

KASPERSKY LAB

---

Kaspersky<sup>®</sup> Administration Kit 6.0

Erste Schritte

KASPERSKY® ADMINISTRATION KIT 6.0

---

# Erste Schritte

© Kaspersky Lab

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

Redaktionsdatum: Februar 2007

# Inhalt

|   |    |
|---|----|
| KAPITEL 1. VORWORT .....  | 4  |
| KAPITEL 2. ERSTE SCHRITTE .....   | 6  |
| 2.1. Installation von MSDE 2000.....  | 7  |
| 2.2. Installation der Komponente der Kaspersky-Lab-Anwendungen.....   | 8  |
| 2.3. Grundlegende Konfiguration des Antiviren-Schutzes .....  | 9  |
| 2.4. Erstellen einer Administrationsgruppe .....  | 11 |
| 2.5. Remote-Installation des Administrationsagenten.....  | 11 |
| 2.6. Remote-Installation einer Antiviren-Anwendung .....  | 13 |
| 2.7. Überprüfen der Update-Funktion für die Antiviren-Datenbanken der Client-<br>Computer .....                 | 14 |
| 2.8. Einstellungen für Benachrichtigungen .....   | 15 |
| 2.9. Überprüfen der Weitergabe von Benachrichtigungen und der Task zum<br>Scan auf Befehl.....                  | 16 |
| 2.10. Empfangen von Protokollen.....  | 16 |
| KAPITEL 3. WECHSEL KASPERSKY ADMINISTRATION KIT VON VERSION<br>5.X UND 6.0 ZU VERSION 6.0 (UPDATEPAKET 1) ..... | 18 |
| KAPITEL 4. NACHWORT .....   | 20 |
| ANHANG A. KASPERSKY LAB.....  | 21 |
| A.1. Andere Produkte von Kaspersky Lab .....  | 22 |
| A.2. Kontaktinformationen .....   | 33 |
| ANHANG B. ENDBENUTZER-LIZENZVERTRAG.....  | 35 |

---

# 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-Installationszenarium beschrieben, bei dem der Antiviren-Schutz nur auf einigen mit dem installierten Microsoft Windows Betriebssystem Computern ohne eine Hierarchie von Administrationsservern eingeführt wird. Eine Voraussetzung für die erfolgreiche Installation ist, dass diese Computer unter den folgenden Betriebssystemen arbeiten: Microsoft Windows 98; Microsoft Windows ME; Microsoft Windows Server 2003 und höher; Microsoft Windows Vista, Microsoft Windows Vista x64, Microsoft Windows 2000 mit Service Pack 1 und höher, Microsoft Windows XP Professional mit Service Pack 1 und höher, Microsoft Windows XP Professional x64 und höher, Microsoft Windows Server 2003 und höher, Microsoft Windows Server 2003 x64 und höher, Microsoft Windows NT4 mit Service Pack 6a und höher.

Das Dokument beschreibt außerdem das Vorgehen zum Wechsel von 5.x-Versionen der Antivirenanwendungen auf Version 6.x der Anwendungen.

[Ausführliche Informationen über die Anwendung Kaspersky Administration Kit finden Sie in der Einleitungshandbuch, dem Handbuch für den Administrator und im Nachschlagbuch.](#)

Die Anwendung Kaspersky Administration Kit dient der Verwaltung des Antiviren-Sicherheitssystems in einem Firmencomputernetzwerk. Mithilfe dieser Anwendung kann der Administrator:

- ein logisches Netzwerk erstellen, das für den Antiviren-Schutz der Firma sorgt.
- die Remote-Installation und Deinstallation von Antiviren-Schutz-Anwendungen der Firma vornehmen.
- die Antiviren-Schutz-Anwendungen zentralisiert im Remote-Betrieb verwalten.
- Benachrichtigungen über kritische Ereignisse bei der Arbeit von Antiviren-Schutz-Anwendungen erhalten.
- eine Statistik und Protokolle über die Arbeit der Antiviren-Schutz-Anwendungen erhalten.
- Lizenzverwaltung aller installierten Antivirusanwendungen ausführen.

- Zentralisiert die Objekte verwalten, welche von den Antivirusanwendungen in die Quarantäne oder Backupspeicher verschoben wurden.

Die Anwendung Kaspersky Administration Kit besteht aus folgenden Basiskomponenten:

- **Administrationsserver** – Diese Komponente erfüllt die Funktion der Speicherung der Informationen über die Kaspersky-Lab-Anwendungen, die den Antiviren-Schutz der Firma realisieren und dient der zentralisierten Verwaltung dessen. Der Administrationsserver führt die zentrale Speicherung von Informationen über den Antiviren-Schutz der Firma in einer Datenbank des Typs MSDE 2000 mit Service Pack 3 und höher oder Microsoft SQL Server 2000 mit Service Pack 3 und höher oder MySQL in der Version 5.0.32 (Code-Seite ist standardmäßig UTF-8) oder Microsoft SQL 2005 und höher oder Microsoft SQL 2005 Express und höher. Die Datenbanken 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 6.0 installiert werden. Vorsichtshalber sollte auf dem Computer das Programm Microsoft Data Access Components (MDAC) in der Version 2.8 und höher installiert sein.
- **Administrationsagent** – Diese Komponente realisiert die Zusammenarbeit des Administrationsserver mit den Kaspersky-Lab-Anwendungen, welche auf bestimmten Arbeitstationen oder Servern installiert sind. Diese Komponente ist einheitlich für alle Windows-Anwendungen von Kaspersky Lab, welche zur Gruppen Business Optimal und Kaspersky Corporate Suite gehören. Für Novell- und Unix-Anwendungen von «Kaspersky Lab» existieren eigene Versionen des Administrationsagenten
- **Administrationskonsole** – Diese Komponente bietet die Benutzeroberfläche für die administrativen Dienste des Agenten und Servers. 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 von Microsoft Data Access Components (MDAC) in der Version 2.8 und höher. Dieser Schritt entfällt, wenn diese Komponente bereits im Firmennetzwerk installiert ist.
2. Installation der Anwendung MSDE 2000 mit Service Pack 3 (s. Pkt. 2.1 auf S. 7) oder Microsoft SQL 2000 mit Service Pack 3 oder MySQL in der Version 5.0.32 oder Microsoft SQL 2005 und höher oder Microsoft SQL 2005 Express und höher. Dieser Schritt entfällt, wenn eine der Komponenten bereits im Firmennetzwerk installiert ist.
3. Installation des Administrationsservers und der Administrationskonsole (s. Pkt. 2.2 auf S. 8).
4. Basiskonfiguration und Einführung des Antiviren-Schutzsystems der Firma mit Hilfe des Schnellstart-Assistenten (s. Pkt. 2.3 auf S. 9).
5. Erstellen von Administrationsgruppen (s. Pkt. 8 auf S. 10), wenn sie nicht mithilfe des Schnellstart-Assistenten erstellt worden sind. Administrationsgruppen erlauben mit Hilfe von Richtlinien und Gruppentasks die einheitliche Verwaltung der in einer Gruppe enthaltenen Client-Computer.
6. Remote-Installation des Administrationsagenten auf ausgewählten Client-Computern zur Kommunikation zwischen Antiviren-Anwendungen und Administrationsserver (s. Pkt. 2.5 auf S. 11).
7. Remote-Installation von Kaspersky-Lab-Anwendungen, die für den Antiviren-Schutz des Unternehmens sorgen und die Verwaltung über Kaspersky Administration Kit (s. Pkt. 2.6 auf S. 13) verwalten, auf ausgewählten Client-Computern, falls diese noch nicht installiert sind.
8. Überprüfen der korrekten Funktion des Task Update-Empfang aus dem Internet durch den Administrationsserver. Überprüfen der korrekten Funktion des Update-Task auf den Client-Computern. Details s. Pkt. 2.7 auf S. 14.
9. 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).

