

# KASPERSKY LAB

---

**SECURE  
YOUR  
CYBERSPACE**

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



---

## Kaspersky® Administration Kit 5.0

Erste Schritte

KASPERSKY® ADMINISTRATION KIT 5.0

---

# Erste Schritte

© Kaspersky Lab

<http://www.kaspersky.com/de/>

Redaktionsdatum: Dezember 2005

# Inhalt

KAPITEL 1. VORWORT .....	4
KAPITEL 2. ERSTE SCHRITTE .....	6
2.1. Installation von MSDE 2000.....	7
2.2. Installation von Administrationsserver und Administrationskonsole .....	8
2.3. Grundlegende Konfiguration des Antiviren-Schutzes .....	9
2.4. Erstellen einer Administrationsgruppe .....	11
2.5. Entfernte Installation des Administrationsagenten .....	11
2.6. Entfernte Installation einer Antiviren-Anwendung .....	12
2.7. Überprüfen der Update-Funktion für die Antiviren-Datenbanken der Client- Computer .....	13
2.8. Einstellungen für Benachrichtigungen .....	15
2.9. Überprüfen der Weitergabe von Benachrichtigungen und der Aufgabe zum Scan auf Befehl.....	15
2.10. Erstellen von Protokollen .....	16
KAPITEL 3. WECHSEL DER ANTIVIREN-ANWENDUNGEN VON VERSION 4.X ZU VERSION 5.X.....	17
KAPITEL 4. NACHWORT .....	19
ANHANG A.        KASPERSKY LAB.....	20
A.1. Andere Produkte von Kaspersky Lab .....	21
A.2. Kontaktinformationen.....	26
ANHANG B.        ENDBENUTZER-LIZENZVERTRAG FÜR KASPERSKY ANTI-VIRUS        28	

---

# KAPITEL 1. VORWORT

Dieses Dokument beschreibt die Schritte, mit denen der Antiviren-Schutz-Administrator einer Firma schnell mit der Anwendung **Kaspersky Administration Kit** zu arbeiten beginnen und den Antiviren-Schutz auf Basis von Kaspersky-Lab-Anwendungen in seinem Netzwerk einführen kann.

Hier wird ausführlich ein einfaches Push-Installationsszenarium beschrieben, bei dem der Antiviren-Schutz nur auf einigen Computern eingeführt wird. Eine Voraussetzung für die erfolgreiche Installation ist, dass diese Computer unter den Betriebssystemen MS Windows NT/2000/2003/XP arbeiten.

Das Dokument beschreibt außerdem das Vorgehen zum Wechsel von 4.x-Versionen der Antivirenanwendungen auf Version 5.x der Anwendungen.



Ausführliche Informationen über die Anwendung Kaspersky Administration Kit erhalten Sie im Administratorhandbuch.

Die Anwendung Kaspersky Administration Kit dient der Verwaltung des Antiviren-Sicherheitssystems eines Firmencomputernetzwerks. Mit Hilfe dieser Anwendung kann der Administrator:

- die entfernte Installation von Antiviren-Schutz-Anwendungen der Firma vornehmen.
- die entfernte zentralisierte Verwaltung von Antiviren-Schutz-Anwendungen durchführen.
- Benachrichtigungen über kritische Ereignisse bei der Arbeit von Antiviren-Schutz-Anwendungen erhalten.
- eine Statistik und Protokolle über die Arbeit der Antiviren-Schutz-Anwendungen erhalten.

Die Anwendung Kaspersky Administration Kit besteht aus folgenden Basiskomponenten:

- **Administrationsserver** – Diese Komponente dient der zentralisierten Verwaltung von Kaspersky-Lab-Anwendungen, die den Antiviren-Schutz der Firma realisieren (Kaspersky Anti-Virus 5.0 for Windows Workstations, Kaspersky Anti-Virus 5.0 for File Servers). Der Administrationsserver führt die zentrale Speicherung von Informationen über den Antiviren-Schutz der Firma in einer Datenbank des Typs MSDE 2000 oder MS SQL 2000 durch. Die Datenbanken MSDE / MY SQL 2000 mit Service Pack 3 müssen vor dem Beginn der Installation und der Arbeit

des Administrationsservers im Firmennetzwerk funktionieren. MSDE 2000 mit Service Pack 3 kann aus der Distribution von Kaspersky Administration Kit 5.0 installiert werden.

- **Administrationsagent** – Diese Komponente wird auf einem Client-Computer (Computer, der durch den Administrationsserver verwaltet und von den Anwendungen Kaspersky Anti-Virus 5.0 for Windows Workstations oder Kaspersky Anti-Virus 5.0 for File Servers geschützt wird) installiert. Der Administrationsagent dient der Kommunikation der Antiviren-Anwendungen mit dem Administrationsserver: Er erhält Verwaltungsbefehle vom Administrationsserver und sendet dem Administrationsserver Informationen über den Antiviren-Schutz des Client-Computers.
- **Administrationskonsole** – Diese Komponente bietet die Benutzeroberfläche für Kaspersky Administration Kit zur vollständigen Bedienung aller funktionalen Optionen des Administrationssystems. Die Administrationskonsole besitzt die Form einer Erweiterungskomponente zu Microsoft Management Console (MMC).

---

# KAPITEL 2. ERSTE SCHRITTE

Zur Einführung des Antiviren-Schutzsystems in einem Firmennetzwerk, sind folgende Aktionen erforderlich:

1. Installation der Anwendung MSDE 2000 mit Service Pack 3 oder MS SQL 2000 mit Service Pack 3 (s. Pkt. 2.1 auf S. 7). Dieser Schritt entfällt, wenn eine der Komponenten bereits im Firmennetzwerk installiert ist.
2. Installation des Administrationsservers und der Administrationskonsole (s. Pkt. 2.2 auf S. 8).
3. Basiskonfiguration und Einführung des Antiviren-Schutzsystems der Firma mit Hilfe des Schnellstart-Assistenten (s. Pkt. 2.3 auf S. 9).
4. Erstellen von Administrationsgruppen (s. Pkt. 2.4 auf S. 11). Administrationsgruppen erlauben mit Hilfe von Richtlinien und Gruppenaufgaben die einheitliche Verwaltung der in einer Gruppe enthaltenen Client-Computer.
5. Entfernte Installation des Administrationsagenten auf ausgewählten Client-Computern zur Kommunikation zwischen Antiviren-Anwendungen und Administrationsserver (s. Pkt. 2.5 auf S. 11).
6. Entfernte Installation der Anwendung Kaspersky Anti-Virus 5.0 for Windows Workstations oder Kaspersky Anti-Virus 5.0 for File Servers auf den ausgewählten Client-Computern, falls diese noch nicht installiert sind (s. Pkt. 2.6 auf S. 12).
7. Überprüfen der korrekten Funktion der Aufgabe für den Update-Empfang aus dem Internet durch den Administrationsserver. Überprüfen der korrekten Funktion der Update-Aufgabe auf den Client-Computern. Details s. Pkt. 2.7 auf S. 13.
8. Konfiguration der Einstellungen für die Benachrichtigungen über Ereignisse bei der Arbeit des Antiviren-Schutzes auf den Client-Computern (s. Pkt. 2.8 auf S. 15).
9. Start der Aufgabe für den Scan auf Befehl und Überprüfen der Funktion zur Benachrichtigung über Ereignisse bei der Arbeit des Antiviren-Schutzsystems auf den Client-Computern (s. Pkt. 2.9 auf S. 15).
10. Erstellen eines Protokolls über den Zustand des Antiviren-Schutzsystems auf den Client-Computern und über die gefundenen Viren (s. Pkt. 2.10 auf S. 16).

