

«KASPERSKY LAB»

Kaspersky Anti-Virus[®] 5.7 für Linux Workstations

Administrator's guide

KASPERSKY ANTI-VIRUS® 5.7 FOR
LINUX WORKSTATIONS

Handbuch für Administratoren

© «Kaspersky Lab» Ltd.
<http://www.kaspersky.com/de/>
Redaktionsdatum: April 2007

Inhalt

KAPITEL 1. EINFÜHRUNG.....	6
1.1. Viren und schädliche Programme.....	6
1.2. Funktionen von Kaspersky Anti-Virus	7
1.3. Was ist neu in Version 5.7	8
1.4. Lizenzierungspolitik.....	8
1.5. Hardware- und Softwarevoraussetzungen.....	8
1.6. Lieferumfang.....	10
1.6.1. Lizenzvertrag.....	10
1.6.2. Textgestaltung.....	11
KAPITEL 2. ARBEITSALGORITHMUS DER ANWENDUNG.....	13
KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-VIRUS.....	15
3.1. Installation der Anwendung auf einem Linux-Computer	15
3.2. Installationsprozess	16
3.3. Konfigurationsprozess	16
3.4. Installation des Administrationsagenten.....	17
3.5. Administrationsagenten einstellen.....	18
3.6. Update-Prozess zur Version 5.7	18
3.7. Installation des Lizenzschlüssels	19
3.8. Anordnung der Dateien in den Verzeichnissen	20
3.9. Abschluss der Installation	22
KAPITEL 4. ARBEITEN MIT KASPERSKY ANTI-VIRUS.....	23
4.1. Update der Antiviren-Datenbanken.....	23
4.1.1. Automatisches Updaten der Antiviren-Datenbanken	25
4.1.2. Update der Antiviren-Datenbanken auf Befehl	26
4.1.3. Erstellen eines Netzwerkordners zum Speichern und Kopieren der Antiviren-Datenbanken	27
4.2. Antivirenschutz des Dateisystems	29
4.2.1. Untersuchungsbereich	29
4.2.2. Modus zur Untersuchung und Desinfektion von Objekten	31

4.2.3. Aktionen für Objekte.....	32
4.2.4. Scan auf Befehl eines einzelnen Ordners.....	33
4.2.5. Zeitgesteuerte Untersuchung eines Ordners.....	33
4.2.6. Zusätzliche Optionen: Verwendung von Skriptdateien	34
4.2.6.1. Desinfektion von infizierten Objekten in einem Archiv	34
4.2.6.2. Senden von Benachrichtigungen an den Administrator.....	35
4.3. Echtzeit-Antivirenschutz.....	36
4.4. Verwaltung von Lizenzschlüsseln	37
4.4.1. Informationen über den Lizenzschlüssel ansehen	38
4.4.2. Lizenzverlängerung.....	39
KAPITEL 5. ERWEITERTE EINSTELLUNGEN.....	41
5.1. Zusammenarbeit mit Webmin einstellen	41
5.2. Optimierung der Arbeit von Kaspersky Anti-Virus	42
5.3. Verschieben von Objekten in Quarantäne-Ordner	44
5.4. Modus zum Erstellen von Sicherheitskopien (Backup).....	46
5.5. Lokalisierung der Datums- und Uhrzeitanzeige.....	46
5.6. Parameter für die Erstellung von Protokollen für Kaspersky Anti-Virus.....	47
KAPITEL 6. ANWENDUNG MIT HILFE VON KASPERSKY ADMINISTRATION KIT VERWALTEN.....	50
6.1. Anwendung verwalten	51
6.1.1. Anwendungsparameter einstellen	53
6.1.1.1. Registerkarte Parameter, Abschnitt Echtzeitschutz: allgemeine Parameter	53
6.1.1.2. Registerkarte Parameter, Abschnitt Echtzeitschutz: Schutzbereich und geschützte Objekte	54
6.2. Tasks verwalten.....	54
6.2.1. Task erstellen.....	55
6.2.1.1. Lokale Tasks erstellen	56
6.2.1.2. Gruppentask erstellen	58
6.2.1.3. Globalen Task erstellen	58
6.2.2. Spezifische Taskparameter einstellen	59
6.2.2.1. Task Scan auf Befehl.....	60
6.2.2.2. Update-Task.....	60
6.2.3. Tasks Starten und Anhalten	61
6.3. Richtlinien Verwalten	61
6.3.1. Richtlinie erstellen	62

