

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://support.kaspersky.com/de/>

INHALT

ÜBER DIESES HANDBUCH.....	4
In diesem Dokument.....	4
Symbole und Stilkonventionen	5
WEITERE INFORMATIONSQUELLEN.....	6
Selbständige Informationssuche.....	6
Diskussion von Kaspersky-Lab-Programmen im Webforum.....	7
Nachricht an das Redaktionsteam für Benutzerdokumentation	7
KASPERSKY SECURITY 8.0 FÜR MICROSOFT EXCHANGE SERVER.....	8
Wesentliche Programmfunktionen.....	9
Lieferumfang.....	9
Lizenzvertrag	10
Service für registrierte Benutzer.....	10
HARDWARE- UND SOFTWAREVORAUSSETZUNGEN.....	10
PROGRAMMINSTALLATION VORBEREITEN.....	12
AKTUALISIERUNG VON VORGÄNGERVERSIONEN.....	13
VORGEHEN BEI DER INSTALLATION.....	14
Schritt 1. Erforderliche Komponenten installieren.....	14
Schritt 2. Begrüßung und Lizenzvertrag	15
Schritt 3. Installationstyp auswählen.....	15
Schritt 4. Programmkomponenten auswählen	15
Schritt 5. Verbindung zum Microsoft SQL Server konfigurieren.....	16
Schritt 6. Dateien kopieren	17
PROGRAMMBETRIEB VORBEREITEN.....	18
Hinzufügen des Schlüssels.....	18
Schutz für den Server anpassen	19
Konfiguration des Proxyservers.....	19
Benachrichtigungen anpassen	20
Mit dem Sicherheitsserver verbinden	20
Programmfunktionen überprüfen	21
PROGRAMM WIEDERHERSTELLEN.....	22
PROGRAMM LÖSCHEN	23
KASPERSKY LAB ZAO	24
INFORMATIONEN ZU VERWENDETEM FREMDCODE	25
HINWEISE ZU MARKENZEICHEN.....	26

ÜBER DIESES HANDBUCH

Sie begrüßen die Spezialisten der geschlossener AG "Kaspersky Lab" (weiter– "Kaspersky Lab")! Wir hoffen, dass diese Dokumentation Ihnen hilft, die Installation, Einrichtung und grundlegenden Funktionen von Kaspersky Security 8.0 for Microsoft Exchange Server (weiter Kaspersky Security oder Programm) weitgehend zu verstehen und selbständig vorzunehmen. Dieses Dokument soll Administratoren für Mailserver unter Microsoft Exchange Server 2007 und 2010 (nachfolgend Microsoft-Exchange-Server) dabei unterstützen, ihre Mailserver mit Kaspersky Security optimal zu schützen.

Dieses Dokument Erstellung zu:

- Programmkomponenten auf Servern zu installieren, den Virenschutz zu aktivieren und die Programmeinstellungen optimal an ihre individuellen Erfordernisse anzupassen;
- Probleme bei der Installation der Anwendung effizient zu lösen und die benötigten Informationen schnell zu finden;
- Informationen über weitere Informationsquellen zum Programm und technischen Support zu erhalten.

IN DIESEM ABSCHNITT

In diesem Dokument	4
Symbole und Stilkonventionen	5

IN DIESEM DOKUMENT

Das Installationshandbuch zu Kaspersky Security 8.0 for Microsoft Exchange Server besteht aus folgenden Abschnitten:

- Über dieses Handbuch (s. S. [4](#)). Dieser Abschnitt beschreibt den Aufbau des Installationshandbuches.
- Weitere Informationsquellen (s. S. [6](#)). Dieser Abschnitt beschreibt verschiedene Informationsquellen zu Erwerb, Installation und Verwendung von Kaspersky Security.
- Kaspersky Security 8.0 für Microsoft Exchange Server (s. S. [8](#)). Dieser Abschnitt beschreibt die wesentlichen Programmfunktionen.
- Hardware- und Softwarevoraussetzungen (s. S. [10](#)). Dieser Abschnitt enthält die Hardware- und Softwarevoraussetzungen für die Verwendung von Kaspersky Security.
- Vorbereiten der Installation (s. S. [12](#)). Dieser Abschnitt beschreibt die erforderlichen Schritte vor der Installation des Programms.
- Aktualisierung von Vorgängerversionen des Programms (s. S. [13](#)). Dieser Abschnitt beschreibt, wie Sie die Vorgängerversion von Kaspersky Security auf die neueste Version aktualisieren können.
- Vorgehen bei der Installation (s. S. [14](#)). Der Abschnitt beschreibt detailliert alle Schritte während der Installation des Programms.
- Vorbereitung zur Verwendung des Programms. Assistent für die Ersteinrichtung (s. S. [18](#)). Dieser Abschnitt enthält genaue Anweisungen zur Einrichtung der wesentlichen Programmparameter unmittelbar nach der Installation.
- Programm wiederherstellen (s. S. [22](#)). Dieser Abschnitt enthält Informationen zur Wiederherstellung des Programms nach möglichen Funktionsstörungen.
- Programm löschen (s. S. [23](#)). Dieser Abschnitt enthält Informationen zum Löschen des Programms

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

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	6
Diskussion von Kaspersky-Lab-Programmen im Webforum	7
Nachricht an das Redaktionsteam für Benutzerdokumentation.....	7

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

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 den Punkt "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

Das Installationshandbuch für Kaspersky Security enthält alle erforderlichen Informationen zur Installation des Programms 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, 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

Wesentliche Programmfunktionen	9
Lieferumfang	9

WESENTLICHE PROGRAMMFUNKTIONEN

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 Ordnebene aufgrund der erstellten Liste der zu schützenden Speicherordner ausführen.