10. Start den Task 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. 16).
11. 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 Microsoft SQL 2000 mit Service Pack 3 oder MySQL in der Version 5.0.32 oder Microsoft SQL 2005 und höher oder Microsoft SQL 2005 Express und höher vorhanden ist.

Vor der Installation von MSDE müssen die Microsoft Data Access Components (MDAC) in der Version 2.8 und höher (Paket steht auf Internetseiten von Microsoft zur Verfügung) installiert werden.

*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 lokal 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.

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, oder mit Hilfe des globalen Task

**Administrationsserver-Backup** (ausführliche Informationen finden Sie im Administratorhandbuch).

## 2.2. Installation der Komponente der Kaspersky-Lab-Anwendungen

Beim Installationsvorgang können benötigten Komponenten ausgewählt werden: **Administrationsserver**, **Posture Validation Server von "Kaspersky Lab" für Cisco NAC**, **Administrationsagent** oder die **Administrationskonsole**. Die Installation der Administrationskonsole und des Administrationsagenten können Sie nicht abwählen, beide Komponenten werden immer installiert. Posture Validation Server von "Kaspersky Lab" für Cisco NAC ist eine standardmäßige Komponente von "Kaspersky Lab" für die Arbeit mit Cisco Network Admission Control und wird in dieser Dokumentation nicht behandelt. Standardmäßig sind alle 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 6.x kann der gleiche sein, auf dem der Administrationsserver und/oder die Konsole der Version 5.x oder 6.x arbeiten.

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 die Variante **Logisches Netzwerk auf Basis des Windows-Netzwerks erstellen**. In diesem Fall wird das logische Netzwerk auf Basis der Struktur von Domänen und Arbeitsgruppen des Microsoft Windows-Netzwerks erstellt (die Administrationsgruppen stimmen mit den Microsoft Windows-Domänen und –Arbeitsgruppen überein).
6. Nehmen Sie die Einstellungen für das Senden von Benachrichtigungen per E-Mail und NET SEND über die Arbeit des Antiviren-Schutzes vor. Diese Werte können später in den Eigenschaften des Administrationsservers geändert werden (ausführliche Informationen siehe Administratorhandbuch).
7. Starten Sie den Vorgang zum Erstellen von Richtlinien für Antiviren-Anwendungen und für bestimmte Tasks, die 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. Tasks dienen den in Administrationsgruppen von den Anwendungen auszuführenden Aktionen.

Folgende Objekte werden erstellt:

- Richtlinien der obersten Ebene für Kaspersky Anti-Virus für Windows Workstation in den Versionen 5.0 und 6.0 mit Standardeinstellungen. Später können Sie die Parameter der Richtlinie anzeigen und ändern. Damit die Werte, die in der Richtlinie stehen, auf den Client-Computern zu gelten beginnen und der Benutzer sie nicht ändern kann, klicken Sie für diese Parameter auf das Symbol .
- Task Update-Download aus dem Internet durch den Administrationsserver mit Standardeinstellungen.

Dieser Task empfängt Updates der Antiviren-Datenbanken und Programmmodule von Kaspersky-Lab-Updateservern und speichert sie in einem freigegebenen Ordner, der bei der Installation des Administrationsservers festgelegt wurde. Die Client-Computer können die Updates unter Verwendung der freigegebenen Ordners empfangen. Des Weiteren lassen sich die Einstellungen für den Update-Download durch die Client-Computer noch flexibler gestalten, indem für die Verbreitung von Updates auf untergeordnete Administrationsserver und Update-Agenten zurückgegriffen wird (Details s. Handbuch für den Administrator). Klicken Sie auf die Schaltfläche **Task-Einstellungen**, um die Einstellungen für den Update-Download von den Kaspersky-Lab-Updateservern anzupassen.

- Gruppentask der obersten Ebene für Updates der Antiviren-Datenbanken auf den Client-Computern mit Standardeinstellungen (für die Kaspersky-Antivirus-Anwendung für Windows Workstations Versionen 5.0 und 6.0). Dieser Task 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.
  - Gruppentask mit Standardeinstellungen zum Scan auf Befehl für die Client-Computer (für die Kaspersky-Antivirus-Anwendung für Windows Workstations Versionen 5.0 und 6.0).
8. Geben Sie an, ob der Task Update-Download durch den Administrationsserver sofort oder nach einem Zeitplan zu starten ist.

9. Im letzten Fenster geben Sie an, ob der Assistent für Remote-Installation sofort nach dem Beenden des Schnellstart-Assistenten zu starten ist.

## 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**. Geben sie den Namen der neuen Gruppe ein und klicken Sie auf **OK**.
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, oder wählen Sie in dem Kontextmenü das Befehl Erstellen/Computer und folgen Sie den Anweisungen des Assistenten.

Um Computer mit Berücksichtigung von bestimmten Kriterien zusammenzustellen, die dann in eine Administrationsgruppe verschoben werden sollen, klicken Sie auf den Eintrag **Computer suchen** im Kontextmenü (oder auf den analog lautenden Eintrag im Menü **Aktion**). Nähere Informationen finden Sie im Handbuch für den Administrator.