Nachdem alle genannten Aktionen ausgeführt wurden, ist das Antiviren-System im Firmennetzwerk eingeführt.

In den folgenden Abschnitten des Dokuments werden die genannten Aktionen ausführlicher beschrieben.

## 2.1. Installation von MSDE 2000

Diese Aktion kann übersprungen werden, wenn im Firmennetzwerk bereits die Komponente MSDE 2000 mit Service Pack 3 oder MS SQL 2000 mit Service Pack 3 vorhanden ist.



*Um MSDE 2000 aus der Distribution von Kaspersky Administration Kit zu installieren,*

1. Wählen Sie den Computer, auf dem die Datenbank des Administrationsservers installiert wird. Gewöhnlich ist dies der gleiche Computer, auf dem der Administrationsserver installiert ist.
2. Starten Sie auf dem ausgewählten Computer die ausführbare Datei **setup.exe**, die sich auf der Distributions-CD der Anwendung Kaspersky Administration Kit im Ordner **MSDE2KSP3** befindet.
3. Folgen Sie den Anweisungen des Installationsassistenten.

Dadurch wird MSDE 2000 mit Service Pack 3 auf dem Computer installiert. Die installierte Anwendung erfordert keinerlei Wartung oder Verwaltung.



*Wenn MSDE aus der Distribution von Kaspersky Administration Kit installiert wurde, kann es nur für die Arbeit dieser Anwendung verwendet werden.*

In der Datenbank von MSDE 2000 mit installiertem Service Pack 3 führt der Administrationsserver die zentrale Speicherung von Informationen über den Antiviren-Schutz der Firma durch.

Das Anfertigen von Sicherheitskopien der Administrationsserver-Daten erfolgt mit Hilfe des Dienstprogramms **klbackup**, das zum Umfang der Distribution von Kaspersky Administration Kit gehört (ausführliche Informationen über die Backup-Utility finden Sie im Administratorhandbuch).

## 2.2. Installation von Administrationsserver und Administrationskonsole

Beim Installationsvorgang können entweder beide Komponenten oder nur die Administrationskonsole ausgewählt werden. Es ist nicht möglich, den Administrationsserver ohne die Konsole auszuwählen. Standardmäßig sind beide Komponenten zur Installation vorgesehen.

Bei Bedarf kann die Administrationskonsole auf einem separaten Computer installiert und der Administrationsserver über das Netzwerk verwaltet werden.



*Um den Administrationsserver und/oder die Administrationskonsole zu installieren,*

1. Wählen Sie den Computer, auf dem die Komponenten installiert werden. Wenn das Firmennetzwerk eine Windows-Domänenstruktur aufweist, wird empfohlen, die Komponenten auf einem Computer zu installieren, der zur Domäne gehört.

Der Computer für die Installation des Administrationsservers und/oder der Konsole von Kaspersky Administration Kit 5.x kann der gleiche sein, auf dem der Administrationsserver und/oder die Konsole der Version 4.x arbeiten. Die Komponenten der Versionen 5.x und 4.x sind voneinander unabhängig und können gleichzeitig auf einem Computer laufen.

Die Installation sollte mit den Rechten des Domänen-Administrators durchgeführt werden. Dadurch wird erlaubt, automatisch die Gruppen **KLAdmins** und **KLOperators** zu erstellen und dem Benutzerkonto, unter dem der Administrationsserver arbeiten wird, die erforderlichen Rechte zuzuweisen.

2. Starten Sie die ausführbare Datei setup.exe, die sich auf der Distributions-CD befindet.
3. Folgen Sie den Anweisungen des Installationsassistenten.

Es wird empfohlen, als Benutzerkonto für den Administrationsserver das Konto eines Benutzers auszuwählen, der über Administratorrechte für die Domäne verfügt.

## 2.3. Grundlegende Konfiguration des Antiviren-Schutzes



*Um die grundlegende Konfiguration der Einstellungen des Antiviren-Schutzes der Firma vorzunehmen,*

1. Starten Sie die Administrationskonsole im Menü **Start > Programme > Kaspersky Administration Kit > Kaspersky Administration Kit**.
2. Stellen Sie eine Verbindung zum Administrationsserver her, indem Sie das entsprechende Element in der Konsolenstruktur auswählen und das Zertifikat dieses Administrationsservers annehmen.
3. Öffnen Sie das Kontextmenü des Administrationsservers und wählen Sie den Befehl **Schnellstart-Assistent**.
4. Warten Sie, bis der Administrationsserver das Durchsuchen des Netzwerks abgeschlossen und die darin vorhandenen Computer gefunden hat.
5. Erstellen Sie die Administrationsgruppen durch eine der folgenden Methoden:
  - Wenn das Antiviren-Schutzsystem für mehrere Client-Computer angelegt wird, wählen Sie die Methode **Logisches Netzwerk manuell erstellen**. In diesem Fall müssen Sie die Struktur des logischen Netzwerks selbständig erstellen.
  - Wenn die Installation auf allen Computern der Firma erfolgt, können die Administrationsgruppen automatisch erstellt werden. Wählen Sie in diesem Fall eine der folgenden Varianten:
    - **Logisches Netzwerk auf Basis des Windows-Netzwerks erstellen**. In diesem Fall wird das logische Netzwerk auf Basis der Struktur von Domänen und Arbeitsgruppen des Windows-Netzwerks erstellt (die Administrationsgruppen stimmen mit den Windows-Domänen und –Arbeitsgruppen überein).
    - **Logisches Netzwerk aus der früheren Version von Kaspersky Administration Kit importieren**. In diesem Fall wird das logische Netzwerk auf Basis der Struktur des logischen Netzwerks von Kaspersky Administration Kit 4.x erstellt.

6. Nehmen Sie die Einstellungen für das Senden von Benachrichtigungen über die Arbeit des Antiviren-Schutzes vor. Diese Werte können später in den Eigenschaften des Administrationssservers geändert werden (ausführliche Informationen siehe Administratorhandbuch).
7. Erstellen Sie eine Richtlinie für die Antiviren-Anwendung und für bestimmte Aufgaben, welche die Konfiguration eines korrekt funktionierenden Antiviren-Schutzsystems im Firmennetzwerk erlauben. Richtlinien werden in der Anwendung Kaspersky Administration Kit zum Erstellen einheitlicher Funktionseinstellungen für die Anwendungen in den Administrationsgruppen verwendet. Aufgaben dienen den in Administrationsgruppen von den Anwendungen auszuführenden Aktionen.

Folgende Objekte werden erstellt:

- Richtlinie der obersten Ebene für die Antiviren-Anwendung mit Standardeinstellungen.
- Aufgabe zum Update-Download aus dem Internet durch den Administrationsserver mit Standardeinstellungen.

Diese Aufgabe empfängt die Updates der Antiviren-Datenbanken und Programmmodule von Kaspersky-Lab-Updateservern und speichert sie in dem gemeinsamen Ordner, der bei der Installation des Administrationssservers festgelegt wurde. Die Client-Computer können die Updates unter Verwendung des gemeinsamen Ordners empfangen. Klicken Sie auf die Schaltfläche **Task-Einstellungen**, um die Einstellungen für den Update-Download von den Kaspersky-Lab-Updateservern anzupassen.