6.3.2. Richtlinienparameter ansehen und ändern.....	63
6.3.2.1. Schutzbereich-Einstellungen.....	65
6.3.2.2. Typ von den überprüfenden Dateien bestimmen	65
6.3.2.3. Aktionen an den Objekten einstellen.....	65
6.3.2.4. Zusätzliche Parameter einstellen	66
KAPITEL 7. DEINSTALLATION VON KASPERSKY ANTI-VIRUS.....	67
KAPITEL 8. TESTEN DER FUNKTIONALITÄT VON KASPERSKY ANTI-VIRUS ...	69
ANHANG A. ZUSÄTZLICHE ANWENDUNGSINFORMATIONEN.....	71
A.1. Konfigurationsdatei des Kaspersky Anti-Virus	71
A.2. Befehlszeilenoptionen der Komponente kavscanner	80
A.3. Rückgabewerte der Komponente kavscanner.....	83
A.4. Befehlszeilenoptionen der Komponente kavmonitor.....	84
A.5. Befehlszeilenoptionen der Komponente licensemanager	84
A.6. Rückgabewerte der Komponente licensemanager.....	85
A.7. Befehlszeilenoption der Komponente keepup2date.....	85
A.8. Rückgabewerte der Komponente keepup2date	87
A.1. Schlüssel der Befehlszeile der Komponente kavmiddleware.....	87
ANHANG B. HÄUFIGE FRAGEN.....	88
ANHANG C. «KASPERSKY LAB»	94
C.1. Weitere Produkte und Services von «Kaspersky Lab».....	95
C.2. Kontaktinformationen	105
ANHANG D. ENDBENUTZER-LIZENZVERTRAG.....	106

KAPITEL 1. EINFÜHRUNG

Mit der steigenden Anzahl der Computerbenutzer und der Möglichkeit des Austausches der Daten zwischen Benutzern mit Hilfe von Email und über das Internet, steigt auch die Gefahr der Infizierung der Computer mit Viren, wie auch Entwendung und Beschädigung der Information durch schädliche Programme.

Unter den gefährlichsten Quellen des Eindringens der schädlichen Programme sind:

Das Internet

Globales Informationsnetz ist die Hauptquelle der Verbreitung aller schädliche Programme. Normalerweise, werden die Viren und andere schädliche Programme auf den populären Internet-Seiten hinterlegt und als „nützliche“ Software ausgegeben. Eine Menge der Skripte, die automatisch beim Öffnen der Internet-Seiten gestartet werden, können auch schädliche Programme enthalten.

Elektronische Post

Emails, die in dem Postfach des Benutzers einkommen und da auch gespeichert werden, können Viren in sich tragen. Schädliche Programme können sowohl in den eingelegten Dokumenten, wie auch im Briefkörper sein. In der Regel, Emails beinhalten in sich Viren oder Netzwürmer. Beim Öffnen des Briefes oder beim Speichern auf der Festplatte können Sie Ihren Computer infizieren.

Eingreifbarkeiten in der installierten Software

So genannte „Lecks“ in Software sind Hauptstellen, die von Hackern für ihre Angriffe benutzt werden. Eingreifbarkeiten geben dem Hacker eine Möglichkeit Fernzugriff auf Ihren Computer zu bekommen, das bedeutet zu Ihren Dateien, zu den Ihnen zugängigen Netzwerk-Ressourcen und anderen Informationsquellen.

In Unix-Systemen sind die Viren wesentlich weniger verbreitet, als, z.B., in Windows-Umgebung. Das heißt aber nicht, dass die Informationsgefahren für Unix-Benutzer nicht existieren. Weiter werden wir die Arten der schädlichen Programme näher behandeln.