Eine detaillierte Beschreibung des Updateprozesses von Kaspersky Administration Kit Versionen 5.x und 6.0 auf die Version 6.0 (Updatepaket 1) s. Kapitel **Error! Reference source not found.** auf S. **Error! Bookmark not defined.**

## 2.5. Remote-Installation des Administrationsagenten

*Zur Remote-Installation des Administrationsagenten*

1. Starten Sie in der Administrationskonsole den Assistenten zur Remote-Installation aus dem Kontextmenü des Administrationssservers.

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 Computer oder die erstellte Administrationsgruppe an.
4. Stellen Sie die Parameter für den Task Remote-Installation ein.
5. Geben Sie bei Bedarf das Benutzerkonto für den Zugriff auf die Client-Computer an. Wenn das Benutzerkonto des Administrationsservers über Administratorrechte für die Client-Computer verfügt, verwenden Sie standardmäßig das Benutzerkonto.
6. Beim folgenden Schritt des Assistenten wird der Gruppentask Remote-Installation des Administrationsagenten für die festgelegten Client-Computer erstellt und gestartet. Im Fenster des Assistenten können Sie in Echtzeit die aktuellen Ergebnisse der Taskausführung verfolgen.
7. Schließen Sie das Fenster des Assistenten für Remote-Installation, nachdem die Installation des Administrationsagenten für alle Client-Computer abgeschlossen wurde und die Ergebnisse angezeigt wurden.
8. Damit der Administrationsserver zu beliebiger Zeit eine Verbindung mit dem Administrationsagenten herstellen kann, muss auf dem Client-Computer der UDP-Port Nummer 15000 geöffnet sein. Wenn sich der UDP-Port nicht öffnen lässt, setzen Sie ein Häkchen in das Kontrollkästchen **Verbindung mit Administrationsserver nicht unterbrechen** auf der Registerkarte **Allgemein** im Einstellungsfenster für die Parameter des Client-Computers **Eigenschaften: <Computername>**.

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.

Wenn die Remote-Installation erfolgreich verlaufen ist, der Administrationsagent aber keine Verbindung mit dem Administrationsserver herstellen konnte, verwenden Sie die Utility **klmagchk.exe**. Dieses Hilfsprogramm gehört zum Lieferumfang des Administrationsagenten und befindet sich nach dessen Installation im Wurzelverzeichnis der Komponente. Beim Starten aus der Befehlszeile liefert die Utility eine detaillierte Diagnose zu den Verbindungseinstellungen mit dem Administrationsserver. Eine ausführliche Beschreibung der Utility finden Sie im Nachschlagebuch.

## 2.6. Remote-Installation einer Antiviren-Anwendung

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

Einige Kaspersky-Lab-Anwendungen, die mit dem Kaspersky Administration Kit, verwaltet werden können, können nur lokal auf Client-Computern installiert werden (Details s. Handbücher zu den jeweiligen Anwendungen).

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

1. Erstellen Sie mit Hilfe des Assistenten ein Paket 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. Geben Sie die Lizenzschlüsseldatei an, 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 des Administrationservers.
3. Führen Sie die Remote-Installation der Anwendung Kaspersky Anti-Virus for Windows Workstation durch. Das Vorgehen zur Remote-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 5.x for Windows Workstations erfolgen. In diesem Fall wird Kaspersky Anti-Virus Version 5.x automatisch entfernt und an seiner Stelle Kaspersky Anti-Virus Version 6.0 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-Task 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 den Task **Update-Download** durch den **Administrationsserver**. Diese Task wird vom Schnellstart-Assistenten erstellt und befindet sich im Element **Tasks** der obersten Ebene der Konsolenstruktur. Der Task 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 Taskausführung abgeschlossen wird.

Die Ergebnisse der Taskausführung 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/avupdates>).

2. Starten Sie die Gruppentask zum Update auf den Client-Computern. Diese Task wird vom Schnellstart-Assistenten erstellt und befindet sich im Ordner **Gruppentasks** des Elements **Gruppen**. Warten Sie, bis die Taskausführung abgeschlossen wird.

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

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



- aus dem gemeinsamen Ordner auf dem Administrationsserver
- aus dem freigegebenen Ordner auf dem Hauptadministrationsserver (mit Beachtung der Serverhierarchie)

- von den Update-Servern bei Kaspersky Lab
- unter Verwendung eines FTP- oder HTTP-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 Gruppentask 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, in dem Sie die Häkchen in den entsprechenden Kästchen setzen: (✉ – E-Mail,  – NET SEND,  – ausführende Datei starten), definieren Sie die Parameter in der Registerkarte **Einstellungen** in dem Eigenschaftfenster des Ereignisses.

Um die Weitergabe von Benachrichtigungen zu überprüfen (s. Pkt. 2.9 auf S. 16), ist es ausreichend, die Benachrichtigung über die Ereignisse **Virus wurde gefunden** und **Auffinden der Viren, Würmer, Trojaner und Hackerprogramme** auszuwählen.

3. Verwenden Sie das Symbol  für die von Ihnen installierten Parameter, damit die Einstellungen für alle Client-Computer übernommen werden. Damit die Änderungen in Kraft treten, gehen Sie zu der Registerkarte **Übernehmen** über, klicken Sie auf den Hyperlink **Erweitert** und in dem darauf folgenden Fenster klicken Sie auf die Schaltfläche **Übernehmen**.
4. Die Richtigkeit der installierten Parameter prüfen Sie, indem Sie manuell eine Benachrichtigung verschicken. Klicken Sie dazu auf der Registerkarte **Benachrichtigung** in dem Eigenschaftfenster des Ereignisses auf die Schaltfläche **Überprüfen**. Es öffnet sich daraufhin das

Fenster für den Versand einer Testnachricht. Sollte ein Fehler auftreten, erscheint eine entsprechende Information.