- Gruppenaufgabe der obersten Ebene für Updates der Antiviren-Datenbanken auf den Client-Computern mit Standardeinstellungen. Diese Aufgabe ist so konfiguriert, dass die Client-Computer die Updates aus dem gemeinsamen Ordner empfangen, in welchem der Administrationsserver die aus dem Internet heruntergeladenen Updates speichert.
- Gruppenaufgabe mit Standardeinstellungen zum Scan auf Befehl für die Client-Computer.

## 2.4. Erstellen einer Administrationsgruppe



*Um dem logischen Netzwerk eine neue Gruppe hinzuzufügen,*

1. Wählen Sie in der Konsolenstruktur oder im Detailfenster im Ordner **Gruppen** den Ordner der Gruppe, zu der die neue Gruppe hinzugefügt werden soll. Öffnen Sie das Kontextmenü und wählen sie den Befehl **Neu / Gruppe**. Dadurch wird der Assistent für neue Gruppen gestartet. Folgen Sie den Anweisungen des Assistenten.
2. Verschieben Sie die ausgewählten Client-Computer aus der Gruppe **Netzwerk** in die erstellte Administrationsgruppe. Dazu dienen die Befehle **Ausschneiden/Einfügen** des Kontextmenüs, oder die Computer können einfach mit der Maus aus der Gruppe **Netzwerk** in die erstellte Administrationsgruppe gezogen werden.

Auf den ausgewählten Client-Computern kann Kaspersky Anti-Virus der Version 4.x arbeiten. Die Administrationssysteme der Versionen 4.x und 5.x funktionieren unabhängig voneinander. Bei der entfernten Installation von Kaspersky Anti-Virus der Version 5.x über die Version 4.x wird Version 4.x automatisch entfernt und an deren Stelle Version 5.x installiert.

## 2.5. Entfernte Installation des Administrationsagenten



*Zur entfernten Installation des Administrationsagenten*

1. Starten Sie den Assistenten zur Remote-Installation aus dem Kontextmenü der Administrationskonsole.
2. Wählen Sie das Installationspaket des Administrationsagenten zur Installation aus. Dieses Paket wird bei der Arbeit des Schnellstart-Assistenten erstellt und enthält Einstellungen, die dem Administrationsagenten nach der Installation die Verbindung mit dem Server erlauben.

3. Geben Sie als Ziel-Client-Computer für die Installation die erstellte Administrationsgruppe an.
4. Geben Sie bei Bedarf den Benutzernamen und das Kennwort des Administrators für den Zugriff auf die Client-Computer an. Dies ist erforderlich, wenn das Benutzerkonto des Administrationssservers nicht über Administratorrechte für die Client-Computer verfügt.
5. Beim folgenden Schritt des Assistenten wird eine Gruppenaufgabe zur entfernten Installation des Administrationsagenten für die festgelegten Client-Computer erstellt und gestartet. Im Fenster des Assistenten können Sie die aktuellen Ergebnisse der Aufgabenausführung und das Protokoll der Aufgabenausführung für alle Client-Computer verfolgen.
6. Schließen Sie das Fenster des Remote-Installationsassistenten, nachdem die Installation des Administrationsagenten für alle Client-Computer abgeschlossen wurde und die Ergebnisse angezeigt wurden.

Um sich zu vergewissern, dass die Installation korrekt verlaufen ist, öffnen Sie das Eigenschaften-Fenster der Client-Computer. Auf der Registerkarte **Anwendungen** muss die Anwendung **Kaspersky Lab Administrationsagent** mit dem Status **Wird ausgeführt** vorhanden sein.

## 2.6. Entfernte Installation einer Antiviren-Anwendung

In diesem Abschnitt wird die entfernte Installation der Anwendung Kaspersky Anti-Virus for Windows Workstations beschrieben. Der Installationsvorgang für andere Antiviren-Anwendungen von Kaspersky Lab entspricht diesem.



*Um die entfernte Installation von Kaspersky Anti-Virus for Windows Workstations vorzunehmen,*

1. Erstellen Sie mit Hilfe des Assistenten ein Paket zur Remote-Installation der Anwendung Kaspersky Anti-Virus for Windows Workstations. Der Assistent wird aus dem Kontextmenüpunkt des Elements **Remote-Installation** gestartet.

Die zum Erstellen des Installationspakets erforderliche Datei mit der Dateinamenserweiterung **.kpd** befindet sich im Stamm der Distribution der Anwendung Kaspersky Anti-Virus for Windows Workstations. Dort befindet sich auch eine Lizenzschlüsseldatei, welche für die Arbeit mit der Anwendung Kaspersky Anti-Virus for Windows Workstations verwendet wird.

Ändern Sie bei Bedarf die Einstellungen des Installationspakets. Insbesondere wird empfohlen, den automatischen Neustart des Client-Computers zuzulassen.

2. Starten Sie den Assistenten zur Remote-Installation aus dem Kontextmenü der Administrationskonsole.
3. Führen Sie die entfernte Installation der Anwendung Kaspersky Anti-Virus for Windows Workstation durch. Das Vorgehen zur entfernten Installation der Anwendung entspricht dem Vorgehen zur Installation des Administrationsagenten (s. Pkt. 2.5 auf S. 11).

Die Installation kann auf Computern mit Kaspersky Anti-Virus 4.x for Windows Workstations erfolgen. In diesem Fall wird Kaspersky Anti-Virus Version 4.x automatisch entfernt und an seiner Stelle Kaspersky Anti-Virus Version 5.x installiert.

Um sich zu vergewissern, dass die Installation korrekt verlaufen ist, öffnen Sie das Eigenschaften-Fenster der Client-Computer. Auf der Registerkarte **Anwendungen** muss die Anwendung **Kaspersky Anti-Virus for Windows Workstations** mit dem Status **Wird ausgeführt** vorhanden sein. Auf der Registerkarte **Tasks** muss die Echtzeitschutz-Aufgabe erscheinen, die von der Anwendung Kaspersky Anti-Virus for Windows Workstations ausgeführt wird.

## 2.7. Überprüfen der Update-Funktion für die Antiviren-Datenbanken der Client-Computer



*Um zu überprüfen, ob der Update-Download durch die Client-Computer korrekt funktioniert,*

1. Starten Sie die Aufgabe **Update-Download durch den Administrationsserver**. Diese Aufgabe wird vom Schnellstart-Assistenten erstellt und befindet sich im Element **Tasks** der obersten Ebene der Konsolenstruktur. Die Aufgabe empfängt Updates von den Kaspersky-Lab-Updateservern und speichert diese in dem gemeinsamen Ordner, welcher bei der Installation des Servers festgelegt wurde. Warten Sie, bis die Aufgabenausführung abgeschlossen wird.

Die Ergebnisse der Aufgabenausführung können mit Hilfe der Schaltfläche **Ergebnisse** angezeigt werden.

Im Element **Update** des Konsolenbaums erscheinen Informationen über die im gemeinsamen Ordner gespeicherten Updates.



Ausführlichere Informationen über die Methoden für den Update-Download erhalten sie auf der Kaspersky-Lab-Webseite (<http://www.kaspersky.com/de/downloads>).

2. Starten Sie die Gruppenaufgabe zum Update auf den Client-Computern. Diese Aufgabe wird vom Schnellstart-Assistenten erstellt und befindet sich im Ordner **Tasks** des Elements **Gruppen**. Warten Sie, bis die Aufgabenausführung abgeschlossen wird.

Die Ergebnisse der Aufgabenausführung können mit Hilfe der Schaltfläche **Ergebnisse** angezeigt werden.