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.

LIZENZVERTRAG

Der Lizenzvertrag ist ein juristischer Vertrag zwischen Ihnen und Kaspersky Lab, in dem steht, unter welchen Bedingungen Sie das von Ihnen gekaufte Programm gebrauchen dürfen.

Lesen Sie sich den Lizenzvertrag genau durch!

Möchten Sie den Lizenzvertrag nicht akzeptieren und das Programm nicht nutzen, haben Sie Anspruch auf Erstattung des Kaufpreises. Hierzu muss jedoch der Umschlag mit der Installations-CD noch versiegelt sein.

Wenn Sie den versiegelten Umschlag mit der Installations-CD öffnen, nehmen Sie dadurch alle Bedingungen des Lizenzvertrages an.

SERVICE FÜR REGISTRIERTE BENUTZER

Kaspersky Lab bietet den legalen Benutzern ein umfangreiches Spektrum an Leistungen an, die den wirkungsvollen Einsatz des Programms effektiver gestalten.

Wenn Sie eine Lizenz erwerben, werden Sie registrierter Benutzer und haben während der Gültigkeitsdauer der Lizenz Anspruch auf folgende Leistungen:

- regelmäßiges Update der Programmdatenbanken und Erhalt neu erscheinender Programmversionen;
- Beratung bei Fragen zur Installation, Konfiguration und Nutzung des Programms per Telefon und E-Mail;
- Benachrichtigung bei Herausgabe von neuen Kaspersky-Lab-Programmen und bei neu aufgetauchten Viren. Die vorliegende Dienstleistung wird den Benutzern, die auf den Versand der Neuheiten geschlossener AG "Kaspersky Lab" auf Support-Seite abonnierten, gewährt.

Es werden allerdings keine Fragen zu Funktion und Gebrauch von Betriebssystemen, zu Programmen von Dritten sowie zu verschiedenen Technologien beantwortet.

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.

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 Planmäßiges Update 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

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 vier 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 ein Cluster des Computers installiert, auf dem auch Microsoft Exchange Server installiert ist. Bei dieser Variante werden der Sicherheitsserver und die Management-Konsole auf jedem Clusterknoten gemeinsam installiert.
- Der Sicherheitsserver wird auf Gruppe des Zugriffs der Datenbanken Microsoft Exchange (DAG) installiert. Bei dieser Variante werden der Sicherheitsserver und die Management-Konsole gemeinsam auf jedem Server, der sich in diese Gruppe.

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.

das Installationsprogramm von Kaspersky Security öffnet sich als Assistent, 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 zu beginnen, müssen Sie die Datei setup_de.exe starten.

IN DIESEM ABSCHNITT

Schritt 1. Erforderliche Komponenten installieren	14
Schritt 2. Begrüßung und Lizenzvertrag	15
Schritt 3. Installationstyp auswählen	15
Schritt 4. Programmkomponenten auswählen.....	15
Schritt 5. Verbindung zum Microsoft SQL Server konfigurieren	16
Schritt 6. Dateien kopieren	17

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	18
Schutz für den Server anpassen	19
Konfiguration des Proxyservers	19
Benachrichtigungen anpassen	20
Mit dem Sicherheitsserver verbinden	20
Programmfunktionen überprüfen.....	21

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.

➤ *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.

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.

MIT DEM SICHERHEITSSERVER VERBINDEN

Nach der Installation von Kaspersky Security baut die Management-Konsole automatisch eine Verbindung zum lokalen Sicherheitsserver auf; 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.

➔ *Zum Verbinden mit einem anderen Server 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. Klicken Sie im Ergebnisfenster auf die Schaltfläche **Server hinzufügen**.
4. Wählen Sie in dem sich öffnenden Fenster **Anderer Computer**.
5. Klicken Sie auf die Schaltfläche **Durchsuchen**, und geben Sie den Server vor, mit dem Sie sich verbinden möchten.
6. Klicken Sie auf **OK**.

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.

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 E-Mail über Microsoft Exchange Server, nachdem Kaspersky Security installiert und eine Verbindung zum Sicherheitsserver hergestellt ist (s. Abschnitt "Verbinden mit dem Sicherheitsserver" auf S. 20).
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. 20) 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. 20) 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. 20).

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.

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

Viren-Enzyklopädie:

www.securelist.com/de/

Antiviren-Labor:

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

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 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.