# MANUELLES UPDATE

➤ *Um Informationen zum Update der Anti-Spam-Datenbanken anzuzeigen und diese bei Bedarf zu aktualisieren, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Updates**.
3. Expandieren Sie den Einstellungsblock **Antiviren-Datenbanken aktualisieren**.

Es werden folgende Informationen zu Datenbankupdates angezeigt:

- **Ergebnis des letzten Updates.** Statusinformationen zum Datenbankupdate.
- **Erscheinungsdatum der Datenbanken.** Die Zeit der Veröffentlichung der Datenbanken auf dem Kaspersky Lab Server, welche im Programm im Moment verwendet werden (UTC).
- **Anzahl Einträge.** Anzahl Virensignaturen in der aktuellen Datenbank.

4. Wählen Sie in der erscheinenden Liste **Startmodus** die Variante **Manuell**.
5. Klicken Sie auf die Schaltfläche **Update starten**.
6. Zum Unterbrechen des Updates klicken Sie auf die Schaltfläche **Anhalten**.

➤ *Um Informationen zum Update der Anti-Spam-Datenbanken anzuzeigen und diese bei Bedarf zu aktualisieren, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Updates**.
3. Expandieren Sie den Einstellungsblock **Anti-Spam-Datenbanken aktualisieren**.

Es werden folgende Informationen zu Datenbankupdates angezeigt:

- **Ergebnis des letzten Updates.** Statusinformationen zum Datenbankupdate.
- **Erscheinungsdatum der Datenbanken.** Die Zeit der Veröffentlichung der Datenbanken auf dem Kaspersky Lab Server, welche im Programm im Moment verwendet werden (UTC).

4. Wählen Sie in der erscheinenden Liste **Startmodus** die Variante **Manuell**.

5. Klicken Sie auf die Schaltfläche **Update starten**.
6. Zum Unterbrechen des Updates klicken Sie auf die Schaltfläche **Anhalten**.

Wenn das Programm auf dem Cluster oder DAG der Server Microsoft Exchange arbeitet, soll die Aktualisierung der Datenbanken auf jedem der Server der Sicherheit, die in den Cluster oder DAG eingehen, manuell erfüllt sein.

## AUTOMATISCHES UPDATE

➤ Um die automatisches Update für die Anti-Viren-Datenbanken einzustellen, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen .
2. Wählen Sie den Node**Updates**.
3. Expandieren Sie im Detailfenster den Einstellungsblock **Anti-Viren-Datenbanken aktualisieren**.
4. Wählen Sie in der sich öffnenden Liste **Startmodus** eine der folgenden Varianten:
  - **Regelmäßig**. Geben Sie im Eingabefeld mit der Scrollbox **alle** N Minuten, Stunden, Tage vor, wie oft Updates ausgeführt werden sollen.
  - **Täglich**. Geben Sie die genaue Uhrzeit ein (lokal): **um hh:min**.
  - **An folgenden Tagen**. Aktivieren Sie das Kästchen neben den Wochentagen, an denen Updates ausgeführt werden sollen, und geben Sie die Uhrzeit ein.
5. Klicken Sie auf die Schaltfläche **Speichern**.
6. Zum Unterbrechen des Updates klicken Sie auf die Schaltfläche **Anhalten**. Sie können nur das aktuelle Update abbrechen. Das nächste Update wird nach dem Zeitplan ausgeführt.

Wenn das Programm auf DAG der Server Microsoft Exchange arbeitet, die Parameter der automatischen Aktualisierung der Anti-Viren-Datenbanken, die auf einem der Server eingestellt sind, erstreckt sich automatisch auf die übrigen Server, die in diese DAG eingehen. Auf den übrigen Servern dieses DAG kann man die automatische Erneuerung nicht einstellen.

➤ Um das automatische Update der Anti-Spam-Datenbanken einzurichten, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node**Updates**.
3. Expandieren Sie im Detailfenster den Einstellungsblock **Anti-Viren-Datenbanken aktualisieren**.
4. Wählen Sie in der sich öffnenden Liste **Startmodus** eine der folgenden Varianten:
  - **Regelmäßig**. Geben Sie im Eingabefeld mit der Scrollbox **alle** N Minuten, Stunden, Tage vor, wie oft Updates ausgeführt werden sollen.
  - **Täglich**. Geben Sie die genaue Uhrzeit ein (lokal): **um hh:min**.
  - **An folgenden Tagen**. Aktivieren Sie das Kästchen neben den Wochentagen, an denen Updates ausgeführt werden sollen, und geben Sie die Uhrzeit ein.
5. Klicken Sie auf die Schaltfläche **Speichern**.
6. Zum Unterbrechen des Updates klicken Sie auf die Schaltfläche **Anhalten**. Sie können nur das aktuelle Update abbrechen. Das nächste Update wird nach dem Zeitplan ausgeführt.

## UPDATEQUELLE AUSWÄHLEN

➤ *Um die Updatequelle für die Anti-Viren-Datenbanken auszuwählen, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Updates**.
3. Expandieren Sie im Detailfenster den Einstellungsblock **Anti-Viren-Datenbanken aktualisieren**, und wählen Sie eine der folgenden Varianten:
  - **Kaspersky Lab Update-Server**, wenn Sie Updates von den Kaspersky Lab Servern herunterladen wollen.
  - **HTTP-, FTP-Server, lokales oder Netzwerkverzeichnis**, wenn eine der genannten Quellen für Updates verwendet werden soll.
4. Geben Sie im Eingabefeld die Adresse für den Server bzw. das lokale oder Netzwerkverzeichnis ein.
5. Klicken Sie auf die Schaltfläche **Speichern**.

Wenn das Programm auf DAG der Server Microsoft Exchange arbeitet, die Parameter der automatischen Aktualisierung der Anti-Viren-Datenbanken (z.B. Updatequelle), die auf einem der Server eingestellt sind, erstreckt sich automatisch auf die übrigen Server, die in diese DAG eingehen. Auf den übrigen Servern dieses DAG kann man die automatische Erneuerung nicht einstellen.

➤ *Um die Updatequelle für die Anti-Spam-Datenbanken auszuwählen, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Updates**.
3. Expandieren Sie im Detailfenster den Einstellungsblock **Anti-Spam-Datenbanken aktualisieren**, und wählen Sie eine der folgenden Varianten:
  - **Kaspersky Lab Update-Server**, wenn Sie Updates von den Kaspersky Lab Servern herunterladen wollen.
  - **HTTP-, FTP-Server, lokales oder Netzwerkverzeichnis**, wenn eine der genannten Quellen für Updates verwendet werden soll.
4. Geben Sie im Eingabefeld die Adresse für den Server bzw. das lokale oder Netzwerkverzeichnis ein.
5. Klicken Sie auf die Schaltfläche **Speichern**.

## VERBINDUNGSEINSTELLUNGEN ANPASSEN

➤ *Um die Parameter der Verbindung mit der Updatequelle einzustellen, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Updates**.
3. Expandieren Sie im Detailfenster den Einstellungsblock **Verbindungseinstellungen**.

4. Falls für die Internetverbindung Proxy-Server eingesetzt werden, setzen Sie das Häkchen **Proxy-Server verwenden** und legen Sie die Verbindungseinstellungen fest.
5. Geben Sie im Eingabefeld **Timeout für Verbindungen** über die Scrollbox die maximale Wartezeit für Verbindungen ein. Bei Verwendung der Standardeinstellungen beträgt das Zeitlimit **60** Sekunden.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Falls für die Internetverbindung Proxy-Server eingesetzt werden, konfigurieren Sie die Parameter des Proxy-Servers.

► *Um die Parameter des Proxy-Servers zu konfigurieren, erfüllen Sie die folgenden Handlungen:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Einstellungen**.
3. Setzen Sie im Detailfenster im Einstellungsblock **Proxy-Server-Einstellungen** gehen Sie wie folgt vor:
  - a. Geben Sie die Proxyserver-Adresse im Feld **Proxyserver-Adresse** ein.
  - b. Wählen Sie im Eingabefeld über die Scroll-down-Liste den gewünschten Proxyserver-Port. Standardmäßig wird Port **8080** verwendet.
  - c. Um die Authentifizierung für den gewählten Proxyserver zu verwenden, markieren Sie das Kontrollkästchen **Authentifizierung verwenden** und geben Sie den Benutzerkonto im Feld **Benutzerkonto** und Passwort im Feld **Password** ein.
  - d. Soll der Download von Updates von einem lokalen Server ihres Firmennetzwerkes ohne Verwendung eines Proxyservers erfolgen, markieren Sie das Kontrollkästchen **Keinen Proxyserver für lokale Adressen verwenden**.
4. Klicken Sie auf die Schaltfläche **Speichern**.

# VIRENSCHUTZ

Eine der Hauptaufgaben von Kaspersky Security ist die Überprüfung des E-Mail-Verkehrs, der in den Postfächern gespeicherten Mails und der öffentlichen Ordner auf Viren, und die Desinfektion befallener Objekte mithilfe der aktuellen Anti-Viren-Datenbanken.

Sämtliche über den Microsoft Exchange-Server eingehenden E-Mails werden in Echtzeit überprüft. Überprüft werden eingehende, ausgehende und weitergeleitete E-Mail-Nachrichten. Für E-Mail-Nachrichten, die schädliche Objekte enthalten, können folgende Aktionen ausgeführt werden:

- Betroffene E-Mail-Nachricht und schädliches Objekt ignorieren.
- Schädliches Objekt löschen und E-Mail ignorieren.
- E-Mail-Nachricht und schädliches Objekt löschen.

Beim Löschen schädlicher Objekte in der Mailbox Rolle werden diese durch eine Textnachricht ersetzt, aus welcher der Name des schädlichen Objektes, das Erscheinungsdatum für die zur Erkennung verwendeten Datenbanken und der Name des Microsoft Exchange-Servers hervorgehen, auf dem das Objekt gefunden wurde.

Beim Auffinden schädlicher Objekte in der Hub Transport Rolle wird in der Betreffzeile der Nachricht folgendes Präfix hinzugesetzt: `Malicious object deleted`.

Ist der Modus E-Mail-Prüfung aktiviert, ist das Programm ständig im Arbeitsspeicher des Computers geladen. Das Abfangmodul für E-Mails analysiert sämtliche vom Microsoft Exchange-Server übertragenen E-Mails und übergibt sie zur Verarbeitung an das Anti-Virus-Modul. Das Anti-Viren-Programm erfüllt die folgenden Handlungen:

- Prüft die E-Mails mit Hilfe der Anti-Viren-Datenbanken;
- Sind E-Mail-Nachrichten ganz oder teilweise infiziert, werden gefundene Objekte gemäß den eingestellten Einstellungen weiter verarbeitet;

Vor der Verarbeitung können Kopien der Objekte im Backup-Ordner gespeichert werden.

Ist der Virenschutz auf dem Server aktiviert, wird die Prüfung des E-Mail-Verkehrs beim Start von Microsoft Exchange Server automatisch mit gestartet bzw. angehalten.

Kaspersky Security prüft keine von geschützten Benutzern erstellten E-Mail-Nachrichten in **öffentlichen Ordnern** auf nicht geschützten Microsoft Exchange-Servern. Beim Verschieben von E-Mail-Nachrichten aus **öffentlichen Ordnern** nicht geschützter Verzeichnisse in geschützte Verzeichnisse werden diese durch das Programm überprüft. Bei der Replikation von Daten zwischen geschützten und nicht geschützten Verzeichnissen werden vom Programm im Ergebnis der Virenprüfung vorgenommene Änderungen nicht synchronisiert.

Die auf dem Server aufbewahrten Meldungen und der Inhalt der Gesamtordner werden auch regelmäßig überprüft, mit Verwendung der letzten Version der Datenbanken falls die Hintergrundprüfung von Ablagen (s. Abschnitt "Prüfung im Hintergrund" auf S. [63](#)) aktiviert ist. Durch die Hintergrundprüfung wird die Serverbelastung zu Spitzenzeiten reduziert und die Sicherheit der E-Mail-Architektur insgesamt erhöht. Die Prüfung läuft im Hintergrund und kann sowohl manuell als auch automatisch nach voreingestelltem Zeitplan gestartet werden.

Die Ausführung der Hintergrundprüfung kann die Performance von Microsoft Exchange Server beeinträchtigen. Daher wird empfohlen, diese auf Zeiten mit möglichst geringer Auslastung der Mailserver zu verlegen, z.B. in die Nachtstunden.

Im Modus "Prüfung im Hintergrund" empfängt das interne Programmsteuerungsmodul in Abhängigkeit der gewählten Einstellungen von Microsoft Exchange-Server sämtliche in öffentlichen Ordnern und geschützten Verzeichnissen gespeicherten E-Mail-Nachrichten. Wurde zur Prüfung von Nachrichten nicht die aktuellste Version der Programmdateienbanken verwendet, übergibt das Programm die Nachrichten an die Komponente Anti-Virus. Die Verbreitung von Objekten im Hintergrundmodus läuft genau so ab, wie bei der Überwachung des E-Mail-Verkehrs.

Das Programm prüft sowohl den Textkörper der E-Mails als auch Dateianhänge in beliebigen Formaten.

Wissen sollten Sie auch, dass Kaspersky Security zwischen einfachen Objekten (nur Textkörper oder Textkörper mit einfacher Anlage - z.B. ausführbare Datei) und Objektcontainern (enthalten mehrere Objekte, wie z.B. Archivdateien oder E-Mails mit E-Mails als Anhang) unterscheidet.

Bei der Prüfung von mehrteiligen Archiven wird jeder Archivteil vom Programm als einzelnes Objekt erkannt und verarbeitet. In diesem Fall kann Kaspersky Security schädliche Codes nur identifizieren, wenn sie als ganzes in einem einzelnen Archivteil auftreten. Werden die Daten nur zum Teil geladen und ein schädlicher Code hierbei ebenfalls, geteilt, wird er während der Prüfung nicht gefunden. In diesem Fall kann es vorkommen, dass nach dem erneuten Zusammenfügen der Objekte sich schädliche Codes ungehindert weiter verbreiten. Aus mehreren Teilen bestehende Archive können nach dem Speichern auf Viren überprüft werden.

Falls gewünscht, können Sie eine Liste von Objekten erzeugen, die von der Virenprüfung ausgeschlossen werden sollen. Folgende Objekte können Sie von der Virenprüfung ausschließen: Archive, Objekte in Containern mit einem Verschachtelungsgrad über dem vorgegebenen Wert und Dateien mit bestimmten Masken.

Dateien größer als 1 MB werden zur Verarbeitung im Hilfsordner Store im Datenspeicherordner des Programms abgelegt. Den Ordner Store und den Speicherordner für temporäre Dateien (TMP) müssen Sie von der Prüfung durch Virenschutzprogramme ausschließen, die auf Servern installiert sind, auf welchen Microsoft Exchange läuft.

## IN DIESEM ABSCHNITT

Virenschutz für den Server aktivieren und deaktivieren .....	<a href="#">57</a>
Verarbeitungsregeln für Objekte erstellen .....	<a href="#">58</a>
Dateianhänge in Archiven und Container prüfen.....	<a href="#">59</a>
Schutzeinstellungen für Postfächer einrichten .....	<a href="#">60</a>
Einstellung der Ausnahmen für die Anti-Virenprüfung.....	<a href="#">60</a>
Prüfung im Hintergrund .....	<a href="#">63</a>

## VIRENSCHUTZ FÜR DEN SERVER AKTIVIEREN UND DEAKTIVIEREN

Ist der Anti-Virenschutz für den Server aktiviert, wird die Anti-Virenprüfung des E-Mail-Verkehrs gemeinsam mit Microsoft Exchange Server gestartet bzw. angehalten. Falls in den Einstellungen des Anti-Virus-Schutzes die Hintergrundprüfung von Ablagen (s. Abschnitt "Prüfung im Hintergrund" auf S. [63](#)) vorgesehen ist, kann sie manuell oder zeitplanmäßig gestartet werden.

Bitte beachten Sie, dass sich durch Deaktivieren des Anti-Virenschutzes die Gefahr des Eindringens schädlicher Objekte erhöht. Sie sollten den Anti-Virenschutz nie für längere Zeit deaktivieren.

Der Antivirusschutz auf Hub Transport Rolle oder Mailbox Rolle Microsoft Exchange Server aktiviert sich abgesondert.

► *Um den Virenschutz für Mailbox Rolle einen angeschlossenen Microsoft Exchange-Server zu aktivieren, gehen Sie wie folgt vor:*

1. Starten Sie Kaspersky Security über **Start** → **Programme** → **Kaspersky Security 8.0 für Microsoft Exchange Server** → **Management-Konsole**.
2. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
3. Wählen Sie den Node **Serverschutz**.

4. Öffnen Sie in der Registerkarte **Schutz für Mailbox Role** im Einstellungsblock **Untersuchungseinstellungen von Anti-Virus** setzen Sie das Häkchen **Virenschutz für Mailbox Role aktivieren**.
5. Klicken Sie auf die Schaltfläche **Speichern**.

Wenn das Programm auf DAG der Server Microsoft Exchange arbeitet, aktiviert sich der Antivirenschutz für Mailbox Role, der auf einem der Server aktiviert ist, auf den übrigen Servern, die in diese DAG eingehen, automatisch. Auf den übrigen Servern dieses DAG kann man den Antivirenschutz für Mailbox Role nicht aktivieren.

- *Um den Virenschutz für Hub Transport Rolle einen angeschlossenen Microsoft Exchange-Server zu aktivieren, gehen Sie wie folgt vor:*
  1. Starten Sie Kaspersky Security über **Start → Programme → Kaspersky Security 8.0 für Microsoft Exchange Server → Management-Konsole**.
  2. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
  3. Wählen Sie den Node **Serverschutz**.
  4. Öffnen Sie in der Registerkarte **Schutz für Hub Transporter Role** im Einstellungsblock **Untersuchungseinstellungen von Anti-Virus** setzen Sie das Häkchen **Virenschutz für Hub Transporter Role aktivieren**.
  5. Klicken Sie auf die Schaltfläche **Speichern**.
- *Falls die Notwendigkeit entsteht, den Kaspersky Security Dienst manuell zu deaktivieren, gehen Sie folgendermaßen vor:*
  1. Deaktivieren Sie den Anti-Virenschutz über die Management-Konsole (s. oben).
  2. Stoppen Sie den Dienst von Kaspersky Security und stellen Sie als Autostarttyp – **Deaktiviert** ein.
- *Um das Programm nach Deaktivierung der Autostart-Option für Kaspersky Security erneut zu starten gehen Sie folgendermaßen vor:*
  1. Überzeugen Sie sich davon, dass für Kaspersky Security der Autostarttyp – **Automatisch** eingestellt ist.
  2. Aktivieren Sie den Anti-Virenschutz über die Management-Konsole (s. oben).

## VERARBEITUNGSREGELN FÜR OBJEKTE ERSTELLEN

Über Verarbeitungsregeln für Objekte können Sie für jeden Objekttyp die gewünschten Aktionen festlegen. Nach einer Virenprüfung wird jedem einzelnen Objekt ein Status zugewiesen:

- **Infiziert** – enthält mindestens einen bekannten Virus.
- **Nicht infiziert** – enthält keine Viren.
- **Geschützt** – Passwortgeschütztes Objekt.
- **Beschädigt** – beschädigtes Objekt.

Die Regeln der Bearbeitung der Objekte auf Hub Transport Rolle oder Mailbox Rolle Microsoft Exchange Server entstehen abgesondert.

- *Um Verarbeitungsregeln für Objekte anzulegen, gehen Sie wie folgt vor:*
  1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
  2. Wählen Sie den Node **Serverschutz**.

3. Erfüllen Sie eine der folgenden Handlungen:
  - Wenn Sie die Regeln der Objektbearbeitung für die Rolle Mailbox erstellen möchten, erweitern Sie im Detailfenster in der Registerkarte **Schutz für Mailbox Role** den Einstellungsblock **Untersuchungseinstellungen von Anti-Virus**.
  - Wenn Sie die Regeln der Objektbearbeitung für die Hub Transport Role erstellen möchten, erweitern Sie im Detailfenster in der Registerkarte **Schutz für Hub Transport Role** den Einstellungsblock **Untersuchungseinstellungen von Anti-Virus**.
4. Wählen Sie im Abschnitt **Verarbeitungsregeln für Objekte** in der sich öffnenden Liste **Infiziertes Objekt** die gewünschte Aktion:
  - **Ignorieren**. Betroffene E-Mail-Nachricht und Objekt ignorieren.
  - **Objekt löschen**. Schädliches Objekt löschen und E-Mail ignorieren.
  - **Nachricht löschen**. Nachricht mit dem schädlichen Objekt mit allen Anlagen löschen.
5. Wählen Sie in der sich öffnenden Liste **Geschütztes Objekt** die gewünschte Aktion:
  - **Ignorieren**. Passwortgeschützte Objekte können möglicherweise nicht auf Viren geprüft werden. Wählen Sie **Ignorieren**, wenn diese Objekte ignoriert werden sollen.
  - **Nachricht löschen**. Wählen Sie diese Aktion, wenn passwortgeschützte Objekte gelöscht werden sollen. Die Nachrichten mit diesen Objekte werden vollständig gelöscht.
6. Wählen Sie in der sich öffnenden Liste **Beschädigtes Objekt** die gewünschte Aktion:
  - **Ignorieren**. Wählen Sie diese Option, wenn diese Objekte ignoriert werden sollen.
  - **Nachricht löschen**. Wählen Sie diese Option, wenn beschädigte Objekte ignoriert werden sollen.
7. Markieren Sie das Kästchen **Kopie der Ursprungsdatei im Backup-Ordner speichern**, um vor der Verarbeitung von Objekten eine Kopie im Backup-Ordner anzulegen.