Die vom Schnellstart-Assistenten erstellte Aufgabe führt das Update der Client-Computer unter Verwendung einer Verbindung zwischen Administrationsagent und Administrationsserver durch. Es werden außerdem folgende Methoden zum Update der Client-Computer unterstützt:

- aus dem gemeinsamen Ordner auf dem Administrationsserver.
- unter Verwendung eines HTTP-Servers.
- unter Verwendung eines FTP-Servers.

Zum korrekten Update-Empfang aus dem gemeinsamen Ordner müssen die Client-Computer über die Rechte zum Lesen dieses Ordners verfügen. Sollte dies nicht möglich sein, dann wird für den Update-Empfang die Verwendung eines FTP- oder HTTP-Servers empfohlen. In diesem Fall wird ein FTP- oder HTTP-Ordner erstellt, der auf den Unterordner **Updates** des gemeinsamen Ordners verweist, der vom Administrationsserver benutzt wird (z.B. `ftp://admserver/updates`). Danach muss in den Einstellungen der Gruppenaufgabe zum Update-Empfang durch die Client-Computer als Update-Quelle der Pfad dieses Ordners angegeben werden (`ftp://admserver/updates`).

## 2.8. Einstellungen für Benachrichtigungen



*Um die Benachrichtigungen über Ereignisse bei der Arbeit des Antiviren-Schutzsystems anzupassen,*

1. Öffnen Sie die Registerkarte **Ereignisbearbeitung** in den Eigenschaften der Richtlinie der obersten Ebene für die Antiviren-Anwendung (z.B. Kaspersky Anti-Virus for Windows Workstations).
2. Wählen Sie die gewünschten Ereignisse aus und legen Sie die Methoden für den Benachrichtigungsempfang fest.

Um die Weitergabe von Benachrichtigungen zu überprüfen (s. Pkt. 2.9 auf S. 15), ist es ausreichend, die Benachrichtigung über das Ereignis **Virus gefunden** auszuwählen.

## 2.9. Überprüfen der Weitergabe von Benachrichtigungen und der Aufgabe zum Scan auf Befehl



*Um die korrekte Weitergabe von Benachrichtigungen über Ereignisse und die Arbeit der Aufgabe zum Scan auf Befehl zu überprüfen,*

1. Versuchen Sie, den "Testvirus" **Eicar** auf einen geschützten Computer zu kopieren. Die Kopieroperation wird gesperrt werden (wenn die Echtzeitschutz-Aufgabe für das Dateisystem funktioniert). Sie erhalten eine Benachrichtigung über den gefundenen Virus und im Element **Ereignisse** der obersten Ebene der Konsolenstruktur erscheint ein entsprechender Eintrag.



Der "Testvirus" IST KEIN VIRUS und enthält keinen Programmcode, der Ihrem Computer schaden könnte. Er wird aber von den Antiviren-Produkten der meisten Herstellerfirmen als Virus identifiziert. Der "Testvirus" kann von der offiziellen Seite der Organisation **EICAR** heruntergeladen werden: [http://www.eicar.org/anti\\_virus\\_test\\_file.htm](http://www.eicar.org/anti_virus_test_file.htm).

2. Beenden Sie die Echtzeitschutz-Aufgabe für das Dateisystem auf dem Client-Computer. Kopieren Sie den "Virus" **Eicar** auf den Client-Computer. Aktivieren Sie erneut die Echtzeitschutz-Aufgabe für das Dateisystem.
3. Starten Sie die Gruppenaufgabe zum Scan auf Befehl der Client-Computer. Während der Ausführung der Aufgabe wird der "Testvirus" gefunden werden. Sie erhalten eine Benachrichtigung über den gefundenen Virus und im Abschnitt **Ereignisse** der obersten Ebene der Konsolenstruktur erscheint ein entsprechender Eintrag.

## 2.10. Erstellen von Protokollen

Auf Basis von Daten, die im Ereignisprotokoll von Kaspersky Administration Kit auf dem Administrationsserver gespeichert werden, können Protokolle über den Zustand des Antiviren-Schutzsystems erstellt werden. Dabei werden zuvor erstellte Protokollvorlagen verwendet, die im Element **Protokolle** der Konsolenstruktur gespeichert sind.

Es sind sieben Standardvorlagen vorhanden, die den Typen der Protokolle über den Zustand des Antiviren-Schutzsystems entsprechen:

- **Protokoll über Versionen der Antiviren-Datenbanken.**
- **Fehler-Protokoll.**
- **Protokoll über Lizenzschlüssel.**
- **Protokoll über Infektionshäufigkeit der Client-Computer.**
- **Protokoll über Antiviren-Schutzniveau.**
- **Protokoll über die Versionen der installierten Kaspersky-Lab-Anwendungen.**
- **Protokoll über Virenaktivität.**

Wenn Sie beispielsweise das Protokoll über Virenaktivität erstellen, erhalten Sie Informationen über alle Virenfunde, die von der Anwendung Kaspersky Administration Kit registriert wurden.

Wenn Sie einer Administrationsgruppe einen Computer hinzufügen, auf dem der Administrationsagent nicht installiert ist, dann enthält das Protokoll über Antiviren-Schutzniveau Informationen darüber, dass auf einem der Computer kein Antiviren-Schutz installiert ist.

---

# KAPITEL 3. WECHSEL DER ANTIVIREN-ANWENDUNGEN VON VERSION 4.X ZU VERSION 5.X

Dieser Abschnitt beschreibt das Vorgehen zum Wechsel von Antiviren-Anwendungen der Version 4.x auf die Anwendungen Kaspersky Anti-Virus 5.x for Windows Workstations oder Kaspersky Anti-Virus 5.x for File Servers. Spezielle Besonderheiten des Wechsels wurden teilweise bereits in den vorhergehenden Abschnitten beschrieben. Hier wird das Szenarium vollständig dargestellt.

Kaspersky Administration Kit 5.x funktioniert unabhängig von Kaspersky Administration Kit 4.x. Dabei wird das Administrationssystem der Version 5.x nur zur Verwaltung von Anwendungen der Version 5.x verwendet, und das Administrationssystem der Version 4.x zur Verwaltung von Anwendungen der Version 4.x. Deshalb werden während des Versionswechsels im Netzwerk für eine bestimmte Zeit gleichzeitig beide Versionen arbeiten.

Das typische Wechselszenarium sieht folgendermaßen aus:

1. Der Administrationsserver der Version 5.x wird im Firmennetzwerk installiert. Dieser kann auf dem gleichen Computer installiert werden, auf dem bereits der Administrationsserver der Version 4.x läuft.
2. Die Struktur des logischen Netzwerks (Administrationsgruppen) für die Anwendungen der Version 5.x wird erstellt. Dabei kann die Struktur des logischen Netzwerks aus dem Administrationssystem der Version 4.x importiert werden.
3. Richtlinien und Gruppenaufgaben für die Anwendungen der Version 5.x werden im logischen Netzwerk erstellt. Die erforderlichen Einstellungen des Antiviren-Schutzes für die Anwendungen werden vorgenommen. Die Bearbeitungsregeln für Ereignisse bei der Arbeit des Antiviren-Schutzes werden festgelegt.
4. Die Computer, für welche der Wechsel von Version 4.x zu Version 5.x erfolgt, werden ausgewählt.
5. Ein Installationspaket zur entfernten Installation für die Version-5.x-Anwendungen wird erstellt. Die Antiviren-Anwendungen der Version 5.x

werden auf den ausgewählten Computern installiert. Dabei werden die Antiviren-Anwendungen der Version 4.x automatisch entfernt und die Antiviren-Anwendungen der Version 5.x installiert.