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

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

1. Versuchen Sie, den "Testvirus" **Eicar** auf einen geschützten Computer zu kopieren. Die Kopieroperation wird gesperrt werden (wenn der Task Echtzeitschutz 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 den Task Echtzeitschutz für das Dateisystem auf dem Client-Computer. Kopieren Sie den "Virus" **Eicar** auf den Client-Computer. Aktivieren Sie erneut den Task Echtzeitschutz für das Dateisystem.
3. Starten Sie den Gruppentask zum Scan auf Befehl der Client-Computer. Während der Taskausführung 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. Empfangen 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 13 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 Programmversionen
- Protokoll über Virenaktivität
- Protokoll über Drittanwendungen
- Protokoll über Netzangriffe
- Zusammengefasster Protokoll über Anwendungstypen
- Zusammengefasster Protokoll über Anwendungen für Arbeitsstationen und Fileserver
- Zusammengefasster Protokoll über Anwendungen für Perimeterschutz
- Zusammengefasster Protokoll über Anwendungen zum Schutz der Mailserver

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 KASPERSKY ADMINISTRATION KIT VON VERSION 5.X UND 6.0 ZU VERSION 6.0 (UPDATEPAKET 1)

Dieser Abschnitt beschreibt das Vorgehen zum Wechsel von Kaspersky Administration Kit der Version 5.x und 6.x auf die Version 6.0 (Updatepaket 1). Dabei wird die Struktur des logischen Netzwerkes für die Anwendungen Kaspersky Anti-Virus 6.x for Windows Workstations oder Kaspersky Anti-Virus 6.x for Windows Servers erstellt. Spezielle Besonderheiten des Wechsels wurden teilweise bereits in den vorhergehenden Abschnitten beschrieben. Hier wird das Szenarium vollständig dargestellt.

Das typische Wechselszenarium sieht folgendermaßen aus:

1. Es wird ein Backup der Daten des installierten Administrationsserver für Kaspersky Administration Kit der früheren Version mit Hilfe des Werkzeuges **klbackup.exe** erstellt. Dieses Werkzeug ist in dem Distributiv von Kaspersky Administration Kit enthalten und befindet sich in dem Hauptinstallationsverzeichnis. Bitte beachten Sie, dass eine Kopie des Administrationsserver zum Wiederherstellen der Daten benötigt wird. Dieser Parameter ist zwingend unter Benutzung des Werkzeuges **klbackup.exe**.
2. Der Administrationsserver der Version 6.0 (Updatepaket 1) wird im Firmennetzwerk installiert. Dieser kann auf dem gleichen Computer installiert werden, auf dem bereits der Administrationsserver der Version 5.x oder 6.x läuft. Beim Updaten der Versionen 5.x oder 6.x auf die Version 6.0 (Updatepaket 1) werden alle Daten und Einstellungen der vorigen Version des Administrationsserver und/oder Administrationskonsole gespeichert.
3. Die Struktur des logischen Netzwerkes (Administrationsgruppen) für die Anwendungen der Version 5.x und 6.x wird erstellt.
4. Richtlinien und Gruppentasks für die Anwendungen der Version 5.x und 6.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.

5. Die Computer, für welche der Wechsel von Version 5.x zu Version 6.x erfolgt, werden ausgewählt.
6. Ein Installationspaket zur Remote-Installation für die Version-5.x- und 6.x-Anwendungen wird erstellt. Die Antiviren-Anwendungen der Version 5.x und 6.x werden auf den ausgewählten Computern installiert. Dabei werden die Antiviren-Anwendungen der älteren Versionen automatisch entfernt und die Antiviren-Anwendungen der neueren Versionen installiert. Die Computer, auf denen die Installation von Antiviren-Anwendungen der Version 5.x und 6.x erfolgte, werden dem logischen Netzwerk des Administrationsservers der Version 6.0 (Updatepaket 1) hinzugefügt.

Stufenweise wird der gesamte Antiviren-Schutz der Firma, welche auf Basis der Antiviren-Anwendungen der Version 5.x und 6.x aufgebaut ist, durch das Administrationssystem der Version 6.0 (Updatepaket 1) 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 des Update-Task für die Antiviren-Datenbanken von Client-Computern.
- Überprüfen der Funktion des Task Echtzeitschutz.
- Erstellen und Starten des Task 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

## Das Unternehmen

Kaspersky Lab ist ein weltweit führendes Unternehmen in den Bereichen Viren-, Spam- und Hacker-Schutz. Unser hoch spezialisiertes Viren-Labor reagiert stets schneller als alle anderen auf neue Bedrohungen, so dass unsere innovativen Programme seit vielen Jahren Heimanwender und Unternehmen jeder Größe zuverlässig schützen.

Bereits 1997 wurde Kaspersky Lab von dem russischen Virenexperten Eugene Kaspersky in Moskau gegründet und hat heute unter anderem Niederlassungen in Deutschland, Frankreich, Großbritannien, Polen, Japan, USA und China.

## Einzigartige Erfahrung

Weltweit beschäftigt Kaspersky Lab über 550 hochspezialisierte Mitarbeiter, darunter Mitglieder der Computer Anti-Virus Researchers Organisation (CARO) und des Virus Bulletin Technical Advisory Board. Im Laufe vieler Jahre Forschung und Kampf gegen Computerviren haben wir Wissen und Fähigkeiten erworben, die heute unser wertvollstes Kapital darstellen.

Dank unserer weit reichenden Erfahrung sind wir in der Lage, Entwicklungstrends bei Malware vorherzusehen. Dieser einzigartige Vorteil bildet die Basis der Produkte und Dienstleistungen von Kaspersky Lab, so dass wir anderen immer einen Schritt voraus sind und unseren Kunden stets den besten Schutz bieten können.

## Kaspersky Anti-Virus

Nach vielen Jahren innovativer Entwicklungen zählt Kaspersky Lab heute zu den führenden Herstellern von Sicherheits-Software. Der hohe Standard unserer Produkte wird durch zahlreiche Auszeichnungen internationaler Forschungseinrichtungen, unabhängiger Testlabors und renommierter Fachpublikationen bestätigt.

Die Programm-Module unseres bekanntesten Programms, Kaspersky Anti-Virus, gewährleisten einen zuverlässigen Schutz für Workstations, Datei- und Web-Server, Mail-Gateways, Firewalls, Pocket-PCs und Smartphones.

Als erstes Unternehmen entwickelte Kaspersky Lab bedeutende Technologien, die heute selbst bei zahlreichen Antiviren-Programmen anderer Hersteller – wie G-Data, Aladdin und F-Secure – als Programm-Kern einen unverzichtbaren Bestandteil bilden. So vertrauen bereits über 200 Millionen Anwender unseren Innovationen, wie dem heuristischen Analysator zur Entdeckung noch unbekannter Viren, den Micro-Updates für die Antiviren-Datenbanken und dem ersten umfassenden Virenschutz für Unix/Linux-Systeme.

## **Komplexe Technologien für Ihre Sicherheit**

Moderne Viren und Schadprogramme sind komplexe Bedrohungen, so dass die bisher üblichen Schutzpakete für PCs und Netzwerke häufig nicht mehr ausreichen.

Aus diesem Grund entwickelte Kaspersky Lab mit Kaspersky Anti-Hacker eine Personal Firewall und mit Kaspersky Anti-Spam einen besonders effektiven Spam-Filter. Mit den Produkten von Kaspersky Lab können Sie Ihren Computer und Ihr Netzwerk optimal vor allen modernen virtuellen Gefahren schützen.