Wenn das Programm auf DAG der Server Microsoft Exchange arbeitet, der Regel der Bearbeitung der Objekte, die für Mailbox Rolle eingestellt sind, erstreckt sich automatisch auf die übrigen Server, die in diese DAG eingehen. Auf den übrigen Servern dieses DAG kann man die Regel der Bearbeitung der Objekte für Mailbox Rolle nicht einstellen. Jedoch, ist es erforderlich, die Regeln der Bearbeitung der Objekte für Hub Transporter Rolle erforderlich, abgesondert auf jedem der Server, die in DAG eingehen, einstellen.

## DATEIANHÄNGE IN ARCHIVEN UND CONTAINER PRÜFEN

Als Voreinstellung prüft Kaspersky Security die Archive und die Container, die in die Nachrichten angelegt sind. Um die Performance von Kaspersky Security zu verbessern, den Server zu entlasten und die Verarbeitungszeit für die E-Mail-Prüfung zu verkürzen, können Sie die Prüfung von Archiven deaktivieren. Sie sollten die Prüfung von Dateianhängen nie für längere Zeit deaktivieren, da diese Viren und andere schädliche Objekte enthalten können.

➤ *Um die Prüfeinstellungen für Dateianhänge in Archiven und Containern anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Serverschutz**.
3. Wählen Sie im Detailfenster die Registerkarte **Ausnahmen von der Untersuchung durch Anti-Virus**.
4. Entfernen Sie das Häkchen **Archive prüfen**, wenn das Programm Archive in der Nachrichten auf Viren nicht prüfen soll. Um die Prüfung der Archive zu aktivieren, setzen Sie dieses Häkchen.

5. Entfernen Sie das Häkchen **Eingebettete Container überprüfen**, wenn das Programm die eingebettete Container auf Viren nicht prüfen soll. Um die Prüfung der eingebetteten Container zu aktivieren, setzen Sie dieses Häkchen und geben Sie im Eingabefeld mit der Scrollbox den maximalen Verschachtelungsgrad für Container vor **Container mit Verschachtelung von maximal prüfen**. Der Maximal mögliche Verschachtelungsgrad beträgt **128**.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Wenn das Programm auf DAG der Server Microsoft Exchange arbeitet, die Parameter der Prüfung der angelegten Archive und Container, die auf einem der Server eingestellt sind, erstreckt sich automatisch auf die übrigen Server, die in diese DAG eingehen. Auf den übrigen Servern dieses DAG kann man die Parameter der Prüfung der angelegten Archive und Container nicht einstellen.

## SCHUTZEINSTELLUNGEN FÜR POSTFÄCHER EINRICHTEN

➤ Um den Virenschutz für E-Mail-Postfächer benutzerdefiniert festzulegen, gehen Sie wie folgt vor:

1. Wählen Sie in der Management-Konsole den Node **Serverschutz**.
2. Öffnen Sie in der Registerkarte **Schutz für das Postfach Rolle** den Einstellungsblock **Schutz von Mail-Postfächern**.

In der Liste **Geschützte Verzeichnisse für E-Mail-Postfächer** und **Geschützte Verzeichnisse in allgemeinen Ordnern** werden sämtliche Verzeichnisse für Postfächer und öffentliche Ordner unter Microsoft Exchange angezeigt. Wenn das Programm auf DAG der Server Microsoft Exchange arbeitet, werden in diesen Listen die Verzeichnisse für Postfächer und öffentliche Ordnern, die sich auf allen Servern befinden, die in diese DAG eingehen, aufgezählt sein.

3. Markieren Sie in Liste **Geschützte Verzeichnisse für E-Mail-Postfächer**, die Verzeichnisse für Postfächer, welche geschützt werden sollen.
4. Markieren Sie in Liste **Geschützte Verzeichnisse in allgemeinen Ordnern** die Verzeichnisse in allgemeinen Ordnern, welche geschützt werden sollen.
5. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu übernehmen.

## EINSTELLUNG DER AUSNAHMEN FÜR DIE ANTI-VIRENPRÜFUNG

Um die Serverauslastung während der Anti-Virenprüfung zu reduzieren, können Sie Ausnahmen von der Prüfung durch Einschränkung der Liste der zu prüfenden Objekte angeben. Die Ausnahmen für die Anti-Virenprüfung gelten sowohl für die Prüfung des E-Mail-Verkehrs als auch für die Prüfung von Speicherordnern im Hintergrund.





Sie können die Ausnahmen von der Anti-Viren-Prüfung durch folgende Möglichkeiten einstellen:

- Deaktivieren Archiven und Container prüfen (s. Abschnitt "Dateianhänge in Archiven und Container prüfen" auf S. [59](#)).
- Dateien ausschließen anhand einer Maske der Dateinamen (s. Abschnitt "Einstellung der Ausnahmen nach einer Dateinamensmaske" auf S. [61](#)). Dateien, deren Namen den angegebenen Masken entsprechen, werden nicht auf Viren geprüft.
- Einstellung der Ausnahmen nach Empfängeradressen. E-Mails, die an die angegebenen Empfänger adressiert sind, werden nicht auf Viren geprüft.

Wenn das Programm auf DAG der Server Microsoft Exchange arbeitet, die Ausnahme aus Prüfung, die auf einem der Server eingestellt sind, erstreckt sich automatisch auf die übrigen Server, die in diese DAG eingehen. Auf den übrigen Servern dieses DAG kann man die Ausnahme aus Prüfung nicht einstellen.

## EINSTELLUNG DER AUSNAHMEN NACH DATEINAMENSMASKEN

➤ Um die Ausnahmen nach einer Dateinamensmaske einzustellen, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Serverschutz**.
3. Wählen Sie im Detailfenster die Registerkarte **Ausnahmen von der Untersuchung durch Anti-Virus**.
4. Markieren Sie das Kästchen **Dateien mit folgenden Masken nicht prüfen**.
5. Um die Maske der Dateinamen (weiter – Maske) in die Maskenliste einzufügen, gehen Sie wie folgt vor:
  - a. Geben Sie die Maske im Eingabefeld ein.  
Beispiele für erlaubte Dateinamensmasken:
    - \*.txt – alle Dateien mit der Erweiterung txt, z.B. readme.txt oder notes.txt;
    - readme.??? – alle Dateien mit Namen readme und einer Erweiterung aus 3 Zeichen, z.B. readme.txt oder readme.doc;
    - test – alle Dateien mit Namen Test und ohne Dateierweiterung.
  - b. Betätigen Sie die Schaltfläche , rechts neben dem Eingabefeld.
6. Um eine Maske aus der Liste der Masken zu entfernen, wählen Sie die Zeile mit der Maske in der Liste aus und betätigen die Schaltfläche .
7. Um die Liste der Masken in eine Datei zu exportieren, klicken Sie auf die Schaltfläche . Geben Sie in dem sich öffnenden Fenster im Feld **Dateiname** den Dateinamen ein, und klicken Sie auf die Schaltfläche **Speichern**.
8. Um die Liste der Masken aus einer Datei zu importieren, klicken Sie auf die Schaltfläche . Geben Sie in dem sich öffnenden Fenster im Feld **Dateiname** den Namen der Datei mit der Maskenliste ein und klicken Sie auf die Schaltfläche **Öffnen**.
9. Klicken Sie auf die Schaltfläche **Speichern**.

## EINSTELLUNG DER AUSNAHMEN NACH EMPFÄNGERADRESSEN

Sie können aus der Virenprüfung E-Mails, die an bestimmte Empfänger adressiert sind, ausschließen, indem Sie die Adressen dieser Empfänger in der Liste der vertrauenswürdigen Adressaten eintragen. Standardmäßig ist der Liste leer.

Sie können in die Liste der vertrauenswürdigen Adressaten Empfänger in folgenden Formen ergänzen:

- Active Directory Objekte:
  - Einfache Benutzer (User).
  - Kontakte (Contact).
  - Verbreitungsgruppe (Distribution Group).
  - Sicherheitsgruppe (Security Group).

Es ist empfehlenswert, die Adressen in Form von Einträgen dieses Typs zu ergänzen.

- SMTP-Adresse als mailbox@domain.com. Einträge dieses Typs sind erforderlich, wenn Anti-Virus für die Rolle Hub Transport eingerichtet ist und die auszuschließende Adresse in Active Directory nicht gefunden werden kann.

Um einen öffentlichen Ordner (Public Folder) aus der Untersuchung durch Anti-Virus für die Rolle Hub Transport auszuschließen, fügen Sie alle SMTP-Adressen des Ordners zur Liste der vertrauenswürdigen Empfänger hinzu, falls es mehrere Empfänger vorhanden sind. Wenn einige SMTP-Adressen des öffentlichen Ordners in der Liste nicht vorhanden sind, können die in den öffentlichen Ordner eingehenden E-Mails untersucht werden.

- Namen von Benutzern oder Gruppen (Display Name). Einträge dieses Typs sind erforderlich, wenn Anti-Virus für die Mailbox Rolle eingerichtet ist und die auszuschließende Adresse in Active Directory nicht gefunden werden kann.
- Öffentliche Ordner (Public Folder). Einträge dieses Typs müssen hinzugefügt werden, wenn Anti-Virus für die Rolle Mailbox installiert wurde. Sie können nicht aus Active Directory ausgewählt werden. Fügen Sie sie hinzu, indem Sie den vollständigen Pfad des öffentlichen Ordners angeben.


Wenn Anti-Virus für die Rolle Mailbox und für die Rolle Hub Transport eingerichtet ist und die auszuschließende Adresse in Active Directory nicht gefunden werden kann, müssen in die "Whitelist" der Empfänger zwei der Adresse entsprechende Einträge vorgenommen werden: die SMTP-Adresse und der Name des Benutzers / der Gruppe. Andernfalls werden an diese Adresse ankommende E-Mails nicht aus der Prüfung ausgeschlossen.

Empfängeradressen, die als Active Directory Objekte angegeben sind, werden aus der Anti-Viren-Prüfung gemäß den folgenden Regeln ausgeschlossen:





- Wenn die Empfängeradresse die Form eines einfachen Benutzer, eines Kontaktes oder eines öffentlichen Ordners hat, werden die daran adressierten E-Mails aus der Prüfung ausgeschlossen.
- Wenn die Adresse in Form einer Verbreitungsgruppe eingetragen ist, werden E-Mails, die an diese Gruppe adressiert sind, aus der Prüfung ausgeschlossen. Jedoch werden E-Mails, die persönlich an Mitglieder der Verbreitungsgruppe adressiert sind, nicht aus der Prüfung ausgeschlossen, wenn diese nicht einzeln in die Liste eingetragen wurden.
- Wenn die Adresse in Form einer Sicherheitsgruppe eingetragen ist, werden E-Mails, die an diese Gruppe sowie Mitglieder dieser Gruppe adressiert sind, aus der Prüfung ausgeschlossen. Jedoch, wenn eine Sicherheitsgruppe ein eingebundenes Mitglied einer Verbreitungsgruppe ist, werden E-Mails, die an deren Mitglieder adressiert sind, nicht aus der Prüfung ausgeschlossen, wenn die Mitglieder nicht einzeln in die Liste eingetragen wurden.


Das Programm erneuert automatisch die aus Active Directory erhaltenen Empfängeradressen bei Veränderung der entsprechenden Einträge in Active Directory (zum Beispiel, wenn sich die E-Mail-Adresse eines Benutzers geändert hat oder wenn einer Sicherheitsgruppe ein neuer Teilnehmer hinzugefügt wurde). Die Erneuerung wird einmal pro Tag durchgeführt.

➔ *Um die Ausnahmen nach der Empfängeradresse einzustellen, gehen Sie wie folgt vor:*




1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Serverschutz**.
3. Wählen Sie im Detailfenster die Registerkarte **Ausnahmen von der Untersuchung durch Anti-Virus**.
4. Setzen Sie das Häkchen **Meldungen für Empfänger nicht überprüfen**.
5. Um eine Empfängeradresse in die Liste der vertrauenswürdigen Adressen einzufügen, führen Sie eine der folgenden Aktionen aus:
  - Um den Eintrag zur Liste aus Active Directory hinzuzufügen, betätigen die Schaltfläche . Finden Sie im sich öffnenden Fenster den gewünschten Active Directory Eintrag und betätigen Sie die Schaltfläche **OK**.

Die aus Active Directory übernommenen Adressen werden in der Liste durch folgende Icons gekennzeichnet:

-  – einfache Benutzer, Kontakte, Verbreitungsgruppe;
-  – Sicherheitsgruppe.
- Um eine SMTP-Adresse, einen Benutzernamen oder einen öffentlichen Ordner in die Liste einzutragen, gehen Sie wie folgt vor:
  - Um eine SMTP-Adresse oder einen Benutzernamen einzutragen, geben Sie diese(n) im Eingabefeld ein und klicken auf die Schaltfläche .
  - Um einen öffentlichen Ordner einzutragen, geben Sie den Pfad zum Ordner ein und klicken auf die Schaltfläche .

Die Adressen, die auf diese Weise hinzugefügt wurden, sind durch das Icon  gekennzeichnet.

Adressen, die auf diese Weise hinzugefügt wurden, werden nicht auf das Vorhandensein in Active Directory geprüft.

6. Um eine Adresse aus der Liste der vertrauenswürdiger Adressen zu entfernen, wählen Sie die Zeile mit der Adressaten in der Liste aus und betätigen die Schaltfläche .
7. Um die Liste der vertrauenswürdiger Adressen zu exportieren, klicken Sie auf die Schaltfläche . Geben Sie in dem sich öffnenden Fenster im Feld **Dateiname** den Dateinamen ein, und klicken Sie auf die Schaltfläche **Speichern**.
8. Um die Liste der vertrauenswürdiger Adressen aus einer Datei zu importieren, klicken Sie auf die Schaltfläche . Geben Sie in dem sich öffnenden Fenster im Feld **Dateiname** den Namen der Datei mit der Liste der vertrauenswürdiger Adressen ein, und klicken Sie auf die Schaltfläche **Öffnen**.
9. Klicken Sie auf die Schaltfläche **Speichern**.

## PRÜFUNG IM HINTERGRUND

Kaspersky Security führt eine Anti-Virenprüfung im Hintergrund für alle auf dem Server gespeicherten E-Mail-Nachrichten und öffentlichen Ordner anhand der vom Benutzer definierten Einstellungen durch. Verarbeitet werden hierbei nur E-Mail-Nachrichten, die noch nicht durch die aktuelle Version von Kaspersky Security geprüft wurden.

Die Prüfung im Hintergrund ist nur für Microsoft Exchange-Server in der Mailbox Rolle verfügbar. Das Programm überprüft den Textkörper von E-Mails und E-Mail-Anlagen anhand der gewählten eingestellten Einstellungen für die Anti-Virenprüfung für diese Rolle. Es werden nur die in geschützten Verzeichnissen befindlichen öffentlichen Ordner und E-Mail-Postfächer überprüft.

Wenn das Programm auf DAG der Server Microsoft Exchange arbeitet, die Parameter der Hintergrundüberprüfung, die auf einem der Server eingestellt sind, erstreckt sich automatisch auf die übrigen Server, die in diese DAG eingehen. Auf den übrigen Servern dieses DAG kann man die Parameter der Hintergrundüberprüfung nicht einstellen.

➤ *Um die Hintergrundprüfung für auf dem Server gespeicherte E-Mail-Nachrichten und öffentliche Ordner zu aktivieren, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Serverschutz**.

3. Expandieren Sie im Detailfenster auf der Registerkarte **Schutz für das Postfach Rolle** den Einstellungsblock **Schutz von Mail-Postfächern**.
4. Wählen Sie im Bereich **Prüfung im Hintergrund** in der sich öffnenden Liste **Zeitplan** die gewünschte Option:
  - **Manuell**. Die Prüfung im Hintergrund muss manuell gestartet werden.
  - **Täglich**. Die Prüfung im Hintergrund muss täglich gestartet werden. Geben Sie im Eingabefeld den genauen Startzeitpunkt für die Prüfung, im Format **hh:min** ein.
  - **An folgenden Tagen**. Die Prüfung im Hintergrund muss in die gewählten Tage gestartet werden. Markieren Sie das Kästchen neben den Wochentagen, an denen die Prüfung im Hintergrund ausgeführt werden soll, und Geben Sie im Eingabefeld den genauen Startzeitpunkt für die Prüfung im Format **hh:mm**.
  - **Monatlich**. Die Prüfung im Hintergrund muss ein Mal monatlich gestartet werden. Geben Sie im Eingabefeld mit der Scrollbox den gewünschten Tag für die Prüfung, und den genauen Startzeitpunkt für die Prüfung im Format **hh:min** ein.
5. Markieren Sie das Kästchen **E-Mail Körper prüfen**, wenn während der Prüfung im Hintergrund nur der E-Mail Körper geprüft werden soll.
6. Markieren Sie das Kästchen **Nur aktuelle E-Mails prüfen**, wenn nur E-Mail geprüft werden sollen, die bis zu einem bestimmten Zeitpunkt vor Beginn der Prüfung eingegangen sind.
7. Geben Sie den gewünschten Zeitraum in Tagen im Eingabefeld mit der Scrollbox **Eingegangene E-Mails prüfen bis <N> Tage vor Beginn der Prüfung** ein. Maximaler Wert für die Tageszahl: – **364**.
8. Markieren Sie das Kästchen **Zeitdauer für die Prüfung einschränken**, und geben Sie einen Wert für **Prüfung spätestens <N> Stunden nach dem Start abrechnen** ein, um die Zeitdauer der Prüfung einzuschränken.
9. Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche **Speichern**.
10. Möchten Sie die Prüfung im Hintergrund sofort starten, klicken Sie auf die Schaltfläche **Prüfung starten**.

Hintergrundüberprüfung wird nur auf dem gewählte Server gestartet. Es ist für eine beliebige Konfiguration der Server Microsoft Exchange gerecht, einschließlich DAG. Wenn Sie die Hintergrundüberprüfung sofort auf anderen Servern DAG starten wollen, muss man für jeden der Server die abgesonderte Handlung machen.

11. Zum Unterbrechen der Hintergrundüberprüfung klicken Sie auf die Schaltfläche **Anhalten**. Zum Starten und Anhalten der Prüfung im Hintergrund benötigt das Programm etwa 1 Minute, nachdem Sie auf die entsprechenden Schaltflächen geklickt haben.

# SPAMSCHUTZ

Eine wesentliche Funktion von Kaspersky Security ist das Filtern des über den Server laufenden E-Mail-Verkehrs auf unerwünschte Nachrichten (Spam). Das Modul für die Spamprüfung (Anti-Spam) prüft eingehende E-Mails während des Empfangs, also bevor diese in die E-Mail-Postfächer der Empfänger gelangen.

Geprüft werden hierbei folgende Datentypen:

- Interner und externer E-Mail-Verkehr per SMTP-Protokoll mit anonymer Serverauthentifizierung;
- Über anonyme externe Verbindungen auf dem Server eingehende E-Mails (Edge Server).

Folgende Datentypen werden nicht auf Spam gefiltert:

- interner E-Mail-Verkehr der Organisation;
- externer E-Mail-Verkehr über den Server im Rahmen authentifizierter Sessions. Die Prüfung derartigen E-Mail-Verkehrs kann manuell aktiviert werden (s. Abschnitt "Anpassung der zusätzlichen Einstellungen" auf S. [74](#)).

Jede E-Mail wird auf darin vorhandene Spam-Merkmale geprüft. Hierzu werden zuerst bestimmte Teile der E-Mails geprüft: Absender- und Empfängeradresse, Größe der Nachricht, Header (einschließlich der Einträge in den Feldern "Von" und "An:") usw.

Danach wird eine Inhaltsfilterung eingesetzt, die den Inhalt der E-Mails und Anlagen analysiert (einschließlich des Eintrags in der Betreffzeile). Zur Anwendung kommen spezielle linguistische und heuristische Verfahren, basierend auf Vergleichen mit Muster-Nachrichten, sowie tiefer detaillierte Analysen von E-Mail-Texten, des Layouts und anderen Merkmalen.