6. Die Computer, auf denen die Installation von Antiviren-Anwendungen der Version 5.x erfolgte, werden dem logischen Netzwerk des Administrations-servers der Version 5.x hinzugefügt. Die übrigen Computer werden weiterhin vom Administrationssystem der Version 4.x verwaltet.

Stufenweise wird der gesamte Antiviren-Schutz der Firma auf die Antiviren-Anwendungen der Version 5.x umgestellt, die durch das Administrationssystem der Version 5.x verwaltet werden.

---

# KAPITEL 4. NACHWORT

Die Möglichkeiten des Administrationssystems Kaspersky Administration Kit sind wesentlich umfangreicher, als in diesem Dokument beschrieben. Hier wird ein einfaches Szenarium beschrieben, das Ihnen erlaubt, die Arbeit mit dem Administrationssystem zu beginnen und den Antiviren-Schutz im Netzwerk auf einigen Computern einzuführen. Das beschriebene Szenarium beschreibt aber alle wichtigen Aktionen, die für den Aufbau eines zuverlässigen Antiviren-Schutzes in einem Firmennetzwerk erforderlich sind:

- Einführung und Konfiguration des Administrationssystems für den Antiviren-Schutz.
- Zentralisierte Einführung des Antiviren-Schutzes auf den Client-Computern eines Firmennetzwerks.
- Erstellen von Richtlinien für den Antiviren-Schutz.
- Konfiguration und Überprüfen der Funktion der Update-Aufgabe für die Antiviren-Datenbanken von Client-Computern.
- Überprüfen der Funktion der Echtzeitschutz-Aufgabe.
- Erstellen und Starten der Aufgabe zum Scan auf Befehl für die Client-Computer.
- Empfang von Benachrichtigungen über kritische Ereignisse bei der Arbeit des Antiviren-Schutzsystems.
- Erstellen von Protokollen über den Status des Antiviren-Schutzes im Netzwerk.

---

# ANHANG A. KASPERSKY LAB

Die Firma Kaspersky Lab wurde 1997 gegründet. Heute sind wir das bekannteste Unternehmen für Datenschutz-Software in Russland und bieten eine breite Palette an Programmen zum Schutz vor Viren, unerwünschten E-Mails (Spam) und Hackerangriffen.

Kaspersky Lab ist ein international operierender Konzern. Unser Firmensitz befindet sich in Russland, regionale Vertretungen bestehen in Großbritannien, Frankreich, Deutschland, Japan, den Benelux-Staaten, China, Polen, Rumänien und den USA (Kalifornien). In Frankreich wurde jüngst ein neues Subunternehmen eröffnet – das Europäische Zentrum für Antivirenforschung. Unser Partnernetzwerk vereint weltweit mehr als 500 Firmen.

Kaspersky Lab heute – das sind mehr als 250 hoch qualifizierte Fachleute, von denen neun den Titel eines MBA sowie fünfzehn einen Dokortitel besitzen und zwei Mitglieder der international angesehenen Computer Anti-virus Researcher's Organization (CARO) sind.

Das wertvollste Potenzial des Unternehmens sind einmaliges Know-how und Erfahrung, gesammelt durch unsere Mitarbeiter im Laufe von vierzehn Jahren ständigen Kampfes mit Computerviren. Durch ständige Analyse der Entwicklung im Bereich Computerviren sind wir in der Lage, neue Tendenzen für gefährliche Programme vorherzusehen und den Anwendern frühzeitig zuverlässige Lösungen zum Schutz vor neuen Attacken anzubieten. Dieser Vorteil ist die Basis für den Erfolg der Programme und Services von Kaspersky Lab. Wir sind unserer Konkurrenz stets einen Schritt voraus und garantieren maximale Sicherheit zum Wohle unserer Klientel.

In jahrelangen Bemühungen ist es uns gelungen, die Marktführerschaft in der Entwicklung von Virenschutzprogrammen zu erobern. Viele moderne Standards für Virenschutzprogramme wurden erstmals von Kaspersky Lab entwickelt. Unser führendes Produkt, Kaspersky Anti-Virus®, garantiert zuverlässigen Schutz für alle Objekte, die Virenattacken ausgesetzt sind: Computer-Arbeitsplätze, Dateiserver, Mail Exchanger, Firewalls und Internet-Gateways, Handheld-Computer. Die bequeme Handhabung erlaubt einen größtenteils automatisierten Virenschutz in den Firmennetzwerken der Anwender. Viele westliche Softwarehersteller verwenden in ihren Programmen die Quellcodes von Kaspersky Anti-Virus®, darunter: Nokia ICG (USA), F-Secure (Finnland), Aladdin (Israel), Sybari (USA), G Data (Deutschland), Deerfield (USA), Alt-N (USA), Microworld (Indien), BorderWare (Kanada).

Die Kunden von Kaspersky Lab erhalten ein breites Spektrum zusätzlicher Dienstleistungen, welche die störungsfreie Funktion der Produkte und die präzise Abstimmung auf spezifische Anforderungen garantieren. Wir planen, implementieren und warten Antivirenkomplexe für Unternehmen. Unsere Antiviren-Datenbanken werden alle drei Stunden aktualisiert. Unseren

Anwendern bieten wir rund um die Uhr technische Unterstützung in mehreren Sprachen.

## A.1. Andere Produkte von Kaspersky Lab

### Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus Personal schützt Ihren daheim genutzten Computer unter Windows 98/ME, 2000/NT/XP vor allen bekannten Virenarten einschließlich potentiell gefährlicher Software. Das Programm kontrolliert laufend sämtliche Kanäle für möglichen Virenbefall – E-Mail, Internet, Disketten, CDs u.a. Das einmalige heuristische Datenanalyse-System neutralisiert auf wirksame Weise unbekannte Viren. Folgende Varianten für die Arbeit des Programms lassen sich unterscheiden (Diese können separat oder gemeinsam verwendet werden):

- **Echtzeitschutz des Computers** – Virenuntersuchung aller Objekte, die auf dem Computer gestartet, geöffnet und gespeichert werden.
- **Scan auf Befehl** – Untersuchung und Desinfektion sowohl des gesamten Computers als auch einzelner Laufwerke, Dateien oder Verzeichnisse. Sie können diese Untersuchung selbständig starten oder den regelmäßigen automatischen Start der Untersuchung konfigurieren.

Kaspersky Anti-Virus Personal untersucht nun Objekte, die während einer vorhergehenden Untersuchung gescannt wurden und seitdem nicht verändert wurden, nicht erneut. Dies gilt sowohl für den Echtzeitschutz als auch für den Scan auf Befehl. Dadurch **erhöht sich die Operationsgeschwindigkeit des Programms wesentlich**.

Das Programm schafft eine zuverlässige Barriere gegen das Eindringen von Viren über E-Mails. Kaspersky Anti-Virus Personal führt automatisch die Untersuchung und Desinfektion des gesamten nach den Protokollen POP3 und SMTP ein- und ausgehenden E-Mailverkehrs durch und bietet die effiziente Untersuchung von Mail-Datenbanken.

Das Programm unterstützt mehr als siebenhundert Formate für Archive und komprimierte Dateien, überprüft deren Inhalt auf Viren und eliminiert gefährliche Codes aus **ZIP, CAB, RAR, AFJ** -Archiven.