### **Service**

Kaspersky Lab bietet seinen Kunden eine ganze Palette zusätzlicher Dienstleistungen, die einen maximalen Schutz garantieren: Die Antiviren-Datenbanken werden stündlich aktualisiert, die Anti-Spam-Dateien 12 bis 24 Mal pro Tag. Zudem steht allen Anwendern ein rund-um-die-Uhr-Support zur Verfügung: Telefonisch oder per E-Mail – in deutscher, englischer, russischer und französischer Sprache.

# **A.1. Andere Produkte von Kaspersky Lab**

## **Kaspersky Lab News Agent**

Das Programm News Agent dient der schnellen Zustellung der Nachrichten von Kaspersky Lab, der Benachrichtigung über das "Virus-Wetter" und über neu erschienene Nachrichten. Das Programm liest in vorgegebenen Zeitabständen von den Kaspersky-Lab-Newsservern eine Liste der verfügbaren Nachrichtenkanäle und der darin enthaltenen Informationen.

News Agent verfügt außerdem über folgende Funktionen:

- Visualisierung des Zustands des "Viren-Wetters" im Infobereich der Taskleiste.
- Abonnieren und Abbestellen der Nachrichtenkanäle von Kaspersky Lab.
- Download von Nachrichten für jeden abonnierten Kanal in festgelegten Zeitabständen. Außerdem erfolgt eine Benachrichtigung über ungelesene Nachrichten.
- Anzeige von Nachrichten der abonnierten Kanäle.
- Anzeige einer Liste der Kanäle und ihrer Status.
- Öffnen der Webseite mit dem vollständigen Nachrichtentext im Browser.

News Agent funktioniert unter dem Betriebssystem Microsoft Windows. Er kann als separates Programm benutzt werden oder zu unterschiedlichen integrierten Lösungen von Kaspersky Lab gehören.

### **Kaspersky® OnLine Scanner**

Dieses Programm ist ein kostenloser Dienst, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antiviren-Untersuchung des Computers im Online-Modus erlaubt. Kaspersky OnLine Scanner wird direkt im Browser ausgeführt. Dadurch kann der Benutzer schnell eine Antwort auf Fragen erhalten, die mit einer Infektion durch schädliche Programme verbunden sind. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

### **Kaspersky® OnLine Scanner Pro**

Dieses Programm stellt einen Abonnementsdienst dar, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antiviren-Untersuchung des Computers und die Desinfektion infizierter Dateien im Online-Modus erlaubt. Kaspersky OnLine Scanner Pro wird direkt im Browser ausgeführt. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in den Formaten txt und html in Berichten speichern.

### **Kaspersky Anti-Virus® 7.0**

Kaspersky Anti-Virus 7.0 dient dem Schutz eines PCs vor schädlichen Programmen. Dabei werden traditionelle Virenschutzmethoden auf optimale Weise mit neuen proaktiven Technologien vereinigt.

Das Programm erlaubt eine komplexe Antiviren-Untersuchung, die folgende Optionen umfasst:

- Antiviren-Untersuchung des Mail-Datenstroms auf Ebene des Datenübertragungsprotokolls (POP3, IMAP und NNTP für eingehende Mails und SMTP für ausgehende Mails) unabhängig vom verwendeten Mailprogramm, sowie Untersuchung und Desinfektion von Mail-Datenbanken.

- Antiviren-Untersuchung des Internet-Datenstroms, der mit HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.
- Antiviren-Untersuchung beliebiger einzelner Dateien, Ordner und Laufwerke. Außerdem sind vordefinierte Untersuchungsaufgaben für die Virenanalyse von kritischen Bereichen des Betriebssystems und von Objekten, die beim Start des Betriebssystem Microsoft Windows gestartet werden, vorhanden.

Der Proaktive Schutz umfasst:

- *Kontrolle über Veränderungen im Dateisystem.* Das Programm erlaubt es, eine Liste der Anwendungen anzulegen, deren Komponentenbestand kontrolliert werden soll. Dadurch lässt sich die Verletzung der Integrität von Anwendungen durch Schadprogramme verhindern.
- *Überwachung von Prozessen im Arbeitsspeicher.* Kaspersky Anti-Virus 7.0 warnt den Benutzer rechtzeitig, wenn gefährliche, verdächtige oder versteckte Prozesse auftreten oder wenn aktive Prozesse auf unerlaubte Weise verändert werden.
- *Überwachung von Veränderungen in der Registrierung des Betriebssystems* durch die Kontrolle des Zustands der Systemregistrierung.
- Die *Rootkit-Suche* zur Kontrolle von versteckten Prozessen erlaubt es, Bedrohungen abzuwehren, die unter Verwendung der Rootkit-Technologie schädlichen Code im Betriebssystem verstecken.
- *Heuristische Analyse.* Bei der Untersuchung eines Programms emuliert der heuristische Analysator seine Ausführung und protokolliert alle verdächtigen Aktionen wie beispielsweise das Öffnen einer Datei, das Schreiben in eine Datei, das Abfangen von Interrupt-Vektoren usw. Auf der Grundlage dieses Protokolls wird darüber entschieden, ob das Programm eine Vireninfektion verursachen kann. Die Emulation erfolgt isoliert in einer virtuellen Umgebung, wodurch eine Infektion des Computers ausgeschlossen wird.
- *Systemwiederherstellung* nach schädlicher Einwirkung von Spyware: Die Wiederherstellung wird durch die Speicherung aller Veränderungen in der Registrierung und im Dateisystem des Computers und durch das vom Benutzer initiierte Rückgängigmachen der Veränderungen ermöglicht.

## **Kaspersky® Internet Security 7.0**

Kaspersky Internet Security 7.0 ist eine komplexe Lösung für den Schutz eines PCs vor den wichtigsten Bedrohungen (Viren, Hackerangriffe, Spam und Spyware), denen Informationen unterliegen. Alle Komponenten lassen sich über eine einheitliche Benutzeroberfläche einstellen und steuern.