1.1. Viren und schädliche Programme

Damit Sie wissen, welche Gefahren ihre Daten bedrohen können, ist es nützlich zu wissen, welche schädlichen Programme es gibt und wie diese arbeiten. Insgesamt können schädliche Programme in drei Klassen unterteilt werden:

- **Netzwürmer (Worms)** – Die zu dieser Kategorie zählenden schädlichen Programme benutzen Netzwerkressourcen um sich zu verbreiten. Ihre Bezeichnung erhielt diese Kategorie auf Grund der für Würmer typischen Fähigkeit, durch Netzwerke und andere InformationScanäle zu "kriechen". Netzwürmer besitzen die Fähigkeit sich sehr schnell zu verbreiten. Diese Art der schädlichen Programme kann Dateien auf der Festplatte erstellen, aber auch nur den Arbeitsspeicher und keine weiteren Ressourcen des Computers beanspruchen (außer Arbeitsspeicher)
- **Viren (Viruses)** – Programme, die andere Programme befallen – fügen ihren eigenen Code ein, um die Steuerung beim Starten der infizierten Datei zu übernehmen. Diese einfache Definition erlaubt die Haupteigenschaft der Viren festzulegen: *Infizierung*. Die Verbreitungsgeschwindigkeit der Viren ist geringer, als bei Netzwürmern.
- **Trojanische Programme (Trojans)** - Ein Trojanisches Programm führt Aktionen aus, welche vom Benutzer nicht sanktioniert wurden. Sie können Daten auf der Festplatte vernichten, das System zum "Absturz" bringen, Information stehlen u.s.w. Diese Art schädlicher Programme infiziert keine Dateien, ist also kein Virus im klassischen Sinne; trojanische Programme sind nicht in der Lage selbständig auf ein Computer zu gelangen, sie werden von Angreifern als „nützliche Software“ getarnt verbreitet. Schäden von Trojanern können wesentlich gravierender sein, als die herkömmlicher Viren-Angriffe.

In der letzten Zeit verbreiten sich im Unix-Umfeld mehr *Netzwürmer und Trojanische Programme*.



Weiter im Text wird der Begriff „Virus“ zum bezeichnen von Viren, Trojanischen Programmen und Netzwürmern benutzt. Bestimmte schädliche Programme werden nur dann genauer bezeichnet, wenn es notwendig ist.

1.2. Funktionen von Kaspersky Anti-Virus

Die Anwendung **Kaspersky Anti-Virus® für Linux Workstation** (weiter auch Kaspersky Anti-Virus, *Anwendung*) ist zum Antiviren-Schutz der File-Server und Arbeitsstationen, die unter LINUX- -Betriebsystemen arbeiten, bestimmt.

Die Anwendung ermöglicht Ihnen:

- Echtzeitschutz des Dateisystems gegen schädlichen Code: aufgerufene Dateien werden abfangen; diese werden analysieren; infizierte Objekte desinfixiert oder gelöscht.

- Scan auf Befehl: infizierte und verdächtige Dateien werden gesucht (Untersuchungsbereiche können definiert werden; infizierte Objekte werden desinfiziert oder gelöscht).
- Verdächtige oder beschädigte Dateien in die Quarantäne zu verschieben.
- Ablegen einer Kopie infizierter Objekte im Backup-Speicher vor dem Desinfizieren oder Löschen. Wenn das Objekt wichtige Informationen enthält ist somit eine Wiederherstellung möglich.
- Das Update der Antiviren-Datenbanken; als Quelle für Updates dienen die Update-Server von „«Kaspersky Lab»“. Alternativ können auch lokale Ordner oder interne Server benutzt werden.
- Die Verwaltung und Einstellung des Kaspersky Anti-Virus Produktes mit Hilfe der Konfigurationsdatei und des Web-Interfaces, basierend auf dem des Programm Webmin und des Kaspersky Administration Kit.

1.3. Was ist neu in Version 5.7

In der Version **Kaspersky Anti-Virus 5.7 für Linux Workstation** wurden im Vergleich zu Version 5.5 folgende Änderungen vorgenommen:

- Hinzugefügt wurde eine Möglichkeit, das Programm mit Hilfe von Kaspersky Administration Kit einzustellen und zu verwalten.