Die komfortable Bedienung des Programms wird durch die Auswahl zwischen drei voreingestellten Sicherheitsstufen realisiert: **Maximale Sicherheit, Empfohlen** und **Maximales Tempo**.

Die Antiviren-Datenbanken werden alle drei Stunden aktualisiert. Die vollständige Übertragung wird auch bei Unterbrechung oder Wechsel der Internetverbindung garantiert.

## Kaspersky Anti-Virus® Personal Pro

Dieses Programmpaket wurde speziell entwickelt, um den vollwertigen Antivirenschutz für Heimcomputer unter den Betriebssystemen Windows 98/ME, Windows 2000/NT, Windows XP, sowie mit MS Office Anwendungen der Business-Edition zu gewährleisten. Kaspersky Anti-Virus® Personal Pro verfügt über eine Funktion zum täglichen Download von Updates für Antiviren-Datenbanken und Programmmodule. Das einmalige heuristische System zur Datenanalyse der zweiten Generation erlaubt, unbekannte Viren wirksam zu neutralisieren. Die einfache und praktische Benutzeroberfläche ermöglicht das schnelle Anpassen der Einstellungen und sorgt für größtmöglichen Komfort im Umgang mit dem Programm.

Kaspersky Anti-Virus® Personal Pro bietet:

- **die Antiviren-Untersuchung** der lokalen Laufwerke **auf Befehl des Benutzers**.
- **die automatische Untersuchung im Echtzeitmodus** auf Viren in allen verwendeten Dateien.
- **einen E-Mail-Filter**, der automatisch die Untersuchung und Desinfektion des gesamten nach den Protokollen POP3 und SMTP ein- und ausgehenden E-Mail-Verkehrs eines beliebigen Mailprogramms vornimmt und Mail-Datenbanken effektiv auf Viren untersucht.
- **Behaviour Blocker**, der hundertprozentigen Schutz vor Makroviren für MS Office Anwendungen garantiert.
- **die Antiviren-Untersuchung** von über 900 Versionen archivierter und gepackter Dateiformate und gewährleistet die automatische Antiviren-Untersuchung des Inhalts, sowie das Entfernen von schädlichem Code aus Archivdateien der Formate **ZIP, CAB, RAR, ARJ**.

## Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker ist eine persönliche Firewall, die Ihren Computer unter Windows vollständig gegen unberechtigten Zugriff auf Daten und gegen Hackerangriffe über das Internet oder lokale Netzwerke abschirmt.

Kaspersky® Anti-Hacker verfolgt die Netzaktivitäten über ein TCP/IP-Protokoll für sämtliche Anwendungen auf Ihrem Computer. Falls für eine Anwendung verdächtige Aktivitäten registriert werden, gibt das Programm eine Warnmeldung aus und blockiert, falls erforderlich, den Zugriff über das Netz für die entsprechende Anwendung, so dass die auf dem Computer gespeicherten Daten geschützt bleiben.

Durch Verwendung der SmartStealth™-Technologie wird das Aufspüren des Computers von außerhalb erheblich erschwert: da der Computer unsichtbar bleibt, ist er vor Hackerangriffen geschützt, ohne dass jedoch Ihre eigene Kommunikations- und Arbeitsfähigkeit über das Internet beeinträchtigt wird. Das

Programm gewährleistet angemessenen Schutz aber auch den standardmäßigen Zugriff auf die Daten des Computers.

Kaspersky® Anti-Hacker blockiert weiterhin die am weitesten verbreiteten Formen von Netzattacken durch Hacker sowie Versuche zum Ausspähen einzelner Ports.

Das Programm bietet vereinfachte Steuerungsmöglichkeiten über fünf verschiedene Sicherheitsstufen. Als Standardeinstellung wird eine lernfähige Systemkonfiguration verwendet, so dass die Sicherheitseinstellungen an Ihre individuelle Reaktion auf verschiedene Ereignisse angepasst werden können. Dadurch wird es möglich, die Konfiguration der Firewall individuell auf bestimmte Anwender und einzelne Computer abzustimmen.

### **Kaspersky® Personal Security Suite**

Kaspersky® Personal Security Suite eignet sich als Programm für den nach allen Seiten vorhandenen Schutz von Computern mit dem Betriebssystem Windows vorgesehen sind. Dieses Programm schützt vor dem Eindringen bössartiger und potentiell gefährlicher Software aus allen möglichen Quellen und schützt außerdem vor dem nicht sanktionierten Zugriffen auf Daten des Computers und vor Spam-Mails.

Kaspersky® Personal Security Suite hat die folgenden Funktionen:

- Antivirenschutz von Daten, die auf dem Computer gespeichert werden.
- Schutz von Benutzern der Mailclients Microsoft Outlook und Microsoft Outlook Express vor unerwünschten E-Mailnachrichten (Spam).
- Schutz des Computers vor nicht sanktionierten Zugriffen auf Daten sowie vor Netzwerkangriffen aus dem lokalen Netzwerk oder aus dem Internet.

### **Kaspersky® Security für PDA**

Kaspersky® Security für PDA gewährleistet zuverlässigen Virenschutz für Daten auf Handheld-PCs (PDA) verschiedener Art und auf Smartphones. Das Programm umfasst eine optimale Auswahl an Virenschutz-Komponenten:

- **einen Virens scanner**, der eine Überprüfung der Daten (sowohl im Speicher des PDA oder Smartphones selbst, als auch auf beliebigen Speicher-Erweiterungskarten) auf Anforderung des Anwenders ausführt;
- **den Antivirus-Monitor**, der während der Synchronisation über HotSync™ und während des Datenaustausches mit anderen PDA Virenprogramme blockiert.

Weiterhin schützt das Programm die auf dem PDA gespeicherten Informationen vor unberechtigtem Zugriff durch Verschlüsselung des Zugriffs auf das Gerät selbst wie auch auf die im Speicher des PDA und auf Speicherkarten enthaltenen Daten.

## Kaspersky Anti-Virus® Business Optimal

Dieses Programmpaket ist die ultimative Lösung zum Schutz vor Computerviren für Unternehmen kleiner und mittlerer Größe.

Kaspersky Anti-Virus® Business Optimal bietet Rundumschutz<sup>1</sup> vor Viren für:

- *Computerarbeitsplätze* unter Windows 98/Me, Windows 2000/NT/XP Workstation, Linux.
- *Dateiserver* unter Windows NT 4.0 Server, Windows 2000/2003 Server/Advanced Server, Novell Netware, FreeBSD und OpenBSD, Linux et Samba Servers.
- *Mailsysteme* vom Typ Microsoft Exchange 2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail und Qmail.
- *Mail-Firewalls*: SMTP-Gateway.
- *Internet-Firewalls*: CheckPoint Firewall –1; MS ISA Server 2000 Standard Edition.

Kaspersky Anti-Virus® Business Optimal beinhaltet außerdem ein zentrales Installations- und Administrationssystem, Kaspersky® Administration Kit.

Sie selbst wählen die geeigneten Virenschutzprogramme in Abhängigkeit von den in Ihrem Unternehmen verwendeten Betriebssystemen und Anwendungen.

## Kaspersky® Corporate Suite

Kaspersky® Corporate Suite ist eine integrierte Softwarelösung zum Datenschutz für Ihr gesamtes Firmennetzwerk ohne Einschränkungen hinsichtlich Größe und Struktur. Die enthaltenen Programmkomponenten schützen jeden Punkt ihres firmeninternen Netzes. Sie sind kompatibel mit den meisten heute verbreiteten Betriebssystemen und Anwendungen, über ein zentrales Steuerungssystem miteinander verbunden und werden über eine gemeinsame Benutzeroberfläche bedient. Mit diesem System erhalten Sie einen Virenschutz, der sich vollständig an die Systemanforderungen Ihres internen Netzes anpassen lässt.