Die Funktion des Antiviren-Schutzes umfasst:

- *Antiviren-Untersuchung des Mail-Datenstroms* auf Ebene des Datenübertragungsprotokolls (POP3, IMAP und NNTP für eingehende Mails und SMTP für ausgehende Mails) unabhängig vom verwendeten Mailprogramm. Für die populären Mailprogramme Microsoft Office Outlook, Microsoft Outlook Express und The Bat! sind Plug-Ins und die Desinfektion von Mail-Datenbanken vorgesehen.
- *Antiviren-Untersuchung des Internet-Datenstroms*, der mit HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.
- *Schutz des Dateisystems*: Der Antiviren-Untersuchung können beliebige einzelne Dateien, Ordner und Laufwerke unterzogen werden. Außerdem sind vordefinierte Untersuchungsaufgaben für die Virenanalyse von kritischen Bereichen des Betriebssystems und von Objekten, die beim Start des Betriebssystems Microsoft Windows gestartet werden, vorhanden.
- *Proaktiver Schutz*: Das Programm führt die ununterbrochene Überwachung der Aktivität von Anwendungen und Prozessen durch, die im Arbeitsspeicher des Computers gestartet werden, verhindert gefährliche Veränderungen des Dateisystems und der Registrierung, und stellt das System nach schädlicher Einwirkung wieder her.

Der *Schutz vor Internetbetrug* beruht auf dem Erkennen von Phishing-Angriffen. Dadurch lässt sich der Diebstahl Ihrer vertraulichen Informationen verhindern (in erster Linie Kennwörter, Konto- und Kreditkartennummern, sowie Sperren der Ausführung gefährlicher Skripts auf Webseiten, Sperren von Pop-up-Fenstern und Werbebannern). Die Funktion zum *Sperren der automatischen Einwahl auf kostenpflichtige Internetressourcen* ermöglicht es, Programme zu identifizieren, die versuchen Ihr Modem für versteckte Verbindungen mit kostenpflichtigen Telefondiensten zu missbrauchen, indem diese Programme gesperrt werden. Das Modul *Schutz von vertraulichen Informationen* gewährleistet den Schutz vor dem unerlaubtem Zugriff und der Übertragung von Informationen mit vertraulichem Charakter. Die Komponente *Kindersicherung* bietet die Kontrolle über den Zugriff von Computerbenutzern auf Internetressourcen.

Kaspersky Internet Security 7.0 *erkennt Versuche zum Scannen der Ports Ihres Computers*, die häufig im Vorfeld von Netzwerkangriffen stattfinden, und wehrt bekannte Netzwerkangriffe erfolgreich ab. Auf der *Basis von vordefinierten Regeln* führt das Programm die Kontrolle aller Netzwerkaktionen durch und überwacht alle *eingehenden und ausgehenden Datenpakete*. Der *Stealth-Modus macht den Computer für die externe Umgebung praktisch unsichtbar*. In diesem Modus wird jede Netzwerkaktivität verboten, wenn sie nicht durch Ausnahmeregelungen erlaubt wird, die vom Benutzer festgelegt wurden.

Im Programm wird eine komplexe Methode zur Spam-Filterung eingehender Mails angewandt:

- Untersuchung nach schwarzen und weißen Adressenlisten (einschließlich Adressen von Phishing-Seiten)
- Phrasenuntersuchung im Mailtext
- Analyse des Mailtexts mit Hilfe eines lernfähigen Algorithmus
- Erkennung von Spam in Form von Grafiken

### **Kaspersky Anti-Virus Mobile**

Kaspersky Anti-Virus Mobile bietet den Antiviren-Schutz für mobile Geräte, die mit den Betriebssystemen Symbian OS und Microsoft Windows Mobile arbeiten. Das Programm erlaubt eine komplexe Antiviren-Untersuchung, die folgende Optionen umfasst:

- *Scan auf Befehl* des Arbeitsspeichers, der Speicherkarten, einzelner Ordner oder einer konkreten Datei eines mobilen Geräts. Beim Fund eines infizierten Objekts wird es in die Quarantäne verschoben oder gelöscht.
- *Echtzeit-Untersuchung*: Alle eingehenden und veränderten Objekte, sowie Dateien, auf die versucht wird zuzugreifen, werden automatisch untersucht.
- *Schutz vor sms- und mms-Spam*

### **Kaspersky Anti-Virus für File-Server**

Das Produkt schützt die Dateisysteme von Servern, die unter den Betriebssystemen Microsoft Windows, Novell NetWare, Linux und Samba laufen, zuverlässig vor allen Arten schädlicher Programme. Das Produkt umfasst folgende Anwendungen von Kaspersky Lab:

- [Kaspersky Administration Kit](#)
- [Kaspersky Anti-Virus for Windows Server](#)
- [Kaspersky Anti-Virus for Linux File Server](#)
- [Kaspersky Anti-Virus for Novell Netware](#)
- [Kaspersky Anti-Virus for Samba Server](#)

Vorzüge und Funktionen:

- *Echtzeitschutz der Dateisysteme von Servern*: alle Dateien der Server werden untersucht, wenn versucht wird, sie zu öffnen und auf dem Server zu speichern.
- *Verhinderung von Viren-Epidemien*

- *Scan auf Befehl* des gesamten Dateisystems oder bestimmter Ordner und Dateien
- *Einsatz von Optimierungstechnologien* bei der Untersuchung von Objekten des Serverdateisystems
- *Systemwiederherstellung nach einer Infektion*
- *Skalierbarkeit* im Rahmen der verfügbaren Systemressourcen
- *Berücksichtigung der Systemauslastung*
- *Verwendung einer Liste mit vertrauenswürdigen Prozessen*, deren Aktivität auf dem Server nicht vom Programm kontrolliert wird.
- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Speicherung von Sicherungskopien infizierter und gelöschter Objekte*, um sie bei Bedarf wiederherzustellen.
- *Isolierung verdächtiger Objekte* in einem speziellen Speicher
- *Benachrichtigungen über Ereignisse* bei der Arbeit des Produkts für den Systemadministrator
- *Ausführliche Berichtsführung*
- *Automatisches Update der Datenbanken* des Softwareprodukts.

### **Kaspersky Open Space Security**

Kaspersky Open Space Security realisiert eine neue Art des Herangehens an die Sicherheit moderner Unternehmensnetzwerke mit beliebigem Umfang. Dabei gewährleistet es den zentralen Schutz von Informationssystemen und unterstützt externe Arbeitsplätze und mobile Benutzer.

Das Softwareprodukt umfasst vier Produkte:

- Kaspersky Work Space Security
- Kaspersky Business Space Security
- Kaspersky Enterprise Space Security
- Kaspersky Total Space Security

Im Folgenden wird jedes Produkt genau beschrieben.

**Kaspersky Work Space Security** bietet den zentralen Schutz von Workstations innerhalb und außerhalb eines Unternehmensnetzwerks. Es schützt vor allen aktuellen Internet-Bedrohungen wie Viren, Spyware, Hackerangriffen und Spam.