1.4. Lizenzierungspolitik

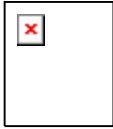
Die Lizenzierungspolitik für Kaspersky Anti-Virus bietet die Begrenzung für die Nutzung der Anwendung hinsichtlich der **Nutzungszeit** (in der Regel beträgt dieser Zeitraum ein Jahr ab dem Erwerb der Anwendung)

1.5. Hardware- und Softwarevoraussetzungen

Für die Arbeit von **Kaspersky Anti-Virus** sind folgende Systemvoraussetzungen erforderlich:

- Hardwarevoraussetzungen:
 - Prozessor der Pentium-Klasse.
 - Mindestens 32 MB Arbeitsspeicher.

- Mindestens 100 MB verfügbarer Festplattenspeicher.
- Softwarevoraussetzungen:
 - folgende Betriebssysteme für die 32 bit Plattform:
 - RedHat Enterprise Linux 5.2 Server (für File server), Desktop (für Workstation);
 - Fedora 9;
 - SUSE Linux Enterprise Server (für File server), Desktop (für Workstation) 10 SP2;
 - Novel Open Enterprise Server 2;
 - openSUSE Linux 11;
 - Debian GNU/Linux 4 R4;
 - Mandriva Corporate Server (für File server), Desktop (für Workstation) 4;
 - Ubuntu 8.04.1 Server (für File server), Desktop (für Workstation) Edition ;
 - Linux XP Enterprise Desktop 2008.
 - Folgenden Betriebssysteme für die 64 bit Plattform:
 - RedHat Enterprise Linux 5.2 Server (für File server), Desktop (für Workstation);
 - Fedora 9;
 - SUSE Linux Enterprise Server (für File server), Desktop (für Workstation) 10 SP2;
 - openSUSE Linux 11.
 - Programm Webmin (www.webmin.com) – zur entfernten Administration von Kaspersky Anti-Virus.
 - Perl Version 5.0 und höher (www.perl.org).
 - Installiertes which-Tool.
 - Installierte Pakete zur Programmkompilierung (gcc, binutils, **glibc-devel**, **make**, **ld**), sowie installierter Quellcode des Betriebssystemkernels – zur Programmkompilierung der Komponente *kavmonitor*.



Beachten Sie, dass Kaspersky Antivirus die gemeinsame Arbeit mit SELinux nicht unterstützt. Das Benutzen SELinux kann zur Warnungen im System-Log führen.

1.6. Lieferumfang

Das Softwareprodukt kann bei unseren Vertriebspartnern (als Hardcopy) oder in einem Online-Shop (z.B. www.kaspersky.com/de, Abschnitt **E-Store**) erworben werden.

Wenn Sie das Produkt als Hardcopy erwerben, umfasst der Lieferumfang des Softwareprodukts folgende Komponenten:

- versiegelter Umschlag mit einer Installations-CD, welche die Dateien des Softwareprodukts enthält.
- Benutzerhandbuch
- Lizenzschlüssel, der auf der Installations-CD oder auf einer separaten Diskette gespeichert ist.
- Lizenzvertrag

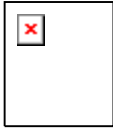


Bitte lesen Sie vor dem Öffnen des Umschlags mit der CD sorgfältig den Lizenzvertrag.

Beim Erwerb des Produkts in einem Online-Shop kopieren Sie das Produkt von der Kaspersky-Lab-Webseite. Die Distribution enthält neben dem eigentlichen Produkt auch das vorliegende Handbuch. Der Lizenzschlüssel ist entweder in der Distribution enthalten oder wird Ihnen nach Eingang der Bezahlung per E-Mail zugeschickt.

1.6.1. Lizenzvertrag

Der Lizenzvertrag ist eine rechtsgültige Vereinbarung zwischen Ihnen und „«Kaspersky Lab»“ Ltd., in der festgelegt wird, zu welchen Bedingungen Sie das von Ihnen erworbene Softwareprodukt verwenden dürfen.






Bitte lesen Sie den Lizenzvereinbarung sorgfältig!