Nach dem Filtern erhalten alle geprüften Nachrichten eine der folgenden Einstufungen (Status):

- Spam. Das Programm identifiziert die Nachricht eindeutig als Spam.
- Potenzieller Spam. Bei der Nachricht handelt es sich möglicherweise um Spam.
- Formelle Benachrichtigung. Technisch bedingte Mitteilung, z.B. über die Zustellung der Nachricht an den Empfänger.
- Nachricht enthält keinen Spam. Die Nachricht enthält keinen Spam.
- Wurde in "Blacklist" übernommen. Die E-Mail- oder IP-Adresse des Absenders befindet sich in der "Blacklist" für Adressen.

Sie können die Aktionen auswählen, die das Programm für die Nachrichten mit einem bestimmten Status ausführt. Folgende Varianten stehen zur Auswahl:

- Ignorieren. Die E-Mail wird an den Empfänger zugestellt, ohne Änderungen vorzunehmen.
- Abweisen. Hierbei wird an den Sender-Server eine Fehlermeldung versandt (Fehlercode 500 - Fehler beim Versenden der E-Mail). Die Nachricht wird nicht an den Empfänger zugestellt.
- Löschen. Hierbei erhält der Sender-Server eine Meldung über den Versand der Nachricht (Code 250) – die Nachricht wird jedoch nicht an den Empfänger zugestellt.
- SCL-Rating hinzufügen. Die Nachricht erhält einen Rating-Wert bezüglich der Wahrscheinlichkeit von Spam (SCL). Die möglichen Werte liegen zwischen 1 und 9. Je höher die Ziffer, desto größer ist die Wahrscheinlichkeit für Spam. Für die Berechnung der SCL-Beurteilung wird das Spam-Rating der Überprüfung durch 10 geteilt. Der erhaltene Wert wird für die SCL-Beurteilung übernommen. Falls nach der Abrechnung der Wert höher als 9 ist, wird die SCL-Beurteilung 9 übernommen.
- Kennzeichen hinzufügen. Nachrichten, die durch Kaspersky Security als Spam oder potenzieller Spam identifiziert werden, erhalten eine spezielle Markierung **[!!SPAM]**, **[!!Probable Spam]** oder **[!!Blacklisted]** im Feld Betreff. Der Text dieser Markierungen kann über die Management-Konsole abgeändert werden.

Im Programm sind verschiedene Intensivitätsstufen für eine flexible Anpassung der Spamprüfung vorgesehen. Es gibt folgende Intensivitätsstufen:

- **Maximal.** Sie sollten diese Intensivitätsstufe wählen, falls Sie sehr häufig Spam erhalten. Dies kann jedoch dazu führen, dass auch häufig ungefährliche und erwünschte Mails als Spam erkannt werden.
- **Hoch.** Das Schutzniveau dieser Intensivitätsstufe ist geringer als das der Stufe Maximal, gewährleistet jedoch eine genauere Spamerkennung als diese. Die Stufe Hoch sollten Sie wählen, wenn Sie sehr häufig Spam erhalten.
- **Niedrig.** Diese Stufe gewährleistet einen schwächeren Spamschutz als die Stufe Hoch. Diese Stufe gewährleistet ein optimales Verhältnis von Performance und Gründlichkeit während der Überprüfung.
- **Minimal.** Sie sollten diese Intensivitätsstufe wählen, falls Sie nur selten Spam erhalten.

Standardmäßig ist für den Spamschutz die Intensivitätsstufe Niedrig eingestellt. Sie können die Intensivitätsstufe herauf- oder herabsetzen. Je nach der angegebenen Aggressivitätsstufe wird den überprüften Nachrichten nach der Überprüfung der Status Spam oder Potenzieller Spam zugewiesen.

Tabella 3. Entsprechung der Intensivitätsstufen und der Spam-Rating-Grenzwerte für die Zuordnung der Einstufung Spam und Potenzieller Spam

INTENSIVITÄTSSTUFE	POTENZIELLER SPAM	SPAM
Maximal	50	75
Hoch	50	80
Niedrig	60	90
Minimal	80	100

Für eine noch sorgfältigere Filterung von Spam ist die Möglichkeit der Nutzung folgender externer Dienste vorgesehen:

- **DNSBL.** Server, die öffentlich verfügbare Listen von IP-Adressen enthalten, die bereits als Versender von Spam bekannt sind.
- **SURBL.** Server, die öffentlich verfügbare Listen von Hyperlinks enthalten, die zu Werbe-Websites von Spambietern führen.

Die Listen DNSBL und SURBL werden, wie auch die Anti-Spam-Datenbanken, regelmäßig im Abstand von 5 Minuten aktualisiert. Bei der Ermittlung des Spam-Ratings einer Nachricht werden die Rückmeldungen von DNSBL- und SURBL-Servern berücksichtigt. Der Wert für das Spam-Rating ist eine ganze Zahl zwischen 0 und 100. Die Berechnung des Spam-Ratings erfolgt gemäß der vom DNSBL- und SURBL-Server erhaltenen Rückmeldungen. Übersteigt der ermittelte Gesamt-Ratingwert auf Basis aller erhaltenen Rückmeldungen von den Servern den Wert 100, so wird das Spam-Rating für die betreffende E-Mail auf 100 heraufgesetzt. Liegt der Gesamt-Ratingwert unter 100, wird das Spam-Rating der betreffenden E-Mail nicht vergrößert.

- **UDS.** Von Kaspersky Lab entwickelter und unterstützter Service zur Erfassung von Spam-Sendungen. Die mit Hilfe des UDS-Services durchgeführte Spam-Überprüfung basiert auf dem Vergleich der Merkmale von Meldungen, die mittels einer speziellen UDS-Anfrage an die Server von Kaspersky Lab mit einer Datenbank bekannter Spam-Meldungen gerichtet werden. Wenn die Anfrage mit einer der bekannten Spamnachrichten übereinstimmt, wird das Spam-Rating der Nachricht erhöht. Das UDS-Verfahren ermöglicht die Filterung bekannter Spam-Sendungen, ohne die Aktualisierung der Datenbanken für die Inhaltsfilterung abzuwarten.

Durch das UDS-Verfahren erhält jede E-Mail auf der Client-Seite eine eindeutige nichtumkehrbare Signatur der Nachricht (diese erlaubt keine Rückschlüsse auf Betreff, Inhalt, Absender-/Empfängernamen und -Adressen), und diese Signatur wird an einen UDS-Server übertragen. Findet sich diese Signatur in den "Blacklists" auf dem UDS-Server, wird das Spam-Rating für die Nachricht erhöht. Um diesen Dienst nutzen zu können, müssen folgende Ports geöffnet werden: 7060 für UDS1 und 7080 für UDS2. Die Verbindung erfolgt über UDP-Protokoll. Standardmäßig ist die Verwendung des UDS-Verfahrens deaktiviert. Um die Verwendung des UDS-Verfahrens zu aktivieren, müssen Sie einer speziellen KSN-Vereinbarung zustimmen, in der das Verfahren zur Datenerfassung bzw. -verwendung auf einem mit funktionsfähigem Kaspersky Security ausgestatteten Computer geregelt wird.

- **KSN.** Komplex von verteilten Diensten, der den Schutz der Benutzer verbessert, die Reaktion von Kaspersky-Lab-Programmen auf neue Arten von Bedrohungen und Spam beschleunigt und die Anzahl der Fehlalarme minimiert. Die Funktion von KSN basiert auf der Analyse von Datenfragmenten, die automatisch von den Rechnern der Benutzer an die Kaspersky-Lab-Server gesendet werden. Die Nutzung von KSN ermöglicht eine umgehende Reaktion von Kaspersky Security auf das Auftauchen neuer Spamarten sowie eine hohe Genauigkeit bei der Bearbeitung von Spammeldungen. Standardmäßig ist die Verwendung von KSN deaktiviert. Um KSN zu aktivieren, müssen Sie einer speziellen KSN-Vereinbarung zustimmen, in der das Verfahren zur Datenerfassung bzw. -verwendung auf einem mit funktionsfähigem Kaspersky Security ausgestatteten Computer geregelt wird.
- **Enforced Anti-Spam Updates Service.** Schnell-Update-Service der Anti-Spam-Datenbanken. Wenn die Verwendung von Enforced Anti-Spam Updates Service aktiviert ist, verbindet sich das Programm ständig mit den Kaspersky-Lab-Servern und aktualisiert die eigenen Anti-Spam-Datenbanken sofort nach dem Erscheinen der neuen Beschreibungen von Spam-Meldungen auf den Kaspersky-Lab-Servern. Das erhöht die Anti-Spam-Reaktionsschnelligkeit beim Auftauchen neuer Spam-Sendungen.

Folgende Bedingungen müssen für die Funktion des Enforced Anti-Spam Updates Service erfüllt sein:

- eine ständige Internet-Verbindung des Computers, auf dem der Sicherheitsserver installiert ist.
- ein regelmäßiges Update der Anti-Spam-Datenbanken (empfohlen wird ein Update alle fünf Minuten).

In Kaspersky Security können Sie einen dynamischen DNS-Client verwenden. Ein dynamischer DNS-Client ermittelt auf Basis des DNS reverse lookups die Wahrscheinlichkeit, dass eine IP-Adresse zu einem Bot-Net gehört. Diese Funktion kann genutzt werden, wenn der geschützte SMTP-Server nicht für eigene Benutzer mit xDSL- oder Dialup-Verbindung verwendet wird.

Zur Spamverarbeitung kann auch das SPF-Verfahren aktiviert werden. Das SPF-Verfahren (Structure Policy Framework) überprüft, ob die Domain des Absenders echt ist. Durch das SPF-Verfahren erlaubt eine Domain bestimmten Computern den E-Mail-Versand unter dem Domainnamen. Wenn der Absender der Nachricht nicht auf der Liste der autorisierten Absender steht, wird das Spam-Rating der Nachricht vergrößert.

## IN DIESEM ABSCHNITT

Einstellungen für die Spamprüfung anpassen.....	<a href="#">67</a>
Einstellung der "Whitelist" und "Blacklist" der Absender .....	<a href="#">69</a>
Einstellung der "Whitelist" für E-Mail-Empfänger .....	<a href="#">70</a>
Konfigurierung der Einstellungen zur Ermittlung des Spam-Ratings.....	<a href="#">72</a>
Externe Dienste zur Spamverarbeitung nutzen.....	<a href="#">73</a>
Einstellungen für Anti-Spam-Berichte anpassen.....	<a href="#">74</a>

## EINSTELLUNGEN FÜR DIE SPAMPRÜFUNG ANPASSEN

➔ *Zum Anpassen der Einstellungen für die Spamprüfung gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Serverschutz**.
3. Öffnen Sie in der Registerkarte **Schutz für Hub Transport Role** den Einstellungsblock **Untersuchungseinstellungen von Anti-Spam**.
4. Markieren Sie das Kästchen **Nachrichten auf Spam prüfen**, wenn eingehende E-Mails durch Anti-Spam geprüft werden sollen.

5. Stellen Sie mit dem Schieberegler die gewünschte **Intensivitätsstufe** für den Spamschutz ein. Kaspersky Security besitzt vier verschiedene Intensivitätsstufen für die Spamprüfung:
  - **Maximal.** Sie sollten diese Intensivitätsstufe wählen, falls Sie sehr häufig Spam erhalten. Dies kann jedoch dazu führen, dass auch häufig ungefährliche und erwünschte Mails als Spam erkannt werden.
  - **Hoch.** Das Schutzniveau dieser Intensivitätsstufe ist geringer als das der Stufe **Maximal**, gewährleistet jedoch eine genauere Spamerkennung als diese. Die Stufe **Hoch** sollten Sie wählen, wenn Sie sehr häufig Spam erhalten.
  - **Niedrig.** Diese Stufe gewährleistet einen schwächeren Spamschutz als bei Wahl der Stufe **Hoch**. Diese Stufe gewährleistet ein optimales Verhältnis von Performance und Gründlichkeit während der Überprüfung.
  - **Minimal.** Diese Intensivitätsstufe sollten Sie wählen, wenn Sie nur selten Spam erhalten, z.B innerhalb eines geschützten Firmennetzwerkes.
  
6. Im Einstellungsblock **Verarbeitungsregeln für Spam** wählen Sie die Aktion, die das Programm mit den Nachrichten mit jedem der aufgezählten Status erfüllen wird:
  - **Ignorieren.** Die Nachricht wird ohne Änderungen an den Empfänger zugestellt.
  - **Abweisen.** Hierbei wird an den Sender-Server eine Fehlermeldung versandt (Fehlercode 500 - Fehler beim Versenden der E-Mail). Die Nachricht wird nicht an den Empfänger zugestellt.
  - **Löschen.** Der Sender-Server erhält eine Meldung über den Versand der Nachricht (Code 250). Die Nachricht wird jedoch nicht an den Empfänger zugestellt.
  
7. Geben Sie die zusätzliche Aktionen, die das Programm mit den Nachrichten mit jedem der aufgezählten Status erfüllen wird, ein. Setzen Sie die Häkchen für die folgenden Parameter nach Ihrem Ermessen fest:
  - **SCL-Rating hinzufügen.** Die Nachricht erhält einen Ratingwert für die Wahrscheinlichkeit unerwünschter E-Mails (SCL). Die möglichen Werte liegen zwischen 1 und 9. Je höher die Ziffer, desto größer ist die Wahrscheinlichkeit für Spam.
  - **Kopie speichern.** Eine Kopie der E-Mail wird im Backup-Ordner gespeichert.
  - **Kennzeichen hinzufügen.** Nachrichten, die durch Kaspersky Security als Spam oder potenzieller Spam identifiziert oder deren Absender in der "Blacklist" eingetragen wurden, erhalten ein spezielles Kennzeichen **[!!SPAM]**, **[!!Probable Spam]** oder **[!!Blacklisted]** im Feld **Betreff**. Die Kennzeichen können angepasst werden.
  
8. Konfigurieren Sie die Einstellungen für die Nutzung zusätzlicher Dienste::
  - Wenn Sie die Nutzung der Services KSN und UDS aktivieren möchten, erfüllen Sie die folgenden Aktionen:
    - a. Lesen Sie das KSN-Vereinbarung und übernehmen Sie seine Bedingungen, und setzen Sie das Häkchen **Ich stimme der KSN-Vereinbarung zu**. Öffnen Sie die KSN-Vereinbarung durch Anklicken von **KSN-Vereinbarung anzeigen** in einem neuen Fenster, um diese vollständig angezeigt zu bekommen.
    - b. Um die Nutzung des Services KSN zu aktivieren, setzen Sie das Häkchen **Verwenden Kaspersky Security Network (KSN)**.
    - c. Geben Sie im Eingabefeld mit der Scrollbox die maximale Wartezeit für die Verbindung zum Server KSN vor **Timeout KSN**. Der voreingestellte Standardwert beträgt 10 Sekunden.
    - d. Um die Nutzung des Services KSN zu aktivieren, setzen Sie das Häkchen **Verwenden Urgent Detection System (UDS)**.
    - e. Geben Sie im Eingabefeld mit der Scrollbox die maximale Wartezeit für die Verbindung zum Server USD vor **Timeout UDS**. Der voreingestellte Standardwert beträgt 10 Sekunden.

- Wenn Sie die Nutzung des Services der schnellen Aktualisierung der Anti-Spam-Datenbanken aktivieren möchten, setzen Sie das Häkchen **Verwenden Enforced Anti-Spam Updates Service**.
- Wenn Sie möchten, dass die Anschließen zu den Servern KSN und Enforced Anti-Spam Updates Service durch den Proxy-Server erfüllt wurden, setzen Sie das Häkchen **Verwenden Proxyserver für den Zugriff auf KSN und Enforced Anti-Spam Updates Service**. Die Einstellungen des Proxyservers können Sie im **Node Einstellungen anpassen**.

9. Klicken Sie auf die Schaltfläche **Speichern**.

## EINSTELLUNG DER "WHITELIST" UND "BLACKLIST" DER ABSENDER





Sie können zwei Arten von Absenderlisten konfigurieren:

- "Whitelists". Adresslisten vertrauenswürdiger Absender, deren E-Mails nicht auf Spam nicht geprüft werden sollen.
- "Blacklists". Adresslisten von Absendern, von denen alle E-Mails als Spam gelten.

Kaspersky Security ermöglicht, "Whitelists" und "Blacklists" von E-Mail-Adressen und IP-Adressen anzulegen.





### Einstellung der "Whitelist" / "Blacklist" mit E-Mail-Absenderadressen

➔ Um die "Whitelist" / "Blacklist" mit E-Mail-Absenderadressen einzustellen, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Serverschutz**.
3. Öffnen Sie in der Registerkarte **Schutz für Hub Transport Role** den Einstellungsblock **Einstellungen "Whitelist" und "Blacklist" von Anti-Spam**.
4. Markieren Sie das Kontrollkästchen **Absenderadresse in "Whitelist" / "Blacklist" übernehmen**.
5. Um eine E-Mail-Adresse in die Liste einzufügen, gehen Sie wie folgt vor:
  - a. Geben Sie im Eingabefeld die E-Mail-Adresse ein. Sie können eine einzelne E-Mail-Adresse oder eine Schablone vom Typ \*@domain.com eingeben, die alle Adressen einer Maildomäne bezeichnet.
  - b. Klicken Sie auf die Schaltfläche .
6. Um eine E-Mail-Adresse aus der Liste zu löschen, wählen Sie die Adresse aus und klicken auf die Schaltfläche .
7. Um die Liste in eine Datei zu exportieren, klicken Sie auf die Schaltfläche .
8. Um die Liste aus einer Datei zu importieren, klicken Sie auf die Schaltfläche .
9. Klicken Sie auf die Schaltfläche **Speichern**.

## Einstellung der "Whitelist" / "Blacklist" mit IP-Absenderadressen

➤ Um die "Whitelist" / "Blacklist" mit IP-Absenderadressen einzustellen, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Serverschutz**.
3. Öffnen Sie in der Registerkarte **Schutz für Hub Transport Role** den Einstellungsblock **Einstellungen "Whitelist" und "Blacklist" von Anti-Spam**.
4. Markieren Sie das Kontrollkästchen **Absenderadresse in "Whitelist" / "Blacklist" für IP-Adressen übernehmen**.
5. Um eine IP-Adresse in die Liste einzufügen, gehen Sie wie folgt vor:
  - a. Geben Sie im Eingabefeld die IP-Adresse ein. Sie können eine einzelne IP-Adresse oder einen IP-Adressbereich in CIDR-Schreibweise angeben (Form XXX.XXX.XXX.XXX/YY).
  - b. Klicken Sie auf die Schaltfläche .
6. Um eine IP-Adresse aus der Liste zu löschen, wählen Sie diese aus und klicken auf die Schaltfläche .
7. Um die Liste in eine Datei zu exportieren, klicken Sie auf die Schaltfläche .
8. Um die Liste aus einer Datei zu importieren, klicken Sie auf die Schaltfläche .
9. Klicken Sie auf die Schaltfläche **Speichern**.

## EINSTELLUNG DER "WHITELIST" FÜR E-MAIL-EMPFÄNGER

Sie können eine "Whitelist" für Empfänger einstellen, indem Sie in diese die Adressen von E-Mail-Empfängern hinzufügen bzw. diese löschen. Die Nachrichten für die Empfänger, die in diese Liste beigefügt sind, werden auf die Spam nicht geprüft werden. Standardmäßig ist die "Whitelist" leer.

Sie können in die "Whitelist" die Empfängeradressen in folgenden Formen ergänzen:

- Active Directory Objekte:
  - Einfache Benutzer (User).
  - Kontakte (Contact).
  - Verbreitungsgruppe (Distribution Group).
  - Sicherheitsgruppe (Security Group).

Es ist empfehlenswert, Adressen in die "Whitelist" in Form von Active Directory Objekten zu ergänzen.

- SMTP-Adresse als mailbox@domain.com. Einträge dieses Typs sind notwendig, wenn die auszuschließende Adresse nicht in Active Directory gefunden werden kann.


Um einen öffentlichen Ordner (Public Folder) aus der Spam-Prüfung auszuschließen, fügen Sie alle SMTP-Adressen des Ordners zur weißen Liste hinzu, falls es mehrere SMTP-Adressen vorhanden sind. Wenn einige SMTP-Adressen des öffentlichen Ordners in der Liste nicht vorhanden sind, können die in den öffentlichen Ordner eingehenden E-Mails untersucht werden.

Empfängeradressen, die als Active Directory Objekte angegeben sind, werden aus der Spam-Prüfung gemäß den folgenden Regeln ausgeschlossen:





- Wenn die Empfängeradresse die Form eines einfachen Benutzer oder eines Kontaktes hat, werden die daran adressierten E-Mails aus der Prüfung ausgeschlossen.
- Wenn die Adresse in Form einer Verbreitungsgruppe eingetragen ist, werden E-Mails, die an diese Gruppe adressiert sind, aus der Prüfung ausgeschlossen. Jedoch werden E-Mails, die persönlich an Mitglieder der Verbreitungsgruppe adressiert sind, nicht aus der Prüfung ausgeschlossen, wenn diese nicht einzeln in die Liste eingetragen wurden.
- Wenn die Adresse in Form einer Sicherheitsgruppe eingetragen ist, werden E-Mails, die an diese Gruppe sowie Mitglieder dieser Gruppe adressiert sind, aus der Prüfung ausgeschlossen. Jedoch, wenn eine Sicherheitsgruppe ein eingebundenes Mitglied einer Verbreitungsgruppe ist, werden E-Mails, die an deren Mitglieder adressiert sind, nicht aus der Prüfung ausgeschlossen, wenn die Mitglieder nicht einzeln in die Liste eingetragen wurden.