Vorzüge und Funktionen:

- *Komplexer Schutz vor Viren, Spyware, Hackerangriffen und Spam*
- *Proaktiver Schutz vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.*
- *Personal Firewall mit IDS/IPS-System*
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Schutz vor Phishing-Angriffen und Spam*
- *Dynamisches Ressourcen-Management bei der vollständigen Untersuchung des Systems*
- *Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung*
- *Unterstützung von Cisco® NAC (Network Admission Control)*
- *Untersuchung von E-Mails und Internet-Traffic in Echtzeit*
- *Sperren von Pop-up-Fenstern und Werbebannern bei der Arbeit im Internet*
- *Sichere Arbeit in Netzwerken aller Art, einschließlich Wi-Fi*
- *Mittel zum Erstellen einer Notfall-CD zur Systemwiederherstellung, um die Folgen von Virenangriffen zu beheben.*
- *Flexibles Informationssystem für den Schutzstatus*
- *Automatisches Update der Datenbanken*
- *Vollständige Unterstützung von 64-Bit-Betriebssystemen*
- *Optimiert für Notebooks mit Intel® Centrino® Duo*
- *Möglichkeit zur Remote-Reparatur (Intel® Active Management - Intel® vPro™)*

**Kaspersky Business Space Security** bietet den optimalen Schutz für die Informationsressourcen einer Firma vor Internet-Bedrohungen. Es schützt Workstations und Dateiserver vor Viren, Trojanern und Würmern, und verhindert Virus-Epidemien. Zudem überwacht es die Integrität der Daten und ermöglicht den Benutzern den schnellen Zugriff auf Netzwerkressourcen.

Vorzüge und Funktionen:

- *Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung*

- *Unterstützung von Cisco® NAC (Network Admission Control);*
- *Schutz von Workstations und Dateiservern vor allen Internet-Bedrohungen*
- *Verwendung der iSwift-Technologie zur Vermeidung wiederholter Untersuchungen innerhalb eines Netzwerks*
- *Dynamische Auslastung der Serverprozessoren*
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Proaktiver Schutz für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.*
- *Untersuchung von E-Mail und Internet-Traffic in Echtzeit*
- *Personal Firewall mit IDS/IPS-System*
- *Schutz bei der Arbeit in Wi-Fi-Netzwerken*
- *Technologie zum Selbstschutz des Antiviren-Programms vor Schadprogrammen*
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Automatisches Update der Datenbanken*

### **Kaspersky Enterprise Space Security**

Das Produkt umfasst Komponenten zum Schutz von Workstations und Groupware-Servern vor allen aktuellen Internet-Gefahren. Viren werden aus dem E-Mail-Datenstrom gelöscht. Die Integrität der Daten sowie die schnelle und sichere Verfügbarkeit der Netzwerkressourcen werden gewährleistet.

Vorzüge und Funktionen:

- *Schutz für Workstations und Server vor Viren, Trojanern und Würmern*
- *Schutz der Mailserver Sendmail, Qmail, Postfix und Exim*
- *Untersuchung aller E-Mails auf einem Microsoft Exchange Server, einschließlich der gemeinsamen Ordner*
- *Bearbeitung von E-Mails, Datenbanken und anderen Objekten auf Lotus Notes/Domino-Servern*
- *Schutz vor Phishing-Angriffen und Spam*
- *Verhinderung von massenhaften E-Mails und Viren-Epidemien*
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung*

- *Unterstützung von Cisco® NAC (Network Admission Control);*
- *Proaktiver Schutz für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.*
- *Personal Firewall mit IDS/IPS-System*
- *Schutz bei der Arbeit in Wi-Fi-Netzwerken*
- *Untersuchung des Internet-Traffics in Echtzeit*
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Dynamisches Ressourcen-Management bei der vollständigen Untersuchung des Systems*
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Berichtssystem über den Status des Schutzsystems*
- *Automatisches Update der Datenbanken*

### **Kaspersky Total Space Security**

Diese Lösung überwacht alle ein- und ausgehenden Datenströme, E-Mails, Internet-Traffic und alle Netzwerkaktionen. Kaspersky Total Space Security umfasst Komponenten zum Schutz von Workstations und mobilen Geräten, gewährleistet den schnellen und sicheren Zugriff der Anwender auf die Informationsressourcen der Firma und auf das Internet. Außerdem garantiert es Sicherheit bei der Kommunikation per E-Mail.

Vorzüge und Funktionen:

- *Komplexer Schutz vor Viren, Spyware, Hackerangriffen und Spam auf allen Ebenen eines Unternehmensnetzwerks von der Workstation bis zur Internet-Gateway.*
- *Proaktiver Schutz für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.*
- *Schutz für Mailserver und Groupware-Server*
- *Echtzeit-Untersuchung des Internet-Datenverkehrs (HTTP/FTP), der in ein lokales Netzwerk eintrifft.*
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Sperren des Zugriffs auf infizierte Workstations*
- *Verhinderung von Viren-Epidemien*
- *Zentrale Berichte über den Schutzstatus*
- *Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung*
- *Unterstützung von Cisco® NAC (Network Admission Control);*
- *Unterstützung von Hardware-Proxyservern*

- *Filterung des Internet-Datenverkehrs* nach einer Liste vertrauenswürdiger Server, nach Objekttypen und nach Benutzergruppen
- *Verwendung der iSwift-Technologie zur Vermeidung wiederholter Untersuchungen* innerhalb eines Netzwerks
- *Dynamisches Ressourcen-Management* bei der vollständigen Untersuchung des Systems
- *Personal Firewall* mit IDS/IPS-System
- *Sichere Arbeit in Netzwerken aller Typen*, einschließlich Wi-Fi
- *Schutz vor Phishing-Angriffen und Spam*
- *Möglichkeit zur Remote-Reparatur* (Intel® Active Management - Intel® vPro™)
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Technologie zum Selbstschutz des Antiviren-Programms vor Schadprogrammen*
- *Vollständige Unterstützung von 64-Bit-Betriebssystemen*
- *Automatisches Update der Datenbanken*

### **Kaspersky Security für Mail-Server**

Kaspersky Security für Mail-Server schützt Mailserver und Groupware-Server gegen Schadprogramme und Spam. Das Produkt umfasst Anwendungen für den Schutz aller bekannten Mailserver wie Microsoft Exchange, Lotus Notes/Domino, Sendmail, Qmail, Postfix und Exim. Zudem kann auch ein separater Mail-Gateway organisiert werden. Zu dieser Lösung gehören:

- [Kaspersky Administration Kit](#)
- [Kaspersky Mail Gateway](#)
- [Kaspersky Anti-Virus for Lotus Notes/Domino](#)
- [Kaspersky Anti-Virus for Microsoft Exchange](#)
- [Kaspersky Anti-Virus for Linux Mail Server](#)

Funktionen:

- Zuverlässiger Schutz vor schädlichen und potenziell gefährlichen Programmen
- Spam-Filterung
- Scan von ein- und ausgehenden E-Mails und E-Mail-Anhängen
- Antiviren-Untersuchung aller E-Mails auf einem Microsoft Exchange Server, einschließlich der gemeinsamen Ordner

- Untersuchung von E-Mails, Datenbanken und anderen Objekten auf Lotus Notes/Domino-Servern
- Filterung von E-Mails nach Typen der Anhänge
- Isolierung verdächtiger Objekte in einem speziellen Speicher
- Komfortable Bedienung
- Verhinderung von Viren-Epidemien
- Monitoring für den Status des Schutzsystems mit Hilfe von Benachrichtigungen
- Berichtssystem über die Arbeit der Anwendung
- Skalierbarkeit im Rahmen der verfügbaren Systemressourcen
- Automatisches Update der Datenbanken

### **Kaspersky Security für Internet-Gateway**

Das Produkt gewährleistet allen Mitarbeitern eines Unternehmens den sicheren Zugriff auf das Internet. Die Lösung löscht automatisch alle schädlichen und potenziell gefährlichen Programme aus dem Datenstrom, der über die Protokolle HTTP und FTP eintrifft. Das Produkt umfasst:

- [Kaspersky Administration Kit](#)
- [Kaspersky Anti-Virus for Proxy Server](#)
- [Kaspersky Anti-Virus for Microsoft ISA Server](#)
- [Kaspersky Anti-Virus for Check Point FireWall-1](#)

Funktionen:

- Zuverlässiger Schutz vor schädlichen und potenziell gefährlichen Programmen
- Echtzeit-Untersuchung des Internet-Datenverkehrs (HTTP/FTP)
- Filterung des Internet-Datenverkehrs nach einer Liste vertrauenswürdiger Server, nach Objekttypen und nach Benutzergruppen
- Isolierung verdächtiger Objekte in einem speziellen Speicher
- Komfortable Bedienung
- Berichtssystem über die Arbeit der Anwendung
- Unterstützung von Hardware-Proxyservern
- Skalierbarkeit im Rahmen der verfügbaren Systemressourcen

- Automatisches Update der Datenbanken

### **Kaspersky® Anti-Spam**

Kaspersky Anti-Spam ist die erste in Russland entwickelte Software zum Spam-Schutz von kleinen und mittleren Unternehmen. 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 E-Mails 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 des Produkts. Die Datenbank-Updates erscheinen alle 20 Minuten.

### **Kaspersky Anti-Virus® for MIMESweeper**

Kaspersky Anti-Virus® for MIMESweeper bietet die Hochgeschwindigkeits-Antiviren-Untersuchung des Datenverkehrs auf Servern, die Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web verwenden.

Das Programm besitzt die Form eines Plug-Ins (Erweiterungsmoduls) und führt im Echtzeit-Modus die Antiviren-Untersuchung und die Bearbeitung der ein- und ausgehenden E-Mail-Nachrichten durch.

## **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.

Weitere Information erhalten Sie bei:

Kaspersky Labs GmbH  
Steinheilstraße 13  
85053 Ingolstadt

|   |  |
|---|--|
| Technischer Support                     | E-Mail: <a href="mailto:support@kaspersky.de">support@kaspersky.de</a>   |
| Allgemeine Informationen                | <a href="http://www.kaspersky.de/">http://www.kaspersky.de/</a><br><a href="http://www.viruslist.de/">http://www.viruslist.de/</a>   |
| Feedback zu unseren Benutzerhandbüchern | <a href="mailto:docfeedback@kaspersky.com">docfeedback@kaspersky.com</a><br>(Diese Adresse ist für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.) |

---

# ANHANG B. ENDBENUTZER- LIZENZVERTRAG

## Endbenutzer-Lizenzvertrag für die erworbene KASPERSKY LAB SOFTWARE

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 14 Tagen an die Einkaufsstelle zurück. Nach Eingabe des Aktivierungscode ist eine Rückgabe der Software ausgeschlossen.

Jede Bezugnahme auf "Software" schließt den Aktivierungscode oder die Schlüsseldatei ein, den Sie von Kaspersky Lab als Teil der Software erhalten.

Dieser EULA ist ein rechtsgültiger Vertrag zwischen Ihnen, dem Besitzer eines Exemplars der SOFTWARE (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:

- Sie sind berechtigt, eine Kopie der SOFTWARE auf einem einzigen Computer zu installieren und zu verwenden. Eine Mehrplatzlizenz der SOFTWARE, dürfen Sie auf so vielen Computern installieren, wie Sie Lizenzen erworben haben.
- Sie sind berechtigt, die installierte SOFTWARE innerhalb der erworbenen Lizenzdauer zu benutzen.

2. EINSCHRÄNKUNGEN

- 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. Sie sind nicht berechtigt, diese Software in automatischen, halbautomatischen oder manuellen Tools zu verwenden, welche dazu dienen, Virensignaturen, Virenerkennungsroutinen, sowie beliebige andere Daten oder Codes zum Erkennen von schädlichem Code oder Daten zu erstellen.

- Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.
- Supportleistungen. Nach Kauf und Aktivierung der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die Lizenzdauer. Supportleistungen verstehen sich wie folgt:
  - stündliche Updates der Antiviren-Datenbank
  - kostenloses Updates der Software
  - kostenlose technische Unterstützung sowohl per e-Mail als auch per Telefon mit KASPERSKY LAB

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:

- die SOFTWARE den Spezifikationen im wesentlichen entspricht.
- im Falle einer physikalischen Lieferung der Originaldatenträger frei von Material- und Herstellungsfehlern ist.
- das Programm korrekt auf den Datenträger aufgezeichnet ist, die Dokumentation sämtliche Informationen enthält, die KASPERSKY LAB für die Benutzung der Software für erforderlich hält.
- die SOFTWARE binnen 90 Tagen ab der ersten Installation oder dem ersten Download, falls richtig behandelt, der in der beiliegenden Dokumentation bestimmten Funktionalität entspricht und laut derer voll funktionsfähig ist.

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 NUTZUNGVERGNÜGEN 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 des Landes, indem das Produkt erworben wurde.