Wenn Sie den Bedingungen des Lizenzvertrags nicht zustimmen, können Sie die Packung mit Kaspersky Anti-Virus an den Händler zurückgeben, bei dem Sie diese erworben haben, und der Kaufbetrag des Abonnements wird an Sie zurückerstattet. Voraussetzung dafür ist, dass der Umschlag mit der Installations-CD nicht geöffnet wurde.

Durch das Öffnen der versiegelten Packung mit der Installations-CD oder die Installation des Programms auf einem Computer akzeptieren Sie alle Bedingungen des Lizenzvertrags.

1.6.2. Textgestaltung

Bestimmte Textteile dieser Dokumentation sind in Abhängigkeit von ihrer Bedeutung durch unterschiedliche Formatierungselemente hervorgehoben. Die Textgestaltung wird in folgender Tabelle erläutert.

Formatierung		Bedeutung
Fette Schrift		Namen von Menüs, Menüelementen, Dialogfenstern, Elementen von Dialogfenstern, usw.
	Hinweis.	Zusatzinformationen, Hinweise.
	Achtung	Sehr wichtige Informationen.
 1. Schritt 1. 2. ...	<i>Um diese Aktion durchzuführen,</i>	Beschreibung einer Folge von Schritten und möglichen Aktionen, die vom Benutzer durchgeführt werden.

Formatierung		Bedeutung
	Aufgabe, Beispiel	Aufgabenstellung, Beispiel für die Realisierung der Optionen des Softwareprodukts.
	Lösung	Lösung der vorhergehenden Aufgabe.
[Parameter] – Funktion des Parameters.		Befehlszeilenparameter.
Text von Meldungen Befehlszeilen		Text von Konfigurationsdateien, informativen Meldungen des Programms und Befehlszeilen.

KAPITEL 2. ARBEITSALGORITHMUS DER ANWENDUNG

Kaspersky Antivirus enthält:

- die Komponente für den Scan auf Befehl *kavscanner*;
- die Komponente für den Echtzeitschutz *kavmonitor*;
- Antivirus-Datenbanken Updatemodul *keepup2date*;
- ein Werkzeug für die Lizenzschlüsselverwaltung *licensemanager*;
- eine Komponente für Fernverwaltung von Kaspersky Administration Kit *kavmiddleware*;
- Modul für die Fernsteuerung des Produktes über Webmin.

Folgend ein Beispiel für die Vorgehensweise von Kaspersky Anti-Virus anhand der Echtzeituntersuchung (Komponente *kavmonitor*).

Folgend der Arbeitsablauf:

1. Wenn eine Anwendung ein Objekt anspricht (Öffnen oder Schließen einer Datei) fängt das Kernel-Modul *kavmonitor* die Datei zum scannen ab.



Die Möglichkeit des abfangens der operationen der schließung der datei wird in den folgenden versionen des kernes nicht unterstützt:

- für die 32-bit-betriebssysteme: von der version des kernes 2.6.21 und mehr;
- für die 64-bit-betriebssysteme: von der version des kernes 2.6.21 und mehr.

2. Die Datei wird mit Hilfe Anti-Viren Daemons durchgeführt, welcher im *kavmonitor*-Modul enthalten ist. Dieser führt die Untersuchung des Objekts anhand der in der Konfigurationsdatei gewählten Parameter durch.
3. Nach dem Scan wird dem *kavmonitor*-Modul der Zugriffscodex (erlaubt/verboten) übergeben und der Status des Objektes definiert.
4. Dem Objektstatus entsprechend erlaubt oder blockiert *kavmonitor* den Zugriff auf die Datei.

Mögliche Dateistatus:

- **Clean** – Objekt ist nicht infiziert.
- **Infected** – Objekt ist infiziert.
- **Cured** – infiziertes Objekt wurde gesäubert.
- **CureFailed** – infiziertes Objekt konnte nicht gesäubert werden.
- **Warning** – Objektcode ist einem bekannten Virus ähnlich.
- **Suspicion** – Objekt kann mit einem unbekanntem Virus infiziert sein.
- **Protected** – Objekt kann nicht überprüft werden, es ist verschlüsselt.
- **Corrupted** – Objekt ist beschädigt.
- **Error** – Beim Überprüfen ist ein Fehler aufgetreten.