Das Programm erneuert automatisch die aus Active Directory erhaltenen Empfängeradressen bei Veränderung der entsprechenden Einträge in Active Directory (zum Beispiel, wenn sich die E-Mail-Adresse eines Benutzers geändert hat oder wenn einer Sicherheitsgruppe ein neuer Teilnehmer hinzugefügt wurde). Die Erneuerung wird einmal pro Tag durchgeführt.

➔ Um die "Whitelist" der Empfänger einzustellen, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Serverschutz**.
3. Öffnen Sie in der Registerkarte **Schutz für Hub Transport Role** den Einstellungsblock **Einstellungen "Whitelist" und "Blacklist" von Anti-Spam**.
4. Markieren Sie das Kontrollkästchen **Empfängeradresse in "Whitelist" übernehmen**.
5. Um eine Empfängeradresse in die Liste einzufügen, nehmen Sie eine der folgenden Handlungen vor:
  - Um den Eintrag zur Liste aus Active Directory hinzuzufügen, betätigen die Schaltfläche . Finden Sie im sich öffnenden Fenster den gewünschten Active Directory Eintrag und betätigen Sie die Schaltfläche **OK**.



Die aus Active Directory übernommenen Adressen werden in der Liste durch folgende Icons gekennzeichnet:

-  – einfache Benutzer, Kontakte, Verbreitungsgruppe;
-  – Sicherheitsgruppe.
- Um eine SMTP-Adresse oder einen öffentlichen Ordner in die Liste einzutragen, gehen Sie wie folgt vor:
  - Um eine SMTP-Adresse einzutragen, geben Sie diese im Eingabefeld ein und klicken auf die Schaltfläche .
  - Um einen öffentlichen Ordner einzutragen, geben Sie den Pfad zum Ordner ein und klicken auf die Schaltfläche .

Die Adressen, die auf diese Weise hinzugefügt wurden, sind durch das Icon  gekennzeichnet.

Adressen, die auf diese Weise hinzugefügt wurden, werden nicht auf das Vorhandensein in Active Directory geprüft.

6. Um Einträge aus der Liste zu löschen, wählen Sie diese aus und klicken auf die Schaltfläche .

7. Um die Liste in eine Datei zu exportieren, klicken Sie auf die Schaltfläche .
8. Um die Liste aus einer Datei zu importieren, klicken Sie auf die Schaltfläche .
9. Klicken Sie auf die Schaltfläche **Speichern**.

## KONFIGURIERUNG DER EINSTELLUNGEN ZUR ERMITTLUNG DES SPAM-RATINGS

Sie können die Parameter der Anti-Spam, die die Bestimmung der speziellen Charakteristik der Nachrichten beeinflussen - der Spam-Ratings, konfigurieren. Diese Parameter lassen zu, die Vergrößerung der Spam-Ratings der Nachrichten als Ergebnis der Analyse des Absenders und des Themas der Nachrichten zu konfigurieren, sowie, wenn die Nachricht auf der Fremdsprache geschrieben ist.

► *Um die Vergrößerung der Spam-Ratings der Nachrichten als Ergebnis der Analyse des Absenders zu konfigurieren, erfüllen Sie die folgenden Aktionen:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Serverschutz**.
3. Öffnen Sie in der Registerkarte **Schutz für Hub Transport Role** den Einstellungsblock **Einstellungen zur Ermittlung des Spam-Ratings**.
4. In der Einstellungsgruppe **Spam-Rating erhöhen bei Analyse der Absenderadresse**: markieren Sie die Kästchen für die gewünschten Einstellungen:
  - **Wenn das Feld "An:" keine E-Mail-Adresse enthält**. Ist das Feld "An:" leer, wird das Spam-Rating für die Nachricht heraufgesetzt.
  - **Wenn die Absenderadresse Zahlen enthält**. Wenn die Absenderadresse Zahlen enthält, wird das Spam-Rating für die Nachricht heraufgesetzt.
  - **Falls die Absenderadresse (im E-Mail-Körper) keine Domain-Endung enthält**. Wenn die Absenderadresse keinen Domainnamen enthält, wird das Spam-Rating für die Nachricht heraufgesetzt.
5. Klicken Sie auf die Schaltfläche **Speichern**.

► *Um das Spam-Rating einer Nachricht nach Analyse des Betreffs von Nachrichten heraufzusetzen, gehen Sie wie folgt vor:*

1. Öffnen Sie in der Registerkarte **Schutz für Hub Transport Role** den Einstellungsblock **Einstellungen zur Ermittlung des Spam-Ratings**.
2. In der Einstellungsgruppe **Spam-Rating nach Analyse der Absenderadresse heraufsetzen**: markieren Sie die Kästchen für die gewünschten Einstellungen:
  - **Wenn der Betreff der E-Mail mehr als 250 Zeichen enthält**. Wenn der Betreff der E-Mail mehr als 250 Zeichen enthält, wird das Spam-Rating für die Nachricht heraufgesetzt.
  - **Wenn der Betreff der Mitteilung sehr viele Leerzeichen und / oder Punkte enthält**. Wenn der Betreff der Mitteilung sehr viele Leerzeichen und / oder Punkte enthält, wird das Spam-Rating für die Nachricht heraufgesetzt.
  - **Wenn der Betreff der E-Mail einen Zeitstempel enthält**. Wenn der Betreff der E-Mail einen digitalen Identifikation oder einen Zeitstempel enthält, wird das Spam-Rating für die Nachricht heraufgesetzt.
3. Klicken Sie auf die Schaltfläche **Speichern**.









➤ Um das Spam-Rating einer Nachricht nach Analyse der Sprachen von Nachrichten heraufzusetzen, gehen Sie wie folgt vor:

1. Öffnen Sie in der Registerkarte **Schutz für Hub Transport Role** den Einstellungsblock **Einstellungen zur Ermittlung des Spam-Ratings**.
2. Markieren Sie in der Einstellungsgruppe **Spam-Rating erhöhen für Mails in:** die Häkchen für jene Sprachen, die Nachrichten in denen erwarten Sie erwarten nicht zu bekommen:
  - **Chinesisch**, wenn Sie das Erhalten der Nachrichten in Chinesisch nicht erwarten.
  - **Koreanisch**, wenn Sie das Erhalten der Nachrichten in Koreanisch nicht erwarten.
  - **Thailändisch**, wenn Sie das Erhalten der Nachrichten in Thailändisch nicht erwarten.
  - **Japanisch**, wenn Sie das Erhalten der Nachrichten in Japanisch nicht erwarten.
3. Klicken Sie auf die Schaltfläche **Speichern**.

## EXTERNE DIENSTE ZUR SPAMVERARBEITUNG NUTZEN

Kaspersky Security kann externe Dienste zur Spamverarbeitung verwenden. Externe Dienste sind allgemein zugängliche Ressourcen und Dienste im Internet, wie z.B. "Blacklists" für IP-Adressen.

➤ Um externe Dienste zur Überprüfung von IP-Adressen und URL-Hyperlinks zu verwenden, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Serverschutz**.
3. Öffnen Sie in der Registerkarte **Schutz für Hub Transport Role** den Einstellungsblock **Erweiterte Optionen des Spamschutzes**.
4. Setzen Sie das Häkchen, **Externe Dienste zur Überprüfung von IP-Adressen und URL-Hyperlinks für die Spamerkennung verwenden**, wenn Sie möchten, dass bei der Prüfung auf die Spam die Ergebnisse der Arbeit dieser Services berücksichtigt wurden.
5. Markieren Sie in der Einstellungsgruppe **Einstellungen für DNSBL-Dienst einrichten** das Kästchen **Voreingestellte Standard-Blacklist des DNSBL-Dienstes verwenden**, um DNSBL-Dienste (Domain Name System Block List) zur Spamprüfung zu verwenden. DNSBL ist eine Liste von IP-Adressen, die bereits als Versender von Spam bekannt sind.
6. Markieren Sie das Kästchen **Andere Liste aus der Blacklist-Auswahl des DNSBL-Dienstes verwenden**. Wenn Sie diesen Einstellungen aktivieren, wird Ihnen weiter unten vorgeschlagen, eine eigene benutzerdefinierte Liste zu erstellen. Um den Eintrag zur Liste hinzuzufügen, geben Sie den DNS-Servernamen und den Gewichtungsfaktor in die entsprechenden Felder ein, und klicken Sie auf die Schaltfläche . Zum Löschen des Eintrags klicken Sie auf . Zum Export oder Import der Liste verwenden Sie  und .
7. Markieren Sie in der Einstellungsgruppe **Einstellungen für SUBRL-Dienst einrichten** das Kästchen **Voreingestellte Standard-Blacklist des SUBRL-Dienstes verwenden**, um die Standard-Blacklist von SUBRL- (Spam URI Realtime Block List) zur Spamprüfung für E-Mails zu verwenden. SURBL ist eine Liste von Hyperlinks, die zu Werbe-Websites von Spambietern führen. Enthalten E-Mails URLs aus dieser Liste, werden sie als Spam erkannt.
8. Markieren Sie das Kästchen **Andere Liste aus der Blacklist-Auswahl des DNSBL-Dienstes verwenden**. Wenn Sie diesen Einstellungen aktivieren, wird Ihnen weiter unten vorgeschlagen, eine eigene benutzerdefinierte Liste zu erstellen. Um den Eintrag zur Liste hinzuzufügen, geben Sie den DNS-Servernamen und den Gewichtungsfaktor in die entsprechenden Felder ein, und klicken Sie auf die Schaltfläche . Zum Löschen des Eintrags klicken Sie auf die Schaltfläche . Zum Export oder Import der Liste verwenden Sie  und .

9. Um zu prüfen, ob in der Reverse-Zone ein Eintrag für die IP-Adresse des Absenders in der DNS existiert, markieren Sie das Kästchen **Prüfen ob eine IP-Adresse in der DNS vorhanden ist**.
10. Um das SPF-Verfahren (Sender Policy Framework) zu verwenden, setzen Sie das Häkchen **SPF-Verfahren anwenden**.
11. Um eine Absender-IP-Adresse auf Zugehörigkeit zu einem Botnetz zu überprüfen, setzen Sie das Häkchen **Zuordnung der IP-Absenderadresse zur dynamischen DNS überprüfen**. Im Falle eines positiven Ergebnisses der Untersuchung wird das Spam-Rating der Nachricht erhöht.
12. Geben Sie im Eingabefeld mit der Scrollbox die maximale Wartezeit für die Verbindung nach der DNS-Abfrage vor. Bei Verwendung der Standardeinstellungen beträgt das Zeitlimit 10 Sekunden.

## EINSTELLUNGEN FÜR ANTI-SPAM-BERICHTE ANPASSEN

Sie können die zusätzlichen Parameter der Anti-Spam, wie die Beschränkungen der Prüfung nach der Zeit und dem Umfang oder der Möglichkeit der Prüfung der Dateien Microsoft Office anpassen.

- *Um Beschränkung für die Dauer der Prüfung und die Größe der zu prüfenden Objekte festzulegen, gehen Sie wie folgt vor:*
  1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
  2. Wählen Sie den Node **Serverschutz**.
  3. Öffnen Sie in der Registerkarte **Schutz für Hub Transport Role** den Einstellungsblock **Zusätzlichen Parameter der Anti-Spam**.
  4. Geben Sie in der Gruppe **Beschränkungen** im Eingabefeld mit der Scrollbox die **Maximale Zeit zur Überprüfung einzelner E-Mails (Sekunden)** vor. Wenn die benötigte Zeit für die Prüfung diesen Wert überschreitet, wird die Prüfung nicht ausgeführt. Der voreingestellte Standardwert beträgt 30 Sekunden. Solche Objekte erhalten das Verdikt Virenfrees Objekt; wenn jedoch die Dienst-Kopfzeilen aktiviert sind, enthalten diese den Hinweis, dass die maximale Zeit für die Prüfung überschritten wurde.
  5. Geben Sie in der Gruppe **Beschränkungen** im Eingabefeld mit der Scrollbox die **Maximale Größe für einzelne zu prüfende Objekte** vor. Wenn die Größe von Objekten diesen Wert überschreitet, wird die Prüfung nicht ausgeführt. Der voreingestellte Standardwert beträgt 300 KB. Solche Objekte erhalten das Verdikt Virenfrees Objekt. Wenn jedoch die Dienst-Kopfzeilen aktiviert sind, enthalten diese den Hinweis, dass die maximale Zeit für die Prüfung überschritten wurde.
- *Um die Einstellungen der Dokumentenüberprüfung Microsoft Office anzupassen, gehen Sie in Gruppe **Einstellungen der Dokumentenüberprüfung Microsoft Office** wie folgt vor:*
  1. Setzen Sie das Häkchen **Dateien im Format .doc überprüfen**, damit Anti-Spam die Dokumente Microsoft Word prüfte.
  2. Setzen Sie das Häkchen **Dateien im Format RTF überprüfen**, damit Anti-Spam die Dokumente RTF prüfte.
- *Um zusätzliche Einstellungen anzupassen, gehen Sie in Gruppe **Weitere Einstellungen** wie folgt vor:*
  1. Markieren Sie das Kästchen **Faktor "Potenzieller Spam" verwenden**, wenn das Programm bei spamverdächtigen Objekten das Verdikt Potenzieller Spam zuweisen soll.
  2. Markieren Sie das Kästchen **Analyseverfahren für Bilder verwenden**, wenn Bilddateien in E-Mails mit dem Bildanalyseverfahren GSG geprüft werden sollen. Mit diesem Verfahren wird überprüft, ob Bilddateien in E-Mails Ähnlichkeiten mit den vorhandenen Mustern in der Spamdatenbank aufweisen. Bei Übereinstimmungen wird das Spam-Rating für die betreffenden E-Mails erhöht.

3. Setzen Sie das Häkchen **Modus der Aufbewahrung und Verwendung von Spam-Mustern in der UTF8-Kodierung aktivieren (Update von Anti-Spam-Datenbanken ist erforderlich)**, um die Aufbewahrung und Verwendung von Spam-Mustern in der UTF8-Kodierung zu aktivieren. Durch diesen Modus werden Datenverluste in Muster-Spamobjekten in asiatischen Sprachen vermieden; allerdings erhöht sich unwesentlich die Bearbeitungszeit pro E-Mail. Dieser Modus sollte aktiviert werden, wenn Sie E-Mails in UTF8-Codierung schreiben und empfangen. Um dieses Modul zu aktivieren, müssen Sie zuvor die Anti-Spam-Datenbanken aktualisieren.
4. Markieren Sie das Kästchen **Dienst-Kopfzeilen aktivieren**, wenn die E-Mails zusätzliche x-Kopfzeilen mit Informationen zum Ergebnis der Prüfung erhalten sollen.
5. Markieren Sie das Kästchen **Autorisierte Verbindungen überprüfen**, wenn über vertrauenswürdige Verbindungen (Trusted Connections) eingehende E-Mails auch auf Spam geprüft werden sollen.
6. Markieren Sie das Kästchen **Nachrichten an die Adresse Postmaster nicht auf Spam überprüfen**, wenn E-Mails an die Adresse Postmaster nicht auf Spam geprüft werden sollen.

# BACKUP

Kaspersky Security speichert vor dem Verarbeiten von Objekten Kopien des Basisobjekts im Backup-Ordner.

Objekte aus dem Backup-Ordner können Sie später:

- **auf Datenträgern speichern**, um die Daten in den Objekten weiter zu nutzen. Sie können die Objekte auch wiederherstellen und erneut mit aktualisierten Anti-Viren-Datenbanken prüfen;
- **löschen**;
- **an Kaspersky Lab zur Untersuchung einsenden** (nur für verdächtige Objekte, die Modifikationen bekannter Viren oder noch unbekanntes Virencodes enthalten). Unsere Spezialisten analysieren diese Dateien, werden sich bemühen, ihre Daten zu retten, und aktualisieren beim Auffinden unbekannter Virencodes die entsprechenden Einträge in den Datenbanken. Solche Objekte können dann durch ein Virenschutzprogramm für Dateisysteme (z.B. Kaspersky Anti-Virus für Windows Server) mit aktualisierten Datenbanken desinfiziert und die enthaltenen Daten wiederhergestellt werden;
- **an die Empfänger versenden**. Die gespeicherten Objekte werden an die Empfänger zugestellt.

Backups mit geprüften Objekten werden nur angelegt, wenn in den Virenschutzeinstellungen das entsprechende Häkchen für **Kopie der Ursprungsdatei im Backup-Ordner speichern** gesetzt ist. Von Anti-Spam verarbeitete Objekte werden ebenfalls im Backup-Ordner gespeichert.

Der Backup-Ordner wird in der Datenbank aufgestellt, die bei der Installation des Programms angegeben ist. Wenn einige Sicherheitsserver eine Datenbank verwenden (zum Beispiel, in der Konfiguration mit DAG), werden im Backup-Ordner die Objekte erhalten bleiben, die von jedem dieser Server bekommen sind.

Die Objekte im Backup-Ordner werden als verschlüsselte Kopie gespeichert. Dies bietet folgende Vorteile:

- Das Risiko von Vireninfectionen wird reduziert (auf die verschlüsselten Objekte kann nicht zugegriffen werden);
- Zeiteinsparung bei der Ausführung von Anti-Virus (im Backup-Ordner gespeicherte Dateien werden nicht als infiziert behandelt).

Für die gespeicherte Datenmenge im Backup-Ordner gelten folgende Beschränkungen:

- Es können maximal 1 Million Einzelobjekte gespeichert werden. Diese Vorgabe kann nicht geändert werden.
- Als Benutzer können Sie die Größe des Backup-Ordners und die Aufbewahrungszeit für Objekte weiter einschränken.

Das Programm prüft regelmäßig (Einmal pro Minute), ob diese Beschränkung noch eingehalten werden. Das Programm geht dabei wie folgt vor:

- Wird die zulässige Anzahl der Einzelobjekte im Backup-Ordner überschritten, wird eine entsprechende Zahl von Objekten gelöscht - beginnend mit den ältesten;
- Ist die Größe des Backup-Ordners beschränkt, und der Höchstwert wird durch neu hinzu kommende Objekte überschritten, gibt das Programm den erforderlichen Speicherplatz durch Löschung vorhandener Objekte, beginnend mit den ältesten, Speicherplatz frei;
- Ist die Aufbewahrungsfrist begrenzt, werden die Objekte, deren Aufbewahrungsfrist abgelaufen ist, gelöscht.

Über den Node **Backup** können Sie:

- Den Backup-Ordner anzeigen;
- Die Backup-Kopien der Objekte bearbeiten: Eigenschaften anzeigen, wiederherstellen, versenden an die Empfänger, zur Untersuchung einsenden und löschen.

Für die bequeme Durchsicht und Informationssuche im Backup-Ordner wird eine Option zur Filterung von Backup-Daten (s. Abschnitt "Einstellung der Backup-Ordner-Filter" auf S. [80](#)) vorgesehen.

## IN DIESEM ABSCHNITT

Backup-Ordner anzeigen .....	<a href="#">77</a>
Eigenschaften von Objekten im Backup-Ordner anzeigen .....	<a href="#">79</a>
Einstellung der Backup-Ordner-Filter .....	<a href="#">80</a>
Objekte aus dem Backup-Ordner wiederherstellen .....	<a href="#">81</a>
Objekt aus dem Backup an die Empfänger versenden .....	<a href="#">81</a>
Entsendung des Objektes aus dem Backup-Ordner zur Untersuchung .....	<a href="#">82</a>
Objekte aus dem Backup-Ordner wiederherstellen .....	<a href="#">82</a>
Einstellungen für Backup-Ordner anpassen .....	<a href="#">83</a>

## BACKUP-ORDNER ANZEIGEN

Im Backup-Ordner können Sie sich eine Liste aller gespeicherten Objekte als Tabelle mit Spaltenüberschriften anzeigen lassen. Jede Spalte enthält bestimmte Informationen zu den betreffenden Objekten. Im Detailfenster links unten können Sie sehen, wieviele Objekte sich insgesamt im Backup-Ordner befinden und wieviel Speicherplatz auf der Festplatte belegt wird.

➔ *Um Informationen zum Inhalt des Backup-Ordners anzuzeigen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Backup**.

Im Detailfenster wird eine Liste der im Backup-Ordner gespeicherten Kopien von Objekten angezeigt (s. Abb. unten).

Standardmäßig werden folgende Eigenschaften für die im Backup-Ordner gespeicherten Objekte angezeigt:

- **Von.** Absenderadresse der Nachricht.
- **An.** Empfängeradresse der Nachricht.
- **Betreff.** Betreff der Nachricht.
- **Verdikt.** Status der Nachricht.