Kaspersky® Corporate Suite bietet Rundumschutz<sup>2</sup> vor Viren für:

- *Computerarbeitsplätze* unter Windows 98/Me, Windows 2000/NT/XP Workstation und Linux.
- *Dateiserver* unter Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux et Samba Servers.

---

<sup>1</sup> Je nach Lieferumfang

<sup>2</sup> Je nach Lieferumfang

- *Mailsysteme* vom Typ Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim und Qmail.
- *Internet-Firewalls*: CheckPoint Firewall –1; MS ISA Server 2004 Enterprise Edition.
- *Handheld-PCs* mit den Betriebssystemen Windows CE und Palm OS sowie Smartphones mit dem Betriebssystem Windows Mobile 2003 für Smartphone und Microsoft Smartphone 2002.

Kaspersky® Corporate Suite beinhaltet außerdem ein zentrales Installations- und Administrationssystem, Kaspersky® Administration Kit.

Sie selbst wählen die geeigneten Virenschutzprogramme in Abhängigkeit von den in Ihrem Unternehmen verwendeten Betriebssystemen und Anwendungen.

### **Kaspersky® Anti-Spam**

Kaspersky® Anti-Spam ist die erste in Russland entwickelte Software zum Schutz vor unerwünschten Mailings (Spam) für Unternehmen kleinerer und mittlerer Größe. Das Programm vereint moderne Verfahren der Sprachanalyse für Informationen in Textform, sämtliche modernen Verfahren zum Filtern von E-Mails (einschließlich RBL-Listen und formeller Prüfung von Nachrichten) sowie eine einmalige Auswahl an Dienstprogrammen, durch die der Nutzer in die Lage versetzt wird, bis zu 95 % der unerwünschten Nachrichten zu identifizieren und zu eliminieren.

Kaspersky® Anti-Spam ist ein Filterprogramm, das, am „Eingang“ des firmeninternen Netzwerks installiert, sämtliche eingehenden Mitteilungen auf Spam überprüft. Das Programm ist kompatibel mit jedem beliebigen Mailing-System und kann sowohl auf bereits funktionierenden als auch auf separaten Mailservern installiert werden.

Die tägliche Aktualisierung der Filterdatenbank mit Mustertexten aus unserem Sprachlabor garantiert eine hohe Effizienz dieses Produkts.

### **Kaspersky SMTP Gateway**

Kaspersky® SMTP-Gateway for Linux/Unix ist ein Programm für die Antivirenuntersuchung von E-Mail-Nachrichten, die über das SMTP-Protokoll eingehen. Die Software enthält eine Reihe von zusätzlichen Filterinstrumenten für den Mailverkehr, filtern nach Namen und MIME-Typen von eingebetteten Dateien sowie eine Reihe von Mitteln, die mit denen die Belastung für das Mailsystem gesenkt und Hackerangriffe abgewehrt werden können. So kann zum Beispiel die Größe einer E-Mail, die Anzahl der Empfänger usw. beschränkt werden. Das DNS Black List wird unterstützt und garantiert so einen Schutz vor Mails von Servern, die in schwarzen Listen als Urheber von unerwünschten E-Mail-Nachrichten (Spam) eingetragen sind.

### **Kaspersky Security® for Microsoft Exchange 2003**

Kaspersky Security for Microsoft Exchange bietet die Antivirenuntersuchung der eingehenden, ausgehenden und auf dem Server gespeicherten E-Mail-Nachrichten einschließlich der Nachrichten in gemeinsamen Ordnern. Außerdem führt er die Filterung unerwünschter Korrespondenz aus, wobei intellektuelle Technologien zum Erkennen von Spam in Verbindung mit Technologien der Firma Microsoft verwendet werden.

Die Anwendung untersucht alle mit dem SMTP-Protokoll auf dem Exchange-Server eingehenden Nachrichten auf das Vorhandensein von Viren, wobei Antivirentechnologien von Kaspersky Lab verwendet werden, und auf Spam-Merkmale, wozu die Filterung nach formalen Kennzeichen (E-Mail-Adresse, IP-Adresse, Größe des Briefs, Kopfzeile) dient. Außerdem analysiert er den Inhalt des Briefs und seiner Anhänge mit Hilfe von intellektuellen Technologien, die unikale grafische Signaturen zum Erkennen von Spam in Form von Bildern umfassen. Der Untersuchung werden sowohl der Nachrichtenkörper als auch angehängte Dateien unterzogen.

### **Kaspersky® Mail Gateway**

Kaspersky Mail Gateway ist eine universelle Lösung für den komplexen Schutz der Benutzer von Mailsystemen. Die Anwendung wird zwischen dem Unternehmensnetzwerk und dem Internet installiert und führt die Untersuchung aller Elemente eines E-Mail-Briefs auf das Vorhandensein von Viren und anderen schädlichen Programmen (Spyware, Adware usw.) durch. Außerdem nimmt er die zentralisierte Filterung des E-Mail-Nachrichtenstroms auf Spam-Merkmale vor. Die Lösung enthält ferner eine Reihe zusätzlicher Optionen für die Filterung des E-Mail-Stroms.

## A.2. Kontaktinformationen

Sollten Sie weitere Informationen wünschen, wenden Sie sich bitte an unsere Vertriebspartner oder direkt an Kaspersky Lab. Wir werden Sie gern umfassend per Telefon oder E-Mail beraten.

Technischer Support	Informationen über den technischen Support finden Sie unter: <a href="http://www.kaspersky.com/supportinter.html">www.kaspersky.com/supportinter.html</a> E-Mail: <a href="mailto:deutsch@support.kaspersky.com">deutsch@support.kaspersky.com</a>
Allgemeine Informationen	WWW: <a href="http://www.kaspersky.com/de/">http://www.kaspersky.com/de/</a> <a href="http://www.viruslist.com/de/">http://www.viruslist.com/de/</a> E-Mail: <a href="mailto:sales@kaspersky.com">sales@kaspersky.com</a>

Feedback zu unseren Benutzerhandbüchern	<a href="mailto:docfeedback@kaspersky.com">docfeedback@kaspersky.com</a> (Diese Adresse ist für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.)
Abteilung für die Erstellung von Dokumentationen	<a href="mailto:docfeedback@kaspersky.com">docfeedback@kaspersky.com</a> (nur für Einsenden von Feedback über die Dokumentationen und über das elektronische Supportsystem)

---

# ANHANG B. ENDBENUTZER- LIZENZVERTRAG FÜR KASPERSKY ANTI-VIRUS

## ENDBENUTZER-LIZENZVERTRAG FÜR KASPERSKY ANTI-VIRUS

WICHTIG - bitte sorgfältig lesen: Lesen Sie die in diesem Kaspersky Lab Endbenutzer-Lizenzvertrag („EULA“) beschriebenen Rechte und Einschränkungen sorgfältig durch. Sie werden gebeten, die Bestimmungen des EULAs zu prüfen und ihnen zuzustimmen oder diese abzulehnen.

Indem Sie das Sicherheitsetikett auf der CD-Box aufreißen oder wenn Sie die SOFTWARE installieren, erklären Sie sich mit den Bestimmungen des EULAs einverstanden. Falls Sie mit den Bestimmungen des EULAs NICHT einverstanden sind, geben Sie die erworbene Software bitte innerhalb von 30 Tagen an die Einkaufsstelle zurück.