Aktionen am Objekt mit einem bestimmten Status werden von den Konfigurationsdatei-Parameter definiert (Details s. **Error! Reference source not found.** auf S. 71).

KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-VIRUS

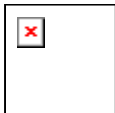
Wir empfehlen Ihnen, vor dem Beginn der Installation von Kaspersky Anti-Virus Ihr System folgendermaßen vorzubereiten:

- Stellen Sie sicher, dass das System den Hardware- und Softwarevoraussetzungen für die Installation von Kaspersky Anti-Virus entspricht (s. Pkt. 1.5 auf S. 10).
- Konfiguration der Internetverbindung.
- Anmeldung am System als Benutzer **root**.

3.1. Installation der Anwendung auf einem Linux-Computer

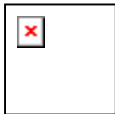
In Abhängigkeit der Distribution wird Kaspersky Anti-Virus in drei Installationsvarianten geliefert.

- **.rpm** – für Systeme, die RPM Package Manager unterstützen;
- **.deb** – für Debian- Distribution.
- **.tgz** – für die Installation ohne Paketmanager



Um die Installation von Kaspersky Anti-Virus aus dem rpm-Paket zu starten, geben Sie in der Befehlszeile ein:

```
rpm -i <Name_der_Distributionsdatei>
```



Um die Installation von Kaspersky Anti-Virus aus dem deb-Paket zu starten, geben Sie in der Befehlszeile ein:

```
dpkg -i <Name_der_Distributionsdatei>
```



Zum Start der Installation von Kaspersky Anti-Virus® aus dem pkg-Paket geben Sie in der Befehlszeile ein:

```
pkg_add < Paketname >
```

3.2. Installationsprozess

Die Installation der Anwendung wird in zwei Etappen durchgeführt und enthält folgende Schritte:

1. Benutzer kluser und Gruppe klusers erstellen.
2. Distributionsdateien auf den Computer entpacken
3. Dienste entsprechend dem Betriebssystem registrieren
4. Die Parameter in den Konfigurationsdateien der Komponente standardmäßig einstellen.

3.3. Konfigurationsprozess

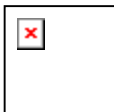
Zweite Etappe der Installation ist die Einstellung des Programms. Um die Einstellung vorzunehmen, benutzen Sie den Script *postinstall.pl*, welcher sich in dem Verzeichnis */opt/kaspersky/kav4ws/lib/bin/setup* befindet.

Die Installation erfolgt automatisch und enthält folgende Schritte:

1. Kopieren der Distributionsdateien auf den Computer
2. Installation des Lizenzschlüssels.

Wenn kein Lizenzschlüssel installiert ist, wird der Konfigurationsprozess nicht ausgeführt und die Arbeit mit der Anwendung ist nicht möglich. Sollte der Lizenzschlüssel vorübergehend nicht vorhanden sein (z.B. wenn die Anwendung über das Internet erworben wurde und der Lizenzschlüssel noch nicht per E-Mail eingetroffen ist), dann kann er nach dem Installationsprozess, direkt vor dem Beginn der Arbeit mit der Anwendung installiert werden. (Details über Installation des Lizenzschlüssels s. Pkt. 5.7.4 auf S. 37)

3. Konfiguration der Komponente *keepup2date*.
4. Installation (Update) der Antiviren-Datenbanken.



Beim Installieren der Anwendung unter OS Debian wird der Script des Konfigurationsprozesses automatisch gestartet.

Nach dem Starten des Scripts müssen Sie folgende Schritte ausführen:

1. Den Pfad zur Datei des Lizenzschlüssels angeben.
2. Parameter für Proxy-Server, welcher zur Verbindung mit dem Internet benutzt wird im folgenden Format einstellen

```
http://<IP-Adresse des Proxy-Servers>:<Port>
```

oder

```
http://<Benutzername>:<Passwort>@< IP-Adresse des Proxy-Servers>:<Port>,
```

abhängig davon, ob dieser Proxy-Server eine Authentifizierung verlangt. Dieser Wert wird von der Update-Komponente (*keepup2date*) der Anwendung für Verbindung mit den Updateservern von «Kaspersky Lab» zum Updaten der Antivirus-Datenbanken benutzt.