- **Eingangszeitpunkt:** Genaue Zeit des Eingangs auf dem Microsoft Exchange-Server.

Kaspersky Security 8.0  
für Microsoft Exchange Server
KASPERSKY

Backup

Wörter suchen

Geben Sie eine Suchanfrage ein

Suchen

Von	An	Betreff	Verdict	Eingangszeitpunkt
exadmin@e7sp2.local	exadmin@e7sp2.local	Warning EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	simple EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Suspicious EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	simple EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Warning EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Suspicious EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Warning EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Suspicious EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	simple EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	simple EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Warning EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Suspicious EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Suspicious EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	simple EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Warning EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	simple EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Warning EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	simple EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Warning EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	simple EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Suspicious EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Suspicious EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Warning EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Suspicious EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Warning EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	simple EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Warning EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	Suspicious EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	simple EICAR	Desinfiziert	21.10.2011 12:49
exadmin@e7sp2.local	exadmin@e7sp2.local	simple EICAR	Desinfiziert	21.10.2011 12:49

Löschen

Erweitert ▲

Angezeigt 481 - 510 aus 6378

<<

<

17

>

>>

Objekte auf Datenträger insgesamt 6378 mit einer Größe von 24,9 MB

Spalten hinzufügen/löschen

Alle löschen

Abbildung 5. Backup-Ordner anzeigen

Sie können die Ansicht für das Detailfenster anpassen, den Satz und die Ordnung der Abbildung der Rubriken der Tabelle ändernd.

➔ Um die Ansicht für das Detailfenster anzupassen, gehen Sie wie folgt vor:

1. Um weitere Spalten hinzuzufügen, klicken Sie auf die Schaltfläche **Spalten hinzufügen / löschen**.
2. Markieren Sie in dem sich öffnenden Fenster die Datentypen, die im Detailfenster angezeigt werden sollen. Entfernen Sie die Häkchen für die Datentypen, die im Detailfenster nicht angezeigt werden sollen.

In der Tabelle können Sie die Daten nach jeder Spalte auf- oder absteigend sortieren. Klicken Sie dazu auf einen der Spaltenköpfe, z.B. **Von**, **Ann**, **Betreff**.

78

Im Detailfenster kann nur eine bestimmte Anzahl Objekte angezeigt werden. Um andere Objekte anzuzeigen, verwenden Sie die Navigationsschaltflächen im Detailfenster unten rechts. Zwischen den beiden Navigationsschaltflächenpaaren wird die Nummer des aktuellen Fensters angezeigt. Um zum nächsten Fenster zu wechseln, klicken Sie auf die Schaltfläche >. Um zum vorherigen Fenster zu wechseln, klicken Sie auf die Schaltfläche <. Um zum letzten Fenster zu wechseln, klicken Sie auf die Schaltfläche >>. Um zum ersten Fenster zu wechseln, klicken Sie auf die Schaltfläche <<.

## EIGENSCHAFTEN VON OBJEKTEN IM BACKUP-ORDNER ANZEIGEN

➤ Um die Eigenschaften des Objektes, das in den Backup-Ordner unterbracht ist, durchzusehen, gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Backup**.
3. Wählen Sie im Detailfenster das gewünschte Objekt im Backup-Ordner.
4. Klicken Sie auf die Schaltfläche **Eigenschaften**. Wenn im Detailfenster nicht genügend Platz ist, um die Schaltfläche **Eigenschaften** anzuzeigen, klicken Sie auf die Schaltfläche **Erweitert** und wählen Sie im Menü den Punkt **Eigenschaften**.

Das Fenster **Eigenschaften der E-Mail** wird geöffnet. Unter Eigenschaften werden folgenden Daten angezeigt:

- **Virus**. Enthält die E-Mail einen Virus, wird in diesem Feld dessen Name angezeigt.
- **Objekttyp**. Objekttyp: Nachricht oder Anlage.
- **Von**. Absenderadresse.
- **An**. Empfängeradresse der Nachricht.
- **CC**: Empfängeradresse der Kopie der Nachricht.
- **Größe auf Datenträger**. Belegter Speicherplatz für die E-Mail auf dem Datenträger.
- **Betreff**. Betreff der Nachricht.
- **Pfad**. Speicherpfad für das Objekt.
- **Servername**. Servername, durch die das Objekt ins Backup verschoben wurde.
- **Name des virtuellen Servers**. Name des virtuellen Servers. Nur für Cluster-Konfiguration Microsoft Exchange.
- **Cluster-Name**. Cluster-Name. Nur für Cluster-Konfiguration Microsoft Exchange.
- **Eingangszeitpunkt**:. Genauer Eingangszeitpunkt der E-Mail (Datum, Monat, Jahr, Stunden, Minuten).
- **Erstellungsdatum der E-Mail**. Genauer Erstellungszeitpunkt der E-Mail (Datum, Monat, Jahr, Stunden, Minuten).
- **Erscheinungsdatum der Datenbanken**. Erscheinungsdatum der Datenbanken.
- **Verdikt**. Das Verdikt, das dem Objekt vom Programm verliehen ist.
- **Größe**. Größe des Objektes (Byte).

Sie können mehrere Objekte gleichzeitig auswählen und deren Eigenschaften anzeigen. Markieren Sie die Objekte und klicken Sie auf Schaltfläche **Eigenschaften**. Wenn im Detailfenster nicht genügend Platz ist, um die Schaltfläche **Eigenschaften** anzuzeigen, klicken Sie auf die Schaltfläche **Erweitert** und wählen Sie im Menü den Punkt **Eigenschaften**. In dem sich öffnenden Fenster **Eigenschaften der markierten Objekte** können Sie die Verdikte der markierten Objekte anzeigen.

## EINSTELLUNG DER BACKUP-ORDNER-FILTER

Mithilfe von Filtern können Sie im Backup-Ordner Daten suchen und strukturieren. Durch Setzen von Filtern (s. Abb. unten) werden nur Daten angezeigt, die den gewählten Filterkriterien entsprechen. Diese Möglichkeit ist nützlich, wenn im Backup-Ordner die große Menge der Objekte bewahrt wird. Mithilfe von Filtern können Sie z.B. nach Objekten suchen, die Sie wiederherstellen möchten.

Kaspersky Security 8.0  
für Microsoft Exchange Server

**Backup**

Benutzerdefinierter Filter | Eingangszeitpunkt | mindestens | 22.10.2011 | 00:00 | Löschen

Benutzerdefinierter Filter | Objekttyp | gleich | Anlage | Löschen

Wörter suchen | Geben Sie eine Suchanfrage ein | Suchen

An	Betreff	Verdikt	Eingangszeitpunkt
exadmin	simple EICAR	Desinfiziert	23.10.2011 12:43
exadmin	simple EICAR	Desinfiziert	23.10.2011 12:43
exadmin	Suspicious EICAR	Desinfiziert	23.10.2011 12:43
exadmin	simple EICAR	Desinfiziert	23.10.2011 12:43
exadmin	Warning EICAR	Desinfiziert	24.10.2011 12:35
exadmin	Suspicious EICAR	Desinfiziert	24.10.2011 12:35
exadmin	Suspicious EICAR	Desinfiziert	24.10.2011 12:35
exadmin	simple EICAR	Desinfiziert	24.10.2011 12:35
exadmin	Warning EICAR	Desinfiziert	24.10.2011 12:35
exadmin	Warning EICAR	Desinfiziert	24.10.2011 12:35
exadmin	simple EICAR	Desinfiziert	24.10.2011 12:35
exadmin	Suspicious EICAR	Desinfiziert	24.10.2011 12:35

Löschen | Eigenschaften | Erweitert ▲ | Angezeigt 1 - 13 aus 168 | << | < | 1 | > | >>

Objekte auf Datenträger insgesamt 6378 mit einer Größe von 24,9 MB  
Gefiltert 168 Objekte mit einem Gesamtvolumen von 672,0 KB

Spalten hinzufügen/löschen | Alle löschen

Abbildung 6. Einstellung der Backup-Ordner-Filter

➤ Zum Anpassen der Filter für den Backup-Ordner gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Backup**.
3. Wählen Sie im Detailfenster in der Dropdown-Liste das gewünschte Filterkriterium für die Objekte des Backup-Ordners. Sie können folgende Kriterien auswählen:
  - **Nur Spam**. In diesem Fall werden im Detailfenster nur E-Mails mit dem Verdikt "Spam" angezeigt.
  - **Nur Viren**. In diesem Fall werden im Detailfenster nur virenverseuchte E-Mails oder E-Mail mit Viren im Text oder in den Anlagen angezeigt.

- **Stichwortsuche.** Geben Sie bei dieser Variante im Eingabefeld die Stichwörter ein, nach denen Nachrichten gesucht werden soll. Die Suche wird in den Rubriken **Von**, **Wem** und **Betreff** erfüllt werden.
  - **Benutzerdefinierte Filter.** Wählen Sie In diesem Fall ein Kriterium für den neuen Filter in der Dropdown-Liste, geben Sie eine Bedingung für den Wert des Filterkriteriums vor, z.B. **ist gleich** oder **ungleich**), und geben Sie einen Wert ein. Für die Kriterien **Erstellungsdatum der E-Mail**, **Eingangszeitpunkt** und **Erscheinungsdatum der Datenbanken** geben Sie die gewünschten Werte über den Kalender ein. Für das Kriterium **Verdikt** Wählen Sie das gewünschte Kriterium in der Dropdown-Liste aus. Für alle anderen Kriterien geben Sie den Wert Manuell im Eingabefeld ein.
4. Klicken Sie auf die Schaltfläche **Suchen**. Der verwendete Filter wird oben die Fenster der Ergebnisse dargestellt werden, und im Fenster werden die Objekte, die den Kriterien der Suche antworten, dargestellt sein.
  5. Um einen Filter zu löschen, klicken Sie auf die Schaltfläche **Löschen** rechts neben dem Filter.

Nach der Verwendung der Filter ebenso können Sie die Daten nach jeder Spalte auf- oder absteigend sortieren. Klicken Sie dazu auf einen der Spaltenköpfe, z.B. **Von**, **Ann**, **Betreff**.

## OBJEKTE AUS DEM BACKUP-ORDNER WIEDERHERSTELLEN

Wiederhergestellte Objekte aus dem Backup-Ordner können zu Virenbefall auf Ihrem Computer führen.

➤ *Um Objekte aus dem Backup-Ordner wiederherzustellen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Backup**.
3. Wählen Sie im Detailfenster das Objekt, das Sie wiederherstellen möchten.
4. Klicken Sie auf die Schaltfläche **Speichern auf Datenträger**. Wenn im Detailfenster nicht genügend Platz ist, um die Schaltfläche **Speichern auf Datenträger** anzuzeigen, klicken Sie auf die Schaltfläche **Erweitert** und wählen Sie im Menü den Punkt **Speichern auf Datenträger**.
5. Geben Sie in dem sich öffnenden Fenster den Ordner ein, in dem das wiederhergestellte Objekt gespeichert werden soll, und geben Sie, falls nötig, den Namen für das Objekt ein, oder ändern Sie ihn.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Das Objekt wird entschlüsselt und eine Kopie unter dem gewählten Namen im gewählten Ordner gespeichert. Wiederhergestellte Objekte haben dasselbe Format, wie die ehemaligen Ursprungsobjekte. Nach erfolgreicher Wiederherstellung von Objekten erscheint eine entsprechende Bildschirmmeldung: "Das gewählte Objekt ist auf Datenträger gespeichert".

## OBJEKT AUS DEM BACKUP AN DIE EMPFÄNGER VERSENDEN

Auch können Sie eine Kopie der im Backup-Ordner gespeicherten Objekte an die vorgesehenen Empfänger versenden.

➤ *Um Objekte aus dem Backup-Ordner den Empfänger zu senden, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Backup**.

3. Wählen Sie im Detailfenster das Objekt, das Sie den Empfänger versenden möchten.
4. Klicken Sie auf die Schaltfläche **den Empfänger versenden**. Wenn im Detailfenster nicht genügend Platz ist, um die Schaltfläche **den Empfänger versenden** anzuzeigen, klicken Sie auf die Schaltfläche **Erweitern** und wählen Sie im Menü den Punkt **den Empfänger versenden**.

Das gewählte Objekt wird den Empfänger der Ausgangsmitteilung abgesandt sein.

## ENTSENDUNG DES OBJEKTES AUS DEM BACKUP-ORDNER ZUR UNTERSUCHUNG

Sie können nur Objekte mit dem Status "Verdächtig" an Kaspersky Lab zur Untersuchung einsenden. Vor dem Objektversand zur Untersuchung soll man allgemeine Benachrichtigungseinstellungen einstellen (s. Abschnitt "Benachrichtigungseinstellungen anpassen" auf S. [84](#)).

➔ *Um Objekte zur Untersuchung einzusenden, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Backup**.
3. Wählen Sie ein Objekt mit dem Status **Verdächtig** in der Tabelle aus, in welcher der Inhalt des Verzeichnisses angezeigt wird. Für die Objektsuche kann man den Filter verwenden (s. Abschnitt "Einstellung der Backup-Ordner-Filter" auf S. [80](#)).
4. Wählen Sie im Kontextmenü des Objekts den Befehl **Datei zur Untersuchung einsenden**.

Auf dem Computer, auf dem der verwaltete Sicherheitsserver installiert ist, wird daraufhin automatisch eine E-Mail mit der verdächtigen Datei im Anhang erstellt und an Kaspersky Lab eingesandt. Das Objekt wird in verschlüsselter Form versandt und deshalb nicht noch einmal von Kaspersky Security beanstandet. Nach Versand der E-Mail erscheint auf dem Bildschirm des Computers, von dem die Steuerung erfolgt, eine entsprechende Versandmeldung.

## OBJEKTE AUS DEM BACKUP-ORDNER WIEDERHERSTELLEN

Hierbei werden aus dem Backup-Ordner folgende Objekte gelöscht:

- Die ältesten Objekte, falls durch Hinzufügen neuerer Objekte die erlaubte maximale Anzahl gespeicherter Objekte im Backup-Ordner (in der vorliegenden Programmversion 1 Million) überschritten wird.
- Die ältesten Objekte, falls durch Hinzufügen neuerer Objekte ein vorgegebener Maximalwert für die Größe des Backup-Ordners auf dem Datenträger überschritten wird.
- Objekte, deren Aufbewahrungsfrist abgelaufen ist, sofern eine maximale Aufbewahrungsdauer vorgegeben wurde.

Objekte aus dem Backup-Ordner können auch manuell gelöscht werden. Dies kann nützlich sein, wenn Sie z.B. Objekte erfolgreich wiederhergestellt und zur Untersuchung an Kaspersky Lab eingesandt haben, oder auch, um das Löschen von Objekten zu erzwingen.

➔ *Um Objekte aus dem Backup-Ordner zu löschen, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Backup**.

3. Wählen Sie im Detailfenster das/die zu löschende(n) Objekt(e) aus. Für die Objekten suchen kann man den Filter verwenden (s. Abschnitt "Einstellung der Backup-Ordner-Filter" auf S. [80](#)).
4. Betätigen Sie die Schaltfläche **Löschen** und in dem sich öffnenden Fenster betätigen auf die Schaltfläche **Ja**.

Die gewählte Objekte werden aus dem Backup-Ordner gelöscht.

5. Um alle Objekte zu löschen, klicken Sie auf die Schaltfläche **Alle löschen** und in dem sich öffnenden Fenster betätigen auf die Schaltfläche **Ja**.

Wenn zum Backup-Ordner die Filter verwendet waren, werden aus dem Backup-Ordner nur die Objekte, die den Kriterien der Filter entsprechen, entfernt sein. Wenn zum Backup-Ordner die Filter nicht verwendet waren, werden aus dem Backup-Ordner alle Objekte entfernt sein.

## EINSTELLUNGEN FÜR BACKUP-ORDNER ANPASSEN

Der Backup-Ordner wird während der Installation der Komponente Sicherheitsserver angelegt. Für die Einstellungen werden Standardwerte voreingestellt, die durch den Administrator geändert werden können.

➔ *Um die Einstellungen des Backup-Ordners anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Einstellungen**.
3. Markieren Sie das Kästchen **Daten aufbewahren** im Detailfenster in der Einstellungsgruppe **Größe des Backup-Ordners einschränken**.
4. Geben Sie im Eingabefeld mit der Scrollbox **Maximale Größe des Backup-Ordners** den gewünschten Maximalwert ein. Grundeinstellung ist 5120 MB.
5. Markieren Sie das Kästchen **Aufbewahrungsdauer für Objekte im Backup-Ordner einschränken**, und geben Sie im Eingabefeld mit der Scrollbox **Objekte maximal aufbewahren für** die gewünschte Frist in Tagen ein. Grundeinstellung ist 30 Tage.

Wenn kein einziges Häkchen gesetzt ist, gilt nur die Beschränkung für die Anzahl der im Backup gespeicherten Objekte (nicht mehr als eine Million). Um die Änderungen zu übernehmen, klicken Sie auf die Schaltfläche **Speichern**.

Unabhängig von der Konfiguration des installierten Programms (ein einzelner Server, ein Cluster von Servern oder DAG) sind die Parameter des Backups autonom für jeden physischen Server. Sie müssen einzeln auf jedem physischen Server konfiguriert werden.

# BENACHRICHTIGUNGEN

In Kaspersky Security können Sie Benachrichtigungen zu während der Prüfung gefundenen infizierten, geschützten und beschädigten Objekten versenden.

Es gibt folgende Möglichkeiten für Benachrichtigungen:

- Versand per E-Mail. Hierzu müssen Sie die allgemeinen Einstellungen zum Versand von Benachrichtigungen anpassen.
- Eintrag für Ereignisse im Systemjournal von Microsoft Windows auf dem Computer, auf dem der Sicherheitsserver installiert ist. In diesem Fall erfolgt der Zugriff auf die Daten mithilfe des Standardtools zum Anzeigen und Verwalten von Journalen unter Windows – **Ereignisse anzeigen**.

Sie können die Versand der Mitteilungen über die infizierten, geschützten und beschädigten Objekte auf die Adressen E-Mail des Absenders der Mitteilung, des Empfängers der Mitteilung, des Verwalters, sowie auf die zusätzlichen Adressen E-Mail, zum Beispiel, die Mitarbeiter des Sicherheitsdienstes einstellen.

## IN DIESEM ABSCHNITT

---

Benachrichtigungseinstellungen anpassen .....	<a href="#">84</a>
Versandeinstellungen für Benachrichtigungen anpassen .....	<a href="#">85</a>

## BENACHRICHTIGUNGSEINSTELLUNGEN ANPASSEN

➤ *Zum Einrichten der Benachrichtigungseinstellungen gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Benachrichtigungen**. Im Detailfenster können Sie Benachrichtigungen für folgende Objekttypen einrichten:
  - Infizierte Objekte. Um Benachrichtigungen zu infizierten Objekten einzurichten, expandieren Sie den Einstellungsblock **Benachrichtigen Bei infizierten Objekten**.
  - Beschädigte Objekte. Um Benachrichtigungen zu infizierten Objekten einzurichten, expandieren Sie den Einstellungsblock **Benachrichtigen bei infizierten Objekten**.
  - Geschützte Objekte. Um Benachrichtigungen zu geschützten Objekten einzurichten, expandieren Sie den Einstellungsblock **Benachrichtigen bei geschützten Objekten**.
  - Systemfehler. Um Benachrichtigungen zu Systemfehlern einzurichten, expandieren Sie den Einstellungsblock **Benachrichtigen bei Systemfehlern**. Für diesen Objekttyp ist die Benachrichtigung von Empfänger und Absender nicht vorgesehen.
3. Passen Sie die Einstellungen für jeden Objekttyp unter **Benachrichtigen per E-Mail** wie gewünscht an.
4. Markieren Sie das Kästchen **Administrator**, wenn E-Mail-Benachrichtigungen an den Administrator versandt werden sollen.
5. Markieren Sie das Kästchen **Absender**, wenn der Absender der E-Mail benachrichtigt werden soll, in der das Objekt gefunden wurde.
6. Markieren Sie das Kästchen **Empfänger**, wenn der Empfänger der E-Mail benachrichtigt werden soll, in der das Objekt gefunden wurde.

7. Markieren Sie das Kästchen **Folgende Empfänger**, und geben Sie im Eingabefeld die E-Mail-Adresse(n) ein, an die außerdem eine Benachrichtigung versandt werden soll.
8. Damit Ereignisse im Systemjournal von Microsoft Windows eingetragen werden, markieren Sie das Kästchen **Registrieren im Ereignisjournal von Microsoft Windows**.

Wenn das Programm auf DAG der Server Microsoft Exchange arbeitet, die Parameter der Nachrichten, die auf einem der Server eingestellt sind, erstreckt sich automatisch auf die übrigen Server, die in diese DAG eingehen. Auf den übrigen Servern dieses DAG kann man die Parameter der Nachrichten nicht einstellen.