Dieser EULA ist ein rechtsgültiger Vertrag zwischen Ihnen, dem Besitzer eines Exemplars von Kaspersky Anti-Virus (entweder als natürlicher oder als juristischer Person) und Kaspersky Lab. Kaspersky Lab wird sich das exklusive Urheberrecht auf die Computersoftware (auf die Software und die Antiviren-Datenbanken) vorbehalten. Indem Sie die SOFTWARE installieren, erklären Sie sich damit einverstanden, durch die Bestimmungen dieses EULAs gebunden zu sein. Falls Sie den Bestimmungen dieses EULAs nicht zustimmen, sind Sie nicht berechtigt, die SOFTWARE zu installieren und zu verwenden.

Die SOFTWARE ist sowohl durch Urheberrechtsgesetze und internationale Urheberrechtsverträge als auch durch andere Gesetze und Vereinbarungen über geistiges Eigentum geschützt. Die SOFTWARE wird lizenziert, nicht verkauft.

1. LIZENZEINRÄUMUNG. Durch diesen EULA werden Ihnen folgende Rechte eingeräumt:

- (a) Sie sind berechtigt, eine Kopie der SOFTWARE auf einem einzigen Computer zu installieren und zu verwenden.
- (b) Sie sind berechtigt, die installierte SOFTWARE ein Jahr lang zu verwenden (Lizenzdauer).

2. EINSCHRÄNKUNGEN.

(a) Einschränkungen im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung. Sie sind nicht berechtigt, die SOFTWARE zurückzuentwickeln (Reverse Engineering), zu dekompileieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Einschränkung, dies ausdrücklich gestattet.

(b) Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.

(c) Supportleistungen. Nach Kauf der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die Lizenzdauer. Supportleistungen verstehen sich wie folgt:

- tägliches Update der Antiviren-Datenbank.
- kostenloses Update der Software.
- kostenlose technische Unterstützung sowohl per e-Mail als auch per Telefon mit Hot-Line-Service.
- Viren-Entdeckung und heilende Updates auf Anfrage innerhalb von 48 Stunden.

3. KÜNDIGUNG. Unbeschadet sonstiger Rechte ist Kaspersky Lab berechtigt, diesen EULA zu kündigen, sofern Sie gegen die Bestimmungen dieses EULAs verstoßen. In einem solchen Fall sind Sie verpflichtet, sämtliche Kopien der SOFTWARE und alle ihre Komponenten zu vernichten.

4. URHEBERRECHT. Eigentum und Urheberrecht auf die SOFTWARE, die gedruckten Begleitmaterialien und jede Kopie der SOFTWARE liegen bei Kaspersky Lab.

5. GEWÄHRLEISTUNG. KASPERSKY LAB gewährleistet, dass:

(a) die SOFTWARE den Spezifikationen im wesentlichen entspricht.

(b) der Originaldatenträger frei von Material- und Herstellungsfehlern ist.

(c) das Programm korrekt auf den Datenträger aufgezeichnet ist, die Dokumentation (sämtliche Informationen enthält, die KASPERSKY LAB für die Benutzung der Software für erforderlich hält).

(d) die SOFTWARE binnen 6 Monaten ab der ersten Installation oder dem ersten Download, falls richtig behandelt, vollfunktionsfähig ist, der in der beiliegenden Dokumentation bestimmten Funktionalität entsprechend.

Die Gewährleistungsfrist beträgt 6 Monate ab der ersten Installation oder dem ersten Download der Software den beiliegenden Dokumentationen von Kaspersky Lab entsprechend. Gewährleistungspflichtige Mängel werden von KASPERSKY LAB oder dessen Lieferanten nach Entdeckung, auf jeden Fall aber vor Ablauf von der Gewährleistungsfrist, dem Ermessen von Kaspersky Lab nach, durch Ersatz, Reparatur, Umtausch oder Rückzahlung beseitigt, falls eine Mangelrüge rechtzeitig an Kaspersky Lab oder dessen Lieferanten gerichtet wurde. KASPERSKY LAB oder dessen Lieferanten übernehmen keine Gewährleistung für Mängel, die auf andere als für die Software vorgesehenen Einsatzbedingungen, unsachgemäße Behandlung oder dergleichen zurückzuführen sind.

ALLE ANDERE GEWÄHRLEISTUNGEN UND BEDINGUNGEN, SEIEN SIE AUSDRÜCKLICH ODER KONKLUDENT, EINSCHLIESSLICH, JEDOCH NICHT

BESCHRÄNKT AUF, (FALLS ZUTREFFEND) JEDE KONKLUDENTE GEWÄHRLEISTUNG IM HINBLICK AUF HANDELSÜBLICHKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, FAHRLÄSSIGKEIT ODER MANGELNDE FACHMÄNNISCHE BEMÜHUNGEN WERDEN VON KASPERSKY LAB ODER DESSEN LIEFERANTEN ABGELEHNT. ES BESTEHT EBENFALLS KEINE GEWÄHRLEISTUNG ODER BEDINGUNG VON RECHTSANSPRÜCHEN IN BEZUG AUF RECHTSINHABERSCHAFT, UNGESTÖRTES NUTZUNGSVERGNÜGEN ODER NICHTVERLETZUNG VON RECHTEN DRITTER. DAS GESAMTE RISIKO, DAS BEI DER BENUTZUNG ODER LEISTUNG DER SOFTWARE ENTSTEHT, LIEGT BEI IHNEN.

6. AUSSCHLUSS DER HAFTUNG FÜR ALLE SCHÄDEN. SOWEIT GESETZLICH ZUGELASSEN, SIND KASPERSKY LAB ODER DESSEN LIEFERANTEN IN KEINEM FALL HAFTBAR FÜR IRGENDWELCHE FOLGE-, ZUFÄLLIGEN, DIREKTEN, INDIREKTEN, SPEZIELLEN, STRAFRECHTLICHEN ODER ANDEREN SCHÄDEN WELCHER ART AUCH IMMER (EINSCHLIESSLICH, ABER NICHT BESCHRÄNKT AUF SCHÄDEN AN PERSONEN ODER SACHEN, SCHÄDEN AUS ENTGANGENEM GEWINN, GESCHÄFTSUNTERBRECHUNG, VERLUST VON GESCHÄFTLICHEN INFORMATIONEN, FÜR DEN VERLUST VON PRIVATSPHÄRE, DIE UNMÖGLICHKEIT, EINE PFLICHT ZU ERFÜLLEN (EINSCHLIESSLICH GEMÄSS TREU UND GUTEN GLAUBENS ODER VERNÜNFTIGER ANGEMESSENER SORGFALT) ZU ERFÜLLEN, FÜR FAHRLÄSSIGKEIT ODER ANDERE VERMÖGENSSCHÄDEN), DIE AUS DER VERWENDUNG DER SOFTWARE ODER DER TATSACHE, DASS SIE NICHT VERWENDET WERDEN KANN, RESULTIEREN ODER DAMIT IN ZUSAMMENHANG STEHEN, SELBST WENN KASPERSKY LAB ODER DESSEN LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WORDEN IST. DIESER HAFTUNGSAUSSCHLUSS FÜR SCHÄDEN GILT AUCH DANN, WENN ABHILFEMASSNAHMEN IHREN WESENTLICHEN ZWECK VERFEHLEN.

7. ANWENDBARES RECHT. Dieser Vertrag unterliegt der Gesetzgebung der Bundesrepublik Deutschland.