Wenn Sie keinen Proxy-Server für die Verbindung mit dem Internet benutzen, wählen Sie den Wert **no** für diesen Parameter.

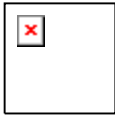
3. Antivirus-Datenbanken von den Servern des «Kaspersky Lab» kopieren. Geben Sie den Wert **yes** oder **no** ein, abhängig davon, ob Sie Update sofort durchführen wollen oder nicht.
4. Arbeit mit Webmin einstellen.
5. Kompilation des Moduls *kavmonitor* starten. In dieser Etappe werden die Bibliotheken kompiliert, welche für die Arbeit der Komponente *kavmonitor* nötig sind. Wenn die Quellcode des Kernels sich nicht im Standardmäßigen Verzeichnis befinden, geben Sie für die Kompilation des Moduls *kavmonitor* in der Befehlszeile ein:

```
# /opt/kaspersky/kav4ws/src/kavmon.pl -b [PATH]
```

wo [PATH] – der Pfad zu Quellcode des Kernels ist.

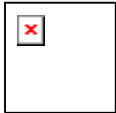
3.4. Installation des Administrationsagenten

Wenn Sie vor haben die Anwendung mit Hilfe von Kaspersky Administration Kit zu verwalten, dann müssen Sie den Administrationsagenten installieren.



Um den Administrationsagenten aus einem rpm-Paket zu installieren, geben Sie in der Befehlszeile ein:

```
# rpm -i <Distributivdatei_Name>
```



Um den Administrationsagenten aus einem deb- Paket zu installieren, geben Sie in der Befehlszeile ein:

```
# dpkg -i <Distributivdatei_Name>
```

3.5. Administrationsagenten einstellen

Nach der Installation muss der Administrationsagent für die Arbeit mit Kaspersky Administration Kit eingestellt werden. Um die Einstellung zu starten, benutzen Sie den Skript *postinstall.pl*, welcher sich in dem Verzeichnis */opt/kaspersky/klnagent/lib/bin/setup* befindet.



Beim Installieren des Administrationsagenten unter OS Debian wird der Script des Konfigurationsprozesses automatisch gestartet.

Nach dem Starten des Skriptes wird Ihnen angeboten folgende Schritte auszuführen:

1. DNS-Name oder IP-Adresse des Administrationsservers angeben.
2. Port-Nummer des Administrationsservers angeben.
3. SSL-Portnummer des Administrationsservers angeben.
4. Benutzung der SSL-Verbindung bestimmen.
5. Name der Standardmäßigen Administrationsgruppe angeben.

3.6. Update-Prozess zur Version 5.7



Update-Prozess funktioniert korrekt unter Version 5.5-27.

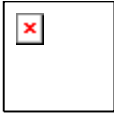
Vor dem Starten des Updateprozesses soll der Dienst *kavmonitor* angehalten werden. Geben Sie dazu in der Befehlszeile ein:

```
# /etc/init.d/kav4ws stop
```



Um Update-Prozess für Kaspersky Antivirus aus einem rpm-Paket zu starten; geben Sie in der Befehlszeile ein:

```
# rpm -U <Distributivdatei_Name>
```



Um Update-Prozess für Kaspersky Antivirus aus einem deb-Paket zu starten; geben Sie in der Befehlszeile ein:

```
# dpkg -i <Distributivdatei_Name>
```

Nach dem Beenden des Update-Prozesses wird die Konfigurationsdatei der Version 5.5 auf eine Datei der Version 5.7 ersetzt. Wenn es nötig ist, nehmen Sie Änderungen per Hand vor.

Ein Teil der standardmäßigen Parameter der Konfigurationsdatei (z.B., Pfad zum Verzeichnis, in dem die Antivirus-Datenbanken gespeichert werden) wird nicht exportiert, sondern während der Installation festgelegt.

Außerdem, sind in der Version 5.5 im Vergleich mit der Version 5.0 Änderungen an der Arbeit einigen Komponenten vorgenommen, wie auch eine Reihe an Optionen hinzugefügt worden. Deswegen wird es empfohlen die Richtigkeit der Ausführung von der Konfigurationsdatei zu überprüfen, bevor Sie die Anwendung benutzen.