## VERSANDEINSTELLUNGEN FÜR BENACHRICHTIGUNGEN ANPASSEN

➔ Zum Konfigurieren der Benachrichtigungseinstellungen gehen Sie wie folgt vor:

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Benachrichtigungen**.
3. Öffnen Sie das Fenster **Einstellungen für den E-Mail-Versand** im Kontextmenü des Nodes **Benachrichtigungen** oder über den Link **Einstellungen für den E-Mail-Versand** Im Detailfenster.

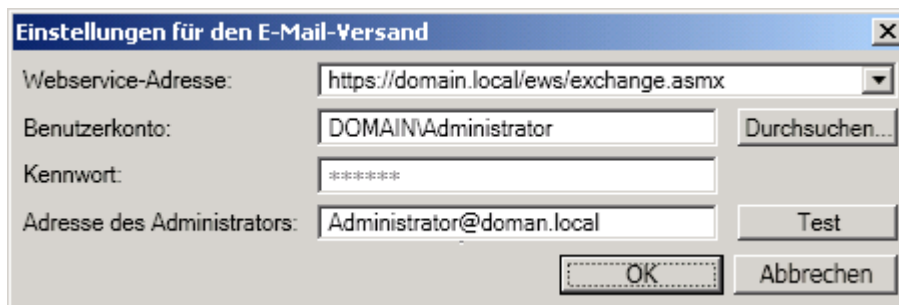


Abbildung 7. Einstellungen für den E-Mail-Versand anpassen

4. Geben Sie im Feld **Webserviceadresse** die Adresse für den verwendeten Webservice zum E-Mail-Versand über Microsoft Exchange Server ein. Standardmäßig ist dies in Microsoft Exchange Server folgende Adresse:  
`https://<Server_name_für_Kunden_zugriff>/ews/exchange.asmx`
5. Geben Sie im Feld **Benutzerkonto** ein beliebiges gewünschtes Benutzerkonto für ein unter Microsoft Exchange Server registriertes Postfach ein.  
 Dafür klicken Sie auf die Schaltfläche **Durchsuchen** und wählen Sie das Benutzerkonto im sich öffnenden Fenster oder führen Sie Name des Benutzerkonto manuell ein.
6. Geben Sie im Feld **Passwort** das Passwort für das gewählte Benutzerkonto ein.
7. Geben Sie im Feld **Adresse Administrator** die Empfängeradresse für Benachrichtigungen ein.
8. Klicken Sie auf die Schaltfläche **Test**, um eine Testnachricht zu versenden.

Kommt die Testnachricht im gewählten Postfach an, sind die Einstellungen für Benachrichtigungen korrekt.

Sie können die Versandeinstellungen für Benachrichtigungen auch über den Einstellungsblock **Benachrichtigungen anpassen** im Node **Einstellungen** einrichten.

Wenn das Programm auf DAG der Server Microsoft Exchange arbeitet, die Parameter der Nachrichten, die auf einem der Server eingestellt sind, erstreckt sich automatisch auf die übrigen Server, die in diese DAG eingehen. Auf den übrigen Servern dieses DAG kann man die Parameter der Nachrichten nicht einstellen.

# BERICHTE

In Kaspersky Security können Sie Berichte zur Ausführung der Komponenten Anti-Virus und Anti-Spam erstellen und anzeigen. In den Berichten finden Sie statistische Daten zur Ausführung des Programms für bestimmte Zeiträume. Für jede Komponente können separate Berichte für Zeiträume von einem Tag bis zu einem Monat angelegt werden.

Es gibt Standard- und Detailberichte. Standardberichte liefern Informationen zur Verarbeitung von Objekten für den Gesamtzeitraum, ohne Angabe zum Zeitabschnitt und genauen Zeitpunkt der Ereignisse. Detailberichte liefern genaue Zeitangaben zu den aufgetretenen Ereignissen. Der kleinstmögliche Erfassungszeitraum für Detailberichte ist eine Stunde.

Berichte können manuell oder automatisch nach einem vorgegebenen Zeitplan erstellt werden. Sie können die Berichte im Programm anzeigen und per E-Mail versenden. Per E-Mail werden Berichte als Datei im Anhang versandt. Die Nachricht enthält folgenden Erläuterungstext:

Die Datei enthält ein Funktionsbericht für Kaspersky Security 8.0 für Microsoft Exchange Server.

Außerdem können Sie Schnellberichte zu sämtlichen Ereignissen für einen benutzerdefinierten Zeitraum erstellen. Schnellberichte können sowohl für Anti-Virus als auch Anti-Spam erstellt werden.

## IN DIESEM ABSCHNITT

---

Die Schnellerstellung eines Berichts .....	<a href="#">86</a>
Einstellungen für Anti-Virus-Berichte anpassen .....	<a href="#">87</a>
Einstellungen für Anti-Spam-Berichte anpassen .....	<a href="#">88</a>
Fertige Berichte anzeigen .....	<a href="#">90</a>

## DIE SCHNELLERSTELLUNG EINES BERICHTS

➔ *Um die Schnellberichte zu schaffen, gehen Sie wie folgt vor:*

1. Wählen Sie in der Konsolenstruktur den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Berichte** und expandieren im Detailfenster den Einstellungsblock **Schnelle Berichte**.
3. Geben Sie im Feld **Berichtsname** einen Namen für den Bericht ein.
4. Wählen Sie in der Dropdown-Liste **Typ** eine der folgenden Varianten:
  - **Antivirus für Mailbox Role**. Es wird ein Bericht über die Ausführung von Anti-Virus für die Mailbox Role erstellt.
  - **Antivirus für Hub Transport Role**. Es wird ein Bericht über die Ausführung von Anti-Virus für die Hub Transport Role erstellt.
  - **Anti-Spam**. Es wird ein Bericht für die Komponente Anti-Spam erstellt.
5. Wählen Sie in der Dropdown-Liste **Genauigkeitsgrad** eine der folgenden Varianten:
  - **Standard**. Der erstellte Bericht liefert Informationen zur Verarbeitung von Objekten für den Gesamtzeitraum, ohne Angabe zum Zeitabschnitt und genauen Zeitpunkt der Ereignisse.

- **Detailliert.** Sie erhalten einen Detailbericht mit genauen Zeitangaben zur Dauer einzelner Ereignisse für den gewählten Berichtszeitraum. Wenn als Berichtszeitraum ein Tag gewählt ist, beträgt das minimale Zeitintervall für jedes Ereignis eine Stunde. Wenn als Berichtszeitraum eine Woche gewählt ist, beträgt das minimale Zeitintervall für jedes Ereignis sechs Stunden. Wenn als Berichtszeitraum ein Monat gewählt ist, beträgt das minimale Zeitintervall für jedes Ereignis einen Tag.
6. Wählen Sie in der Dropdown-Liste **Zeitraum** eine der folgenden Varianten:
    - **pro Tag.** Es wird ein Bericht für die letzten 24 Stunden erstellt.
    - **pro Woche.** Es wird ein Bericht für die letzte Woche erstellt.
    - **pro Monat.** Es wird ein Bericht für den letzten Monat erstellt.
  7. Geben Sie im Feld **Beginnend mit** manuell oder über den Kalender das gewünschte Startdatum des Berichtszeitraums ein.
  8. Wenn Sie möchten, dass der erstellte Bericht per E-Mail abgesandt ist, bezeichnen Sie die Empfänger des Berichtes:
    - a. Wenn Sie möchten, dass der Bericht an die E-Mail-Adresse des Administrators gesendet wird, aktivieren Sie das Häkchen **Administrator**.
    - b. Wenn Sie möchten, dass der Bericht auf die zusätzlichen Adressen E-Mail abgesandt ist, setzen Sie das Häkchen **Folgende Adressaten**, und zählen Sie diese Adressen E-Mail im Feld durch das Komma auf. Um die Richtigkeit des Hinweises der zusätzlichen Adressen E-Mail zu prüfen, senden Sie auf ihnen die Prüfungsmitteilung ab, mit Betätigung auf die Schaltfläche **Test**.  
  
Kommt die Testnachricht im gewählten Postfach an, sind die Einstellungen für den Versand von Berichten korrekt. Falls die Textmeldung nicht erhalten ist, überzeugen Sie sich davon, dass die Einstellungen für den E-Mail-Versand (s. Abschnitt "Versandeeinstellungen für Benachrichtigungen anpassen" auf S. [85](#)) korrekt eingestellt sind.
  9. Um mit diesen Einstellungen einen Schnellbericht zu erstellen, klicken Sie auf die Schaltfläche **Bericht erstellen**.  
  
Im Einstellungsblock **Fertige Berichte** können Sie den neu erstellten Bericht einsehen.
  10. Klicken Sie auf die Schaltfläche **Speichern**, um die Veränderungen zu speichern, die in den Parametern gemacht sind.

## EINSTELLUNGEN FÜR ANTI-VIRUS-BERICHTE ANPASSEN

➔ *Um die Einstellungen für Anti-Virus-Berichte anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Berichte** und expandieren im Detailfenster einer der Einstellungsblock:
  - a. Wenn Sie die Parameter des Antivirusberichtes für Mailbox Rolle konfigurieren können, öffnen Sie den Einstellungsblock **Anti-Virus-Bericht für das Postfach**.
  - b. Wenn Sie die Parameter des Antivirusberichtes für Hub Transporter Rolle konfigurieren können, öffnen Sie den Einstellungsblock **Anti-Virus-Bericht für Hub Transporter Rolle**.
3. Markieren Sie das Kästchen **Bericht automatisch nach Zeitplan erstellen**, wenn die Anti-Virus-Berichte nach einem Zeitplan erstellt werden sollen.

4. Geben Sie im Feld **Berichtsname** einen Namen für den Bericht ein.
5. Wählen Sie in der Dropdown-Liste **Genauigkeitsgrad** eine der folgenden Varianten:
  - **Standard.** Der erstellte Bericht liefert Informationen zur Verarbeitung von Objekten für den Gesamtzeitraum, ohne Angabe zum Zeitabschnitt und genauen Zeitpunkt der Ereignisse.
  - **Detailliert.** Sie erhalten einen Detailbericht mit genauen Zeitangaben zur Dauer einzelner Ereignisse für den gewählten Berichtszeitraum. Wenn als Berichtszeitraum ein Tag gewählt ist, beträgt das minimale Zeitintervall für jedes Ereignis eine Stunde. Wenn als Berichtszeitraum eine Woche gewählt ist, beträgt das minimale Zeitintervall für jedes Ereignis sechs Stunden. Wenn als Berichtszeitraum ein Monat gewählt ist, beträgt das minimale Zeitintervall für jedes Ereignis einen Tag.
6. Wählen Sie in der Dropdown-Liste **Zeitplan für Berichte** eine der folgenden Varianten:
  - **Täglich.** Geben Sie bei dieser Variante im Eingabefeld die genaue Uhrzeit vor, zu der Berichte erstellt werden sollen.
  - **Wöchentlich.** Geben Sie bei dieser Variante in der Dropdown-Liste den Wochentag vor, zu dem Berichte erstellt werden sollen. Geben Sie im Eingabefeld die genaue Uhrzeit vor.
  - **Monatlich.** Geben Sie bei dieser Variante den Tag des Monats vor, zu dem die Berichte erstellt werden sollen. Geben Sie im Eingabefeld die genaue Uhrzeit vor.
7. Wenn Sie möchten, dass der erstellte Bericht per E-Mail abgesandt ist, bezeichnen Sie die Empfänger des Berichtes:
  - a. Wenn Sie möchten, dass der Bericht an die E-Mail-Adresse des Administrators gesendet wird, aktivieren Sie das Häkchen **Administrator**.
  - b. Wenn Sie möchten, dass der Bericht auf die zusätzlichen Adressen E-Mail abgesandt ist, setzen Sie das Häkchen **Folgende Adressaten**, und zählen Sie diese Adressen E-Mail im Feld durch das Komma auf. Um die Richtigkeit des Hinweises der zusätzlichen Adressen E-Mail zu prüfen, senden Sie auf ihnen die Prüfungsmitteilung ab, mit Betätigung auf die Schaltfläche **Test**.
 

Kommt die Testnachricht im gewählten Postfach an, sind die Einstellungen für den Versand von Berichten korrekt. Falls die Textmeldung nicht erhalten ist, überzeugen Sie sich davon, dass die Einstellungen für den E-Mail-Versand (s. Abschnitt "Versandinstellungen für Benachrichtigungen anpassen" auf S. [85](#)) korrekt eingestellt sind.
8. Um mit diesen Einstellungen einen Anti-Virus-Bericht zu erstellen, klicken Sie auf die Schaltfläche **Bericht erstellen**.

Im Einstellungsblock **Fertige Berichte** können Sie den neu erstellten Bericht einsehen.

Der gebildete Bericht wird die Daten für die vergangene Periode enthalten, die um 00:00 der laufenden Tage zu Ende geht. Die Daten für die laufenden Tage im Bericht werden nicht vorgestellt sein.

9. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu übernehmen.

## EINSTELLUNGEN FÜR ANTI-SPAM-BERICHTE ANPASSEN

➔ *Um die Einstellungen für Anti-Spam-Berichte anzupassen, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Berichte**, und expandieren Sie im Detailfenster den Einstellungsblock **Anti-Virus-Bericht**.

3. Markieren Sie das Kästchen **Bericht automatisch nach Zeitplan erstellen**, wenn Anti-Spam-Berichte nach einem Zeitplan erstellt werden sollen.
4. Geben Sie im Feld **Berichtsname** einen Namen für den Bericht ein.
5. Wählen Sie in der Dropdown-Liste **Genauigkeitsgrad** eine der folgenden Varianten:
  - **Standard**. Der erstellte Bericht liefert Informationen zur Verarbeitung von Objekten für den Gesamtzeitraum, ohne Angabe zum Zeitabschnitt und genauen Zeitpunkt der Ereignisse.
  - **Detailliert**. Sie erhalten einen Detailbericht mit genauen Zeitangaben zur Dauer einzelner Ereignisse für den gewählten Berichtszeitraum. Wenn als Berichtszeitraum ein Tag gewählt ist, beträgt das minimale Zeitintervall für jedes Ereignis eine Stunde. Wenn als Berichtszeitraum eine Woche gewählt ist, beträgt das minimale Zeitintervall für jedes Ereignis sechs Stunden. Wenn als Berichtszeitraum ein Monat gewählt ist, beträgt das minimale Zeitintervall für jedes Ereignis einen Tag.
6. Wählen Sie in der Dropdown-Liste **Zeitplan für Berichte** eine der folgenden Varianten:
  - **Täglich**. Geben Sie bei dieser Variante im Eingabefeld die genaue Uhrzeit vor, zu der Berichte erstellt werden sollen.
  - **Wöchentlich**. Geben Sie bei dieser Variante in der Dropdown-Liste den Wochentag vor, zu dem Berichte erstellt werden sollen. Geben Sie im Eingabefeld die genaue Uhrzeit vor.
  - **Monatlich**. Geben Sie bei dieser Variante den Tag des Monats vor, zu dem die Berichte erstellt werden sollen. Geben Sie im Eingabefeld die genaue Uhrzeit vor.
7. Wenn Sie möchten, dass der erstellte Bericht per E-Mail abgesandt ist, bezeichnen Sie die Empfänger des Berichtes:
  - a. Wenn Sie möchten, dass der Bericht an die E-Mail-Adresse des Administrators gesendet wird, aktivieren Sie das Häkchen **Administrator**.
  - b. Wenn Sie möchten, dass der Bericht auf die zusätzlichen Adressen E-Mail abgesandt ist, setzen Sie das Häkchen **Folgende Adressaten**, und zählen Sie diese Adressen E-Mail im Feld durch das Komma auf. Um die Richtigkeit des Hinweises der zusätzlichen Adressen E-Mail zu prüfen, senden Sie auf ihnen die Prüfungsmitteilung ab, mit Betätigung auf die Schaltfläche **Test**.

Kommt die Testnachricht im gewählten Postfach an, sind die Einstellungen für den Versand von Berichten korrekt. Falls die Textmeldung nicht erhalten ist, überzeugen Sie sich davon, dass die Einstellungen für den E-Mail-Versand (s. Abschnitt "Versandeesinstellungen für Benachrichtigungen anpassen" auf S. [85](#)) korrekt eingestellt sind.
8. Um mit diesen Einstellungen einen Bericht für Anti-Spam zu erstellen, klicken Sie auf die Schaltfläche **Bericht erstellen**.
9. Im Einstellungsblock **Fertige Berichte** können Sie den neu erstellten Bericht einsehen.

Der gebildete Bericht wird die Daten für die vergangene Periode enthalten, die um 00:00 der laufenden Tage zu Ende geht. Die Daten für die laufenden Tage im Bericht werden nicht vorgestellt sein.
10. Klicken Sie auf die Schaltfläche **Speichern**, um die Änderungen zu übernehmen.

## FERTIGE BERICHTE ANZEIGEN

Für die richtige Abbildung der Darstellungen in den Berichten ist es empfehlenswert, Microsoft Internet Explorer bis zur Version 8.0 oder höher zu aktualisieren.

➤ *Um die Berichte zur Ausführung der einzelnen Programmkomponenten Anti-Virus und Anti-Spam anzuzeigen, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Berichte** und expandieren im Detailfenster den Einstellungsblock **Fertige Berichte**.

In der Tabelle "Fertige Berichte" können Sie alle bereits erstellten Berichte anzeigen. Jeder Bericht zeigt Ihnen folgende Daten:

- **Name.** Standardname laut Voreinstellung oder benutzerdefinierter Name.
- **Typ.** Berichtstyp: Anti-Spam, Anti-Virus für Mailbox Role oder Anti-Virus für Hub Transport Role.
- **Datum.** Datum der Berichtserstellung.
- **Zeit.** Zeit der Berichtserstellung.

In dieser Rubrik und in den Fenstern der Durchsicht der Berichte wird die lokale Zeit entsprechend der Region, das in den Parametern des Computers, auf dem die Management-Konsole gestartet ist, eingestellt ist, dargestellt.

- **Genauigkeitsgrad.** Standard- oder Detailbericht.
- **Zeitraum.** Vom Bericht erfasster Berichtszeitraum.

3. Um ein bestimmtes Bericht anzuzeigen, markieren Sie es in der Liste, und klicken Sie auf **Anzeigen**.

Kaspersky Security 8.0  
für Microsoft Exchange Server

**Berichte** Speichern Abbrechen

Schnelle Berichte

Anti-Virus-Bericht für das Postfach

Anti-Virus-Bericht für Hub Transport Role

Anti-Spam-Bericht

Fertige Berichte

Name	Typ	Datum	Zeit	Genauigkeitsgrad	Zeitraum
Schneller Bericht - Anti-Virus-Beri	Virenschutz für Hub Transport Role	26.10.2011	16:04:01	Detailliert	14.09.2011 - 13.10.2011
Schneller Bericht - Anti-Virus-Beri	Virenschutz für Hub Transport Role	26.10.2011	16:03:53	Detailliert	26.09.2011 - 25.10.2011
Detailliert - Anti-Virus-Bericht für c	Anti-Virus für Mailbox Role	26.10.2011	16:03:21	Detailliert	25.10.2011 - 25.10.2011
Schneller Bericht - Anti-Spam-Ber	Anti-Spam	26.10.2011	16:03:04	Standard	19.10.2011 - 25.10.2011
Schneller Bericht - Anti-Virus-Beri	Anti-Virus für Mailbox Role	26.10.2011	16:02:54	Standard	26.10.2011 - 26.10.2011

Anzeigen Speichern Löschen

[Einstellungen für den E-Mail-Versand](#)

Abbildung 8. Fertige Berichte anzeigen

## Anti-Virus-Berichte anzeigen

Ein Standardbericht für Anti-Virus enthält folgende Daten in der Kopfzeile:

- Berichtstyp;
- Der Name des Servers, des Clusters oder DAG, für die der Bericht geschaffen ist;
- Vom Bericht erfasster Berichtszeitraum;
- Tag, Monat, Jahr, und Zeit (lokal) der Berichtserstellung.

In der Tabelle zu Standardberichten für den Anti-Virus werden folgende Daten angezeigt:

- **Verdikt.** Status der Objekte nach Verarbeitung durch Anti-Virus.
- **Anzahl Objekte.** Gesamtzahl Objekte nach Verdikten.
- **% der Gesamtmenge.** Gesamtzahl Objekte nach Verdikten in % aller Objekte.
- **Größe.** Größe der Objekte (MB).

Ein Detailbericht für den Anti-Virus enthält folgende Daten in der Kopfzeile:

- Berichtstyp;
- Der Name des Servers, des Clusters oder DAG, für die der Bericht geschaffen ist;
- Vom Bericht erfasster Berichtszeitraum;
- Gesamtzahl Objekte nach Verdikten in % aller Objekte.

In der Tabelle zu Detailberichten für Anti-Virus werden folgende Daten angezeigt:

- **Berichtszeitraum.** Zeitraum, in dem ein Objekt/Objekte gefunden wurde(n).
- **Nicht infizierte Objekte.** Anzahl nicht infizierte Objekte.
- **Desinfizierte Objekte.** Anzahl Objekte, die erfolgreich desinfiziert wurden.
- **Infizierte Objekte.** Anzahl infizierte Objekte.
- **Verdächtige Objekte.** Anzahl Objekte, die eventuell bekannte Viren enthalten.
- **Geschützte Objekte.** Anzahl Passwortgeschützte Objekte, z.B. Archive.
- **Beschädigte Objekte.** Anzahl beschädigter Objekte.
- **Verletzung der Lizenzbedingungen.** Anzahl Objekte, die auf Grund von Verstößen gegen die Lizenzbedingungen für Kaspersky Security nicht geprüft wurden.
- **Fehler in Anti-Viren-Datenbanken.** Die Zahl der Objekte, die wegen des Fehlers nicht geprüft waren, der infolge der unkorrekten Datenbanken entstand.
- **Verarbeitungsfehler.** Die Zahl der Objekte, die wegen der übrigen Fehler nicht geprüft waren.
- **Objekte insgesamt.** Gesamtzahl der empfangenen Objekte.

In den Antivirusberichten für Mailbox Rolle die Informationen über den summarischen Umfang der Objekte in jeder Rubrik enthalten. In der Zeile **Für gesamten Zeitraum** wird die Gesamtzahl aller Objekte im gesamten Berichtszeitraum angezeigt.

### Berichte für Anti-Spam anzeigen

Ein Standardbericht für Anti-Spam enthält folgende Daten in der Kopfzeile:

- Berichtstyp;
- Name des Servers, auf dem der Bericht erstellt wurde;
- Vom Bericht erfasster Berichtszeitraum;
- Gesamtzahl Objekte nach Verdikten in % aller Objekte.

In der Tabelle zu Standardberichten für Anti-Virus werden folgende Daten angezeigt:

- **Verdikt.** Status der Objekte nach Verarbeitung durch Anti-Spam.
- **Anzahl E-Mails.** Gesamtzahl E-Mails nach Verdikten.
- **% der Gesamtmenge.** Gesamtzahl Nachrichten nach Verdikten in % aller Nachrichten.
- **Größe.** Größe der Nachrichten.

Ein Detailbericht für Anti-Spam enthält folgende Daten in der Kopfzeile:

- Berichtstyp;
- Name des Servers, auf dem der Bericht erstellt wurde;
- Vom Bericht erfasster Berichtszeitraum;
- Gesamtzahl Objekte nach Verdikten in % aller Objekte.

In der Tabelle zu Detailberichten für Anti-Spam werden folgende Daten angezeigt:

- **Berichtszeitraum.** Zeitraum, in dem die E-Mails verarbeitet wurden.
- **Spamfrei.** Gesamtzahl Objekte nach Verdikten in % aller Objekte.
- **Vertrauenswürdig.** Anzahl E-Mails von vertrauenswürdigen Absendern.
- **Spam.** Anzahl Spamnachrichten.
- **Potenzieller Spam.** Anzahl wahrscheinlichen Spamnachrichten.
- **Formelle Benachrichtigung.** Anzahl Zustellungsbenachrichtigungen für E-Mails und andere Servicemeldungen.
- **Wurde in "Blacklist" übernommen.** Anzahl Meldungen, Absender-Adressen von denen in "Blacklist" eingetragen sind.
- **Nicht überprüft.** Von Anti-Spam nicht überprüfte Anzahl E-Mails.

Die Anti-Spam-Berichte enthalten die Informationen über den summarischen Umfang der Nachrichten in jeder Rubrik. In der Zeile **Für gesamten Zeitraum** wird die Gesamtzahl aller Objekte im gesamten Berichtszeitraum angezeigt.

# EREIGNISJOURNALE DES PROGRAMMS

In Kaspersky Security können Ereignisse im Journal des Betriebssystems Microsoft Windows und in Journalen des Programms selbst protokolliert werden.

Der Umfang der ins Journal übernommenen Daten richtet sich nach der in der Programmkonfiguration eingestellten Diagnosetiefe.

Die Anzeige der Daten im Ereignisjournal von Microsoft Windows erfolgt mithilfe des Standardtools von unter Windows **Ereignisse anzeigen**. In der Spalte **Quelle** steht für Kaspersky Security die Zeile `KSCM8`.

Ereignisjournale für Kaspersky Security werden in verschiedenen Formaten geführt und haben in Abhängigkeit vom Format eine unterschiedliche Struktur des Dateinamens:

- `kselog.ttmjijij[N].log` ist das Hauptjournal des Programms; N ist hierbei die Nummer des Journals. Eine Journalnummer wird vergeben, wenn während des Rotationszeitraumes mehrere Journale angelegt wurden.
- `anti-Virus_updater_tracelog_ttmjijij[N].log` ist das Updatejournal für die Anti-Viren-Datenbanken.
- `antispam_updater_tracelog_ttmjijij[N].log` ist das Updatejournal für die Anti-Spam-Datenbanken.

Standardmäßig wird für jeden Tag ein neues Journal angelegt. Neue Daten werden immer am Ende des neuesten Ereignisjournals hinzugefügt. Die Standardgröße des Ereignisjournals beträgt 100 MB. Diesen Wert können Sie ändern. Ist diese Maximalgröße erreicht, wird das Journal archiviert und ein neues angelegt.

Die Anzeige von Ereignisjournalen erfolgt mithilfe eines Standardprogramms zur Anzeige von Textdateien (z.B. WordPad).

Journale werden im Ordner Logs aufbewahrt. Dieser Ordner befindet sich auf dem Server im Installationsordner des Programms. Der Pfad für den Installationsordner wird während der Installation festgelegt.

Für jeden Sicherheitsserver entstehen die abgesonderten Journale unabhängig von der Variante der Installation des Programms.

## IN DIESEM ABSCHNITT

Diagnosetiefe anpassen.....	<a href="#">94</a>
Journaleinstellungen anpassen.....	<a href="#">95</a>

## DIAGNOSETIEFE ANPASSEN

Der Umfang der in Journale übernommenen Daten richtet sich nach der in den Programmeinstellungen eingestellten Diagnosetiefe.

➡ *Zum Einrichten der Diagnosetiefe gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Einstellungen**.
3. Wählen Sie im Detailfenster unter **Diagnose** in der Dropdown-Liste **Genauigkeitsgrad** die Option **Minimal**. In diesem Fall enthalten die Journale lediglich einen minimalen Umfang an Informationen.

4. Um die detaillierte Protokollierung für die gewünschten Ereignisse zur Analyse und Beseitigung von Fehlern einzurichten, klicken Sie auf die Schaltfläche **Einstellungen** und markieren Sie im sich öffnenden Fenster **Diagnoseeinstellungen einrichten** die Kästchen für die Module und Ereignisse, die im Detail protokollierte werden sollen.
5. Klicken Sie auf die Schaltfläche **OK** im Fenster **Diagnoseeinstellungen anpassen**. In der Dropdown-Liste **Genauigkeitsgrad** erscheint **Anderer**.

Das Aktivieren der Detailprotokollierung kann die Performance Ihres Computers beeinträchtigen.

6. Klicken Sie auf die Schaltfläche **Speichern** im Detailfenster.

Wenn das Programm auf DAG der Server Microsoft Exchange arbeitet, die Diagnosetiefe, die auf einem der Server eingestellt ist, erstreckt sich automatisch auf die übrigen Server, die in diese DAG eingehen. Auf den übrigen Servern dieses DAG kann man die Diagnosetiefe nicht einstellen.

## JOURNALEINSTELLUNGEN ANPASSEN

➤ *Zum Einrichten der Journaleinstellungen gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Einstellungen**.
3. Wählen Sie im Detailfenster unter **Diagnose** in der Dropdown-Liste **Neue Journaldatei schreiben** den entsprechenden Wert aus:
  - **Täglich**. Es wird jeden Tag ein neues Journal angelegt.
  - **Wöchentlich**. Es wird jede Woche ein neues Journal angelegt.
  - **Monatlich**. Es wird jeden Tag ein neues Journal angelegt.
  - **Wenn die Datei die erlaubte Maximalgröße überschreitet**. Es wird ein neues Journal angelegt, sobald die Journaldatei die erlaubte Maximalgröße überschreitet.
4. Geben Sie für den Einstellungen **Maximale Größe der Datei** im Eingabefeld mit der Scrollbox einen Wert ein. Die maximal erlaubte Größe der Datei beträgt 100 KB.
5. Setzen Sie das Häkchen **Über auftretende Fehler per E-Mail benachrichtigen**, um außer dem Eintragen von angegebenen Ereignissen ins Journal auch Benachrichtigungen von ihnen per E-Mail (s. Abschnitt "Versandeeinstellungen für Benachrichtigungen anpassen" auf S. [85](#)) zu erhalten. Die Benachrichtigungen werden an den Administrator versandt.
6. Klicken Sie auf die Schaltfläche **Speichern**.

Wenn das Programm auf DAG der Server Microsoft Exchange arbeitet, die Parameter der Journale, die auf einem der Server eingestellt sind, erstreckt sich automatisch auf die übrigen Server, die in diese DAG eingehen. Auf den übrigen Servern dieses DAG kann man die Parameter der Journale nicht einstellen.

# KONFIGURATIONSVERWALTUNG

Kaspersky Security ermöglicht den Export der Programmkonfiguration als Datei sowie den Import der Konfiguration aus einer Datei. Die Konfigurationsdatei hat das xml-Format.

## IN DIESEM ABSCHNITT

---

Konfiguration exportieren .....	<a href="#">96</a>
Konfiguration importieren .....	<a href="#">97</a>

## KONFIGURATION EXPORTIEREN

➔ *Um die Programmkonfiguration in eine Datei zu exportieren, gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Einstellungen**.
3. Klicken Sie im Ergebnisfenster im Abschnitt **Konfigurationsverwaltung** auf die Schaltfläche **Exportieren**.  
Es öffnet sich das Fenster **Konfiguration auswählen**.
4. Setzen Sie die Häkchen für die Gruppen der Parameter, die Sie exportieren wollen:
  - **Gesamte Konfiguration**. Alle Parameter des Programms.
  - **Registerkarte Schutz für Hub Transport Role**. Parametergruppe, die sich auf die Komponente Schutz für Hub Transport Role bezieht.
  - **Virenschutz für Mailbox Role**. Parametergruppe, die sich auf die Komponente Virenschutz für Mailbox Role bezieht.
  - **Ausnahmen von der Untersuchung durch Anti-Virus**. Festgelegte Ausnahmen von der Untersuchung durch Anti-Virus.
  - **Updates**. Update-Parameter.
  - **Logging**. Einstellungen für Diagnoseparameter und Ereignisjournale des Programms.
  - **Berichte**. Parameter für Berichte.
  - **Benachrichtigungen**. Benachrichtigungseinstellungen.
  - **Architektur**. Parametergruppe, die folgende Parameter beinhaltet:
    - Parameter der Verbindung zum Microsoft SQL Server: Namen des Servers und der Datenbank;
    - Parameter der Verbindung zum Proxy-Server.
5. Klicken Sie auf die Schaltfläche **OK**.

6. Es öffnet sich das Fenster **Speichern als**.
7. Geben Sie den Dateinamen ein, wählen Sie den Zielordner aus und klicken Sie auf die Schaltfläche **Speichern**.

Die ausgewählten Konfigurationsparameter werden in die Datei gespeichert.

## KONFIGURATION IMPORTIEREN

➔ *Zum Import der Programmkonfiguration aus einer Datei gehen Sie wie folgt vor:*

1. Wählen Sie im Konsolenbaum den Node für den gewünschten Server, und öffnen Sie ihn durch einen Klick auf das Pluszeichen oder Doppelklick auf den Servernamen.
2. Wählen Sie den Node **Einstellungen**.
3. Klicken Sie im Ergebnisfenster im Abschnitt **Konfigurationsverwaltung** auf die Schaltfläche **Importieren**.  
Es öffnet sich das Fenster **Öffnen**.
4. Wählen Sie die Datei mit der Programmkonfiguration und klicken Sie auf die Schaltfläche **Öffnen**. Sie können nur die Dateien mit .kseconfig-Erweiterung wählen.

Die Konfiguration aus der ausgewählten Datei wird importiert. Die in der Datei gespeicherten Parametereinstellungen werden durch die aktuellen Parameterwerte des Programms ohne zusätzliche Bestätigungen ersetzt.

# HÄUFIG GESTELLTE FRAGEN

In diesem Kapitel finden Sie Antworten zu häufig gestellten Fragen der Benutzer von Kaspersky Security 8.0 für Microsoft Exchange Server.

**Frage:** Kann ich das Programm gemeinsam mit Viren- und Spamschutzprogrammen anderer Hersteller nutzen?

Kaspersky Security 8.0 für Microsoft Exchange Server ist ein Programm zum Schutz des E-Mail-Verkehrs vor Viren und Spam im internen Netzwerk Ihres Unternehmens. Daher kann es mit anderen im Netzwerk installierten Virenschutzprogrammen von Kaspersky Lab gemeinsam verwendet werden, die Bestandteil von Kaspersky Open Space Security sind (z.B. Kaspersky Anti-Virus 6.0 für Windows Workstations, Kaspersky Anti-Virus 6.0 für Windows Servers).

Viren- und Spamschutzprogramme anderer Hersteller können auf Microsoft Exchange-Servern in der Hub Transport Rolle oder Edge Transport Rolle gemeinsam mit den Abfangprogrammen von Kaspersky Security für diese Rollen verwendet werden. Dabei steigt die Computerbelastung wesentlich sowie auch die Anforderungen an die Qualifikation des Administrators, welcher die Übereinstimmung der Einstellungen aller Anti-Virus- und Anti-Spam-Programme sichert. Es ist empfehlenswert, Anti-Viren- und die Anti-Spam-Produkte der Fremdproduzenten vor der Installation Kaspersky Security 8.0 für Microsoft Exchange Server zu löschen.

Kaspersky Security 8.0 für Microsoft Exchange Server funktioniert nicht mit Viren- und Spamschutzprogrammen anderer Hersteller auf Microsoft Exchange-Servern in der Mailbox Rolle!

**Frage:** Warum beeinträchtigt das Programm die Performance des Computers und führt zu einer spürbar höheren Belastung für den Prozessor?

Die Suche nach Viren und die Spamfilterung sind rechnerische (mathematische) Operationen, bei welchen Strukturen analysiert, Kontrollsummen berechnet und Daten durch mathematische Verfahren umgewandelt werden. Daher wird für diese Operationen hauptsächlich Prozessorzeit gebraucht. Außerdem verlängert jede in die Datenbanken neu eingetragene Anti-Virus-Definition die Gesamtdauer der Virenprüfung.

Im Unterschied zu anderen Herstellern von Virenschutzprogrammen, die bemüht sind, durch Ausschließen schwer zu findender oder komplizierterer Viren aus den Anti-Viren-Datenbanken (z.B. durch geografische Beschränkung), aber auch durch Ausschließen schwer zu prüfender Dateiformate (z.B. PDF) die Gesamtdauer der Prüfung zu verkürzen, sind wir bei Kaspersky Lab der Meinung, dass die erste Aufgabe eines Virenschutzprogramms der wirkliche und wirksame Schutz des Benutzers vor eindringenden Viren ist.

In Kaspersky Security 8.0 für Microsoft Exchange Server können erfahrene Nutzer die Virensuche und Spamfilterung beschleunigen, indem sie verschiedene Dateitypen von der Prüfung ausschließen. Sie sollten dabei aber nicht vergessen, dass dies auch zu einer geringeren Sicherheit führt.

Kaspersky Security 8.0 für Microsoft Exchange Server erkennt mehr als 700 Formate für archivierte und gepackte Dateien. Dies ist besonders wichtig für den wirksamen Virenschutz, weil jede erkannte Datei in diesen Formaten einen schädlichen Programmcode enthalten kann, der sich nach dem Einpacken archiviert.

**Frage:** Warum brauche ich eine Lizenz für Kaspersky Security? Funktioniert das Programm nicht auch ohne Lizenz?

Kaspersky Security funktioniert nicht ohne Lizenz.

Wenn Sie noch keine lizenzierte Version des Programms erwerben möchten, können Sie eine Testlizenz (Demo) für zwei Wochen oder einen Monat erhalten. Diese wird nach Ablauf der Probezeit automatisch deaktiviert.

**Frage:** Was passiert, wenn die Lizenz für Kaspersky Security abgelaufen ist?

Nach Ablauf der Lizenz können Sie das Programm weiter verwenden. Ein Update der Datenbanken ist jedoch nicht mehr möglich. Kaspersky Security 8.0 für Microsoft Exchange Server prüft weiterhin Ihren E-Mail-Verkehr auf Viren und Spam sowie die Speicherordner im Hintergrund, verwendet hierbei jedoch die veralteten Datenbanken. Nach Ablauf von der Laufzeit der Probelizenz hört das Programm auf, die Prüfung der Post zu erfüllen.

Wenden Sie sich vor Ablauf Ihrer Lizenz wegen einer Verlängerung an den Verkäufer, bei dem Sie Kaspersky Security 8.0 für Microsoft Exchange Server erworben haben, oder direkt an Kaspersky Lab ZAO.

Frage: Wie oft muss ich ein Update ausführen?

Noch vor wenigen Jahren wurden Viren auf Disketten verbreitet. Damals war es ausreichend, ein Virenschutzprogramm zu installieren und nur hin und wieder eine Virenprüfung durchzuführen. Die letzten Virenepidemien konnten sich jedoch binnen weniger Stunden weltweit ausbreiten. Veraltete Virenschutzprogramme mit veralteten Datenbanken können derartige Gefahren eventuell nicht abwehren. Um wirklich sicher vor neuen Bedrohungen zu sein, sollten Sie die Datenbanken täglich oder sogar noch öfter aktualisieren. Die Anti-Spam-Datenbanken werden im Abstand von 5 Minuten aktualisiert. Dadurch ist eine rechtzeitige Aktualisierung des Spamschutzes für Ihre Server gesichert.

Frage: Können die Datenbanken von Kaspersky Security vorsätzlich ausgetauscht werden?

Alle Datenbanken besitzen eine individuelle Signatur, die bei Zugriffsversuchen auf die Datenbanken vom Programm geprüft wird. Wenn die vorhandene Signatur nicht von Kaspersky Lab vergeben wurde, oder die vorhandene Datenbank nach Ablauf der Lizenz für Kaspersky Security veröffentlicht wurde, verwendet das Programm solche Datenbanken nicht.

Frage: Ich verwende einen Proxyserver, und das Update funktioniert nicht. Was kann ich tun?

Wahrscheinlich verwenden Sie einen Proxyserver, der das Protokoll http 1.0 nicht in vollem Umfang unterstützt. Wir empfehlen für diesen Fall, einen beliebigen anderen Proxyserver zu verwenden.

Frage: Nach dem Hinzufügen neuer Verzeichnisse in Microsoft Exchange erscheinen diese nicht in der Liste der geschützten Verzeichnisse. Was kann ich tun?

Die neuen Verzeichnisse erscheinen nach der Aktualisierung des Inhalts des Serverschutznodes. Für die Aktualisierung muss man in einen anderen beliebigen Node wechseln und dann wieder den Node Serverschutz öffnen.

Frage: Manchmal werden meine an E-Mails angehängten Maildateien im Format msg, beim Versand beschädigt, und ich kann sie nicht mehr öffnen. Hängt das damit zusammen, dass diese Dateien von Kaspersky Security überprüft werden?

Dieser Fall wurde in Testläufen für das Programm nachgestellt. Es wurde festgestellt, dass Dateien in diesem Format beim Versand über Microsoft Exchange immer beschädigt werden können. Dies hat nichts damit zu tun, ob Kaspersky Security 8.0 für Microsoft Exchange Server installiert ist oder nicht.

# KONTAKTAUFNAHME MIT DEM TECHNISCHEN SUPPORT

Wenn Sie Kaspersky Security bereits erworben haben, können Sie sich von den Support-Spezialisten per Telefon oder über das Internet beraten lassen.

Die Spezialisten des technischen Supports beantworten Ihre Fragen zur Installation und Verwendung des Programms. Wenn Ihr Computer durch Viren infiziert wurde, helfen sie Ihnen, den Schaden zu begrenzen.

Bevor Sie sich an unseren technischen Support wenden, lesen Sie bitte unsere Support-Regeln (<http://support.kaspersky.com/de/support/rules>).

## E-Mail-Anfrage an den technischen Support

Sie können eine Frage an die Spezialisten vom Technischen Support stellen, indem Sie das Anfrageformular des Kundenbetreuungssystems Helpdesk (<http://www.kaspersky.com/de/support>) ausfüllen.

Die Anfrage kann in deutscher, englischer, französischer, spanischer oder russischer Sprache gestellt werden.

Um eine E-Mail-Anfrage zu stellen, ist die Angabe der **Kundennummer**, die Sie bei der Anmeldung auf der Support-Webseite erhalten haben, und des **Kennworts** erforderlich.