3.7. Installation des Lizenzschlüssels

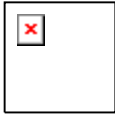
Auf dieser Etappe der Installation erfolgt im aktuellen Verzeichnis die Suche nach einem Lizenzschlüssel – nach einer Datei (mit der Dateinamenserweiterung *key*), welche für die Arbeit von Kaspersky Anti-Virus erforderlich ist. Diese Datei erlaubt den Zugriff auf die vollständige Funktionalität der Anwendung. Vor der Installation des Lizenzschlüssels ist die Arbeit mit Kaspersky Anti-Virus nicht möglich.

Wenn ein Lizenzschlüssel gefunden wird, werden entsprechende Informationen auf der Konsole angezeigt und der Installationsprozess geht zur nächsten Etappe über, die in der Installation der Antiviren-Datenbanken besteht.

Wenn kein Lizenzschlüssel gefunden wird, wird der Administrator aufgefordert, den vollständigen Pfad des Lizenzschlüssels anzugeben. Sollte kein Schlüssel vorhanden sein dann muss der Schritt zur Pfadangabe des Lizenzschlüssels abgelehnt werden, um dann den Installationsprozess fortgesetzt werden.

Sobald der Lizenzschlüssel vorliegt, muss dieser installiert werden (Details auf S. 37).

3.8. Anordnung der Dateien in den Verzeichnissen



Nach dem Kaspersky Antivirus auf eine Linux-Workstation installiert ist, werden die Dateien der Distribution wie folgt verteilt:

/etc/opt/kaspersky/ – Verzeichnis, in dem die Konfigurationsdatei des Kaspersky Antivirus liegt:

kav4ws.conf – Konfigurationsdatei.

/etc/init.d/kav4ws/ – Script zur Verwaltung des Dienstes *kavmonitor*.

/opt/kaspersky/kav4ws/ – Hauptverzeichnis des Kaspersky Antivirus, der enthält:

/bin/ – Verzeichnis, in dem die ausführenden Dateien aller Komponente des Kaspersky Antivirus liegen:

kav4ws-kavscanner – Ausführende Datei der Komponente des Antivirus-Schutzes;

kav4ws-keepup2date – Ausführende Datei der Komponente des Updates der Antivirendatenbanken;

kav4ws-licensemanager – Ausführende Datei der Komponente für die Verwaltung von Lizenzschlüsseln.

/lib/ – Verzeichnis, in dem die Dienstdateien des Kaspersky Antivirus.

/setup/ – Verzeichnis, welcher Skripts zur Einstellung der Anwendung:

postinstall.pl – Skript des Konfigurationsprozesses der Anwendung.

uninstall.pl – Skript zur Deinstallation der Anwendung.

setup.pl – Skript zur Einstellung der Anwendung.

/man/ – Verzeichnis zum Speichern der man-Dateien.

/sbin/ – Verzeichnis zum Speichern der Services des Kaspersky Antivirus:

kav4ws-kavmonitor – ausführende Datei der Komponente des Antivirusschutzes.

kav4ws-kavmiddleware – ausführende Datei der Komponente der Fernverwaltung *kavmiddleware*.

/src/ – Verzeichnis zum Speichern des Antivirus Kernel-Modules der Anwendung.

/opt/kaspersky/kav4ws/share/contrib/kav4ws.wbm – Plug-In für das Programm Webmin.

/opt/kaspersky/kav4ws/share/contrib/vox.sh – Skript *vox.sh*, wird zum säubern der Archive benutzt.

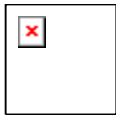
/opt/kaspersky/kav4ws/share/doc/LICENSE – Lizenzvereinbarung.

/opt/kaspersky/kav4ws/share//man/ – Verzeichnis zur Speicherung der man-Dateien.

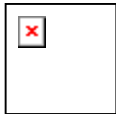
/var/opt/kaspersky/kav4ws/bases – Verzeichnis zum Speichern der Antivirus-Datenbanken.

/