Falls Sie noch kein registrierter Benutzer von Kaspersky Lab Anwendungen sind, füllen Sie das Anmeldeformular aus (<https://support.kaspersky.com/de/personalcabinet/registration/form/>). Geben Sie bei der Registrierung den *Aktivierungscode* für das Programm oder *den Namen der Schlüsseldatei* ein.

Die Antwort auf Ihre Anfrage von Kaspersky Lab erhalten Sie über Ihr persönliches Kabinett (<https://support.kaspersky.com/ru/personalcabinet?LANG=de>) und an die in der Anfrage angegebene E-Mail-Adresse.

Beschreiben Sie Ihr Problem im Anfrageformular möglichst genau. Füllen Sie bitte alle Pflichtfelder aus:

- **Art der Anfrage.** Wählen Sie einen Betreff aus, der dem Problem möglichst nahe kommt, beispielsweise: "Problem bei Installation / Deinstallation des Produkts" oder "Problem bei Suche / Desinfektion von Viren". Wenn keine der Kategorien zutrifft, wählen Sie den Punkt "Allgemeine Frage".
- **Name und Versionsnummer des Programms.**
- **Anfragetext.** Beschreiben Sie Ihr Problem möglichst genau.
- **Kundennummer und Passwort.** Geben Sie Ihre Kundennummer und das Passwort ein, dass Sie beim Anmelden auf der Support-Seite von Kaspersky lab erhalten haben.
- **E-Mail-Adresse.** An diese Adresse erhalten Sie Antwort auf Ihre Anfrage von Kaspersky Lab.

## Technischer Service per Telefon

Bei dringenden Problemen können Sie den technischen Support in Ihrer Nähe telefonisch erreichen. Vor der Anfrage an die Spezialisten vom russischsprachigen (<http://support.kaspersky.ru/support/international>) oder internationalen (<http://support.kaspersky.ru/support/international>) Technischen Support, sammeln Sie bitte Informationen (<http://support.kaspersky.ru/support/details>) über Ihren Computer und auf ihm installierte Anti-Virus-Software. So können wir Ihnen besser helfen.

# GLOSSAR

## A

### **ABFANGPROGRAMM**

Unterprogramm der Komponente *Sicherheitsserver*, das bestimmte Typen von E-Mails überprüft. Die Auswahl der verfügbaren Abfangprogramme für die Installation richtet sich danach, für welche Rolle Microsoft Exchange Server installiert ist.

### **ANTI-SPAM: LISTE BLOCKIERTER ABSENDER**

(auch "Blacklist" der Adressen)

Liste der E-Mail-Adressen, von denen eingehende Nachrichten vom Programm Kaspersky Lab unabhängig vom Inhalt blockiert werden.

### **ANTI-SPAM: LISTE ERLAUBTER ABSENDER**

(auch "Whitelist" der Adressen)

Liste der E-Mail-Adressen, von denen eingehende Nachrichten vom Programm Kaspersky Lab nicht geprüft werden.

### **ARBEITSPLATZ DES ADMINISTRATORS**

Computer mit der installierten Komponente Kaspersky Security Management-Konsole. Aus dieser Komponente wird die Serverkomponente des Programms – die Komponente Sicherheitsserver eingerichtet und verwaltet.

## B

### **BACKUP**

Spezielles Verzeichnis zum Speichern der Backupkopien der Objekte vor deren Desinfizieren, Löschen oder Ersetzen. Es ist ein Hilfsordner, er wird im Datenspeicherordner des Programms beim Installieren der Komponente Sicherheitsserver angelegt.

### **BACKUPKOPIEN**

Erstellung der Backupkopie des Objekts vor dessen Verarbeitung und Hinzufügen dieser Kopie zum Backup-Ordner. Im Weiteren kann das Objekt aus dem Backup-Ordner wiederhergestellt, zum Kaspersky Lab zur Untersuchung gesendet oder gelöscht werden.

### **BLACKLIST DER SCHLÜSSELDATEIEN**

Datenbank, die die Informationen über vom Kaspersky Lab blockierte Schlüsseldateien enthält. Der Inhalt der Datei mit der "Blacklist" wird zusammen mit den Datenbanken aktualisiert.

## D

### **DATENBANKEN VON KASPERSKY SECURITY**

Die Datenbanken, die die Beschreibungen der Drohungen die Computersicherheit, die für Kaspersky Lab zum Zeitpunkt der Ausgabe der Datenbanken bekannt sind, enthalten. Die Einträge in den Datenbanken lassen zu, in den testbaren Objekten den schadenverursachenden Code aufzudecken. Die Datenbanken entwickeln sich von den Spezialisten Kaspersky Lab und werden jede Stunde erneuert.

### **DESINFIZIEREN VON OBJEKTEN**

Verarbeitungsverfahren für *infizierte Objekte*, bei dem Daten ganz oder teilweise wiederhergestellt werden oder festgestellt wird, dass Desinfizieren nicht möglich ist. Die Desinfektion erfolgt anhand der Datenbankeinträge. Vor dem Desinfizieren von Objekten wird eine *Backupkopie* angelegt, wenn diese Option nicht deaktiviert wurde. Beim Desinfizieren können Daten zum Teil verloren gehen. Die Backup-Kopie kann verwendet werden, um Objekte später wiederherzustellen.

**DNS BLACK LIST (DNSBL)**

Öffentlich verfügbare Listen von IP-Adressen, die bereits als Versender von Spam bekannt sind.

**E****E-MAIL-VERKEHR-PRÜFUNG**

Anti-Virus- und Anti-Spam-Prüfungen für auf den Microsoft Exchange-Server eingehende E-Mails in Echtzeit mit Verwendung der Informationen der aktuellen (letzten) Version der Anti-Viren- und Anti-Spam-Datenbanken.

**EINFACHES OBJEKT**

Textkörper oder einfacher Anhang, z.B. ausführbare Datei. Sieh auch Objektcontainer.

**ENFORCED ANTI-SPAM UPDATES SERVICE.**

Schnell-Update-Service der Anti-Spam-Datenbanken, der die Anti-Spam-Reaktionsschnelligkeit beim Auftauchen neuer Spam-Sendungen erhöht. Für die Arbeit des Enforced Anti-Spam Updates Service ist eine ständige Internet-Verbindung notwendig.

**ERSETZEN VON OBJEKTEN**

Verarbeitungsverfahren für Objekte, bei dem verarbeitete Objekte durch anhand von Vorlagen erstellte Texte (Textkörper) oder *txt*-Dateien (Anhänge) ersetzt werden.

**F****FÖRMLICHE NACHRICHT**

Nachricht, die automatisch generiert und von Mail-Programmen und Roboter-Programmen gesendet wird (z.B. dass die Nachricht nicht gesendet werden kann oder dass die Registrierung des Benutzers auf irgendwelcher Internet-Ressource bestätigt werden soll).

**G****GÜLTIGKEITSDAUER DER LIZENZ.**

Die Laufzeit der Lizenz - die Periode, im Laufe von der Sie die Funktionen des Programms und die zusätzlichen Dienstleistungen benutzen können. Der Umfang der zugänglichen Funktionen und der zusätzlichen Dienstleistungen hängt vom Typ der Lizenz ab.

**I****INFIZIERTES OBJEKT**

Das Objekt, dessen Bereich des Codes mit dem Bereich des Codes der bekannten Drohung vollständig übereinstimmt. Wir empfehlen Ihnen, solche Objekte nicht zu verwenden.

**K****KASPERSKY SECURITY NETWORK (KSN)**

Infrastruktur der Online-Dienste und Services, die den umfassenden Zugriff zur Kaspersky-Lab-Wissensdatenbank über den "Ruf" von Dateien, Web-Ressourcen und Software gewährleistet. Die Nutzung der Daten des Kaspersky Security Network gewährleistet eine höhere Reaktionsschnelligkeit der Kaspersky-Lab-Programme auf neue Bedrohungen, erhöht die Effektivität der Arbeit vieler Schutzkomponenten und verringert die Wahrscheinlichkeit von Fehlalarmen.

**M****MANAGEMENT-KONSOLE**

Eine Komponente von Kaspersky Security. Enthält die Benutzeroberfläche für die Dienste zum Verwalten des Programms und erlaubt das Verwalten und Einrichten der Serverkomponente. Das Verwaltungsmodul ist als Erweiterungskomponente für Microsoft Management Console (MMC) gestaltet.

**N****NACHRICHT LÖSCHEN**

Verarbeitungsverfahren, wenn die E-Mail-Nachricht physisch gelöscht wird. Dieses Verarbeitungsverfahren wird für Nachrichten empfohlen, die Spam oder schädliches Objekt enthalten. Vor dem Löschen der Nachricht wird deren Backupkopie im Backup-Ordner gespeichert (wenn diese Option nicht deaktiviert wurde).

**O****OBJEKT LÖSCHEN**

Verarbeitungsverfahren, wenn das Objekt vom Computer physisch gelöscht wird. Dieses Verarbeitungsverfahren wird für infizierte Objekte empfohlen. Vor dem Löschen von Objekten wird eine Backupkopie angelegt, wenn diese Option nicht deaktiviert wurde. Sie können diese zum Wiederherstellen des Originalobjekts verwenden.

**OBJEKTCONTAINER**

Objekt, das mehrere einzelne Bestandteile enthält, z.B. Archive und E-Mails mit beliebigen verschachtelten E-Mails). S. auch "Einfaches Objekt".

**OBJEKTIGNORIERUNG**

Verarbeitungsverfahren, wenn Objekt vom Benutzer ohne Änderungen ignoriert wird. Beachten Sie, dass die Auswahl dieser Aktion zu Virenbefall auf Ihrem Computer führen kann.

**P****PRÜFUNG FÜR SPEICHERVERZEICHNISSE**

Anti-Viren-Prüfung für auf dem E-Mail-Server gespeicherte E-Mails und Inhalte der öffentlichen Ordner mit Verwendung der letzten Version der Datenbanken. Die Prüfung läuft im Hintergrund und kann sowohl manuell als auch automatisch nach voreingestelltem Zeitplan gestartet werden. Geprüft werden sämtliche geschützten öffentlichen Ordner und E-Mail-Speicherverzeichnisse. Bei der Prüfung können neue Viren gefunden werden, die bei vorigen Prüfungen in Datenbanken noch nicht bekannt waren.

**R****RESERVELIZENZ**

Zusätzlich installiert, jedoch nicht aktive Lizenz für Programme von Kaspersky Lab. Die Reservelizenz wird nach Ablauf einer kommerziellen Lizenz zur aktiven Lizenz.

**S****SCHLÜSSELDATEI**

Eine Datei im Format xxxxxx.key, die es ermöglicht, das Programm von Kaspersky Lab unter den Bedingungen der Test- oder der kommerziellen Lizenz zu verwenden. Die Schlüsseldatei ist vom Programm aufgrund des Codes der Aktivierung geschaffen. Sie können das Programm nur bei Vorhandensein von der Schlüsseldatei verwenden.

**SICHERHEITSSERVER**

Serverkomponente Kaspersky Security. Prüft den E-Mail-Verkehr auf Viren und Spam, aktualisiert Datenbanken, unterstützt seine Unversehrtheit, speichert Statistikdaten, enthält auch Verwaltungsdienste zur Remote-Steuerung und Einrichtung. Die Komponente beinhaltet einen oder mehrere *Abfangprogramme*.

**SPAM**

Unbefugtes Massenversenden der E-Mails, meistens zu Werbezwecken.

**SPAM URI REALTIME BLACKLIST (SURBL)**

Öffentlich verfügbare Listen von Hyperlinks, die zu Werbe-Websites von Spambietern führen.

**U****UNBEKANTER VIRUS**

Neuer Virus, zu dem es noch keinen Eintrag in den Datenbanken gibt. Unbekannte Viren in Objekten werden vom Programm in der Regel mithilfe der heuristischen Analyse gefunden und erhalten den Status virenverdächtig.

**UPDATE**

Vorgang zum Ersetzen / Hinzufügen neuer Dateien (Datenbanken und Programmmodule), nach Herunterladen von den Kaspersky Lab Updateservern.

**UPDATE-SERVER VON KASPERSKY LAB**

Liste der HTTP- und FTP-Server von Kaspersky Lab, von denen das Programm Datenbanken und Modulaktualisierungen auf Ihren Computer kopiert.

**URGENT DETECTION SYSTEM (UDS)**

Von Kaspersky Lab entwickelter und unterstützter Service zur Erfassung von Spam-Sendungen. Die mit Hilfe des UDS-Services durchgeführte Spam-Überprüfung basiert auf dem Vergleich der Merkmale von Meldungen, die mittels einer speziellen UDS-Anfrage an die Server von Kaspersky Lab mit einer Datenbank bekannter Spam-Meldungen gerichtet werden. Wenn die Anfrage mit einer der bekannten Spamnachrichten übereinstimmt, wird das Spam-Rating der Nachricht erhöht. Das UDS-Verfahren ermöglicht die Filterung bekannter Spam-Sendungen, ohne die Aktualisierung der Datenbanken für die Inhaltsfilterung abzuwarten.

**V****VERDÄCHTIGES OBJEKT**

Objekt, dessen Code den modifizierten Code eines bekannten Virus enthält, oder den Code, der einem Virus ähnlich ist, aber dem Kaspersky Lab noch nicht bekannt ist. Verdächtige Objekte werden mithilfe der heuristischen Analyse gefunden.

**W****WIEDERHERSTELLEN**

Verschieben von Kopien von Objekten aus dem *Backup-Ordner* in einen vom Administrator bestimmten Ordner, Entschlüsselung und Speichern unter dem vorgegebenen Namen. Wiederhergestellte Objekte haben dasselbe Format, wie die ehemaligen Ursprungsobjekte vor Verarbeitung durch Kaspersky Security.

# KASPERSKY LAB ZAO

Kaspersky Lab ist ein weltweit bekannter Hersteller von Systemen, die Computer vor Viren und anderer Malware, Spam, Netzwerk- und Hackerangriffen schützen.

Seit 2008 gehört Kaspersky Lab international zu den vier führenden Unternehmen im Bereich der IT-Sicherheit für Endbenutzer (Rating des "IDC Worldwide Endpoint Security Revenue by Vendor"). Nach einer Studie des Marktforschungsinstituts COMCON TGI-Russia war Kaspersky Lab 2009 in Russland der beliebteste Hersteller von Schutzsystemen für Heimanwender.

Kaspersky Lab wurde 1997 in Russland gegründet. Inzwischen ist Kaspersky Lab ein international tätiger Konzern mit Hauptsitz in Moskau und verfügt über fünf regionale Niederlassungen, die in Russland, West- und Osteuropa, im Nahen Osten, in Afrika, Nord- und Südamerika, Japan, China und anderen Ländern aktiv sind. Das Unternehmen beschäftigt über 2.000 hochspezialisierte Mitarbeiter.

**Produkte.** Die Produkte von Kaspersky Lab schützen sowohl Heimanwender als auch Firmennetzwerke.

Die Palette der Heimanwender-Produkte umfasst Antiviren-Anwendungen für Desktops, Laptops, Smartphones und andere mobile Geräte.

Das Unternehmen bietet Programme und Services für den Schutz von Workstations, Datei- und Webservern, Mail-Gateways und Firewalls. In Verbindung mit Administrationstools ermöglichen es diese Lösungen, netzwerkweit einen effektiven automatisierten Schutz vor Computerbedrohungen aufzubauen. Die Produkte von Kaspersky Lab sind durch namhafte Testlabore zertifiziert, mit den Programmen der meisten Softwarehersteller kompatibel und für die Arbeit mit unterschiedlichen Hardwareplattformen optimiert.

Die Virenanalysten von Kaspersky Lab sind rund um die Uhr im Einsatz. Sie finden und analysieren jeden Tag Hunderte neuer Computerbedrohungen. Mit diesem Wissen entwickeln sie Mittel, um Gefahren zu erkennen und zu desinfizieren. Diese Informationen fließen in die Datenbanken ein, auf die die Kaspersky-Programme zurückgreifen. *Die Antiviren-Datenbanken von Kaspersky Lab werden stündlich aktualisiert, die Anti-Spam-Datenbanken im 5-Minuten-Takt.*

**Technologien.** Viele Technologien, die für ein modernes Antiviren-Programm unerlässlich sind, wurden ursprünglich von Kaspersky Lab entwickelt. Es spricht für sich, dass viele Softwarehersteller den Kernel von Kaspersky Anti-Virus in ihren Produkten einsetzen. Zu ihnen zählen SafeNet (USA), Alt-N Technologies (USA), Blue Coat Systems (USA), Check Point Software Technologies (Israel), Clearswift (Großbritannien), CommuniGate Systems (USA), Critical Path (Irland), D-Link (Taiwan), M86 Security (USA), GFI (Malta), IBM (USA), Juniper Networks (USA), LANDesk (USA), Microsoft (USA), NETASQ (Frankreich), NETGEAR (USA), Parallels (Russland), SonicWALL (USA), WatchGuard Technologies (USA), ZyXEL Communications (Taiwan). Eine Vielzahl von innovativen Technologien des Unternehmens ist durch Patente geschützt.

**Auszeichnungen.** Im Verlauf eines kontinuierlichen Kampfes mit Computerbedrohungen hat Kaspersky Lab Hunderte von Auszeichnungen erworben. So wurde Kaspersky Anti-Virus 2010 in einem Test des anerkannten österreichischen Antiviren-Labors AV-Comparatives mit mehreren Premium-Awards Advanced+ ausgezeichnet. Die höchste Auszeichnung stellt für Kaspersky Lab aber das Vertrauen seiner Benutzer auf der ganzen Welt dar. Die Produkte und Technologien des Unternehmens schützen mehr als 300 Millionen Anwender. Über 200.000 Firmen zählen zu den Kunden von Kaspersky Lab.

Website von Kaspersky Lab:

[www.kaspersky.de](http://www.kaspersky.de)

Viren-Enzyklopädie:

[www.securelist.com/de/](http://www.securelist.com/de/)

Antiviren-Labor:

[newvirus@kaspersky.com](mailto:newvirus@kaspersky.com) (nur zum Einsenden verdächtiger Objekte, die zuvor archiviert wurden)

<http://support.kaspersky.com/virlab/helpdesk.html?LANG=de>

(für Fragen an die Virenanalysten)

Webforum von Kaspersky Lab

[www.kaspersky.de/forum](http://www.kaspersky.de/forum)

# **INFORMATIONEN ZU VERWENDETEM FREMDCODE**

Informationen zum Fremdcode sind in der Datei legal\_notices.txt zu finden, die im Installationsordner des Programms liegt.

# HINWEISE ZU MARKENZEICHEN

Die eingetragenen Warenzeichen und Handelsmarken sind Eigentum ihrer Rechteinhaber.

Microsoft, Windows, Windows Server, Windows Vista, SQL Server und Active Directory sind Handelsmarken von Microsoft Corporation, die in den USA und anderen Ländern eingetragen sind.

Intel und Pentium sind Handelsmarken von Intel Corporation, die in den USA und anderen Ländern eingetragen sind.

# INDEX

## A

Anlagen .....	59
Anti-Spam	
Faktor "Potenzieller Spam" .....	74
Import der Liste erlaubter Absender .....	69
Intensivitätsstufe .....	67
Liste blockierter Absender .....	69
Liste erlaubter Absender .....	69
Aufruffilter und SMS	
Blacklist .....	69
Whitelist .....	69
Ausnahmen .....	60

## B

Backupkopien	
Informationen zu Backupkopien anzeigen .....	79
Speicherplatzfreigabe im Backup-Ordner .....	82
BENACHRICHTIGUNGEN .....	84
BERICHTE .....	86
Blacklist	
Aufruffilter und SMS .....	69

## C

Cluster .....	18
---------------	----

## D

Desinfizieren von Objekten .....	101
Diagnose .....	94

## E

EICAR .....	28
EREIGNISJOURNAL .....	94

## H

Hauptfenster .....	37
Konsolenbaum .....	37

## I

Infiziertes Objekt .....	102
--------------------------	-----

## K

KASPERSKY LAB .....	105
KASPERSKY LAB ZAO .....	105

## L

Lizenz	
lizenzvertrag .....	32
Lizenzvertrag .....	32

**M**

Management-Konsole .....	102
--------------------------	-----

**P**

PROGRAMM INSTALLIEREN .....	20
Programmkomponenten .....	15
PROGRAMMOBERFLÄCHE .....	37
Prüfung der Arbeitsfähigkeit .....	28
Prüfung im Hintergrund .....	63

**S**

Schutz von Mail-Postfächern .....	36
Schutz von öffentlichen Ordner .....	36
Schutz von Speicherverzeichnisse .....	36
Server hinzufügen .....	48
Sicherheitsserver .....	16
Starten	
Management-Konsole .....	48

**U**

UPDATE .....	51
--------------	----

**W**

Werkzeugleiste .....	37
Whitelist	
Aufruffilter und SMS .....	69
Wiederherstellen .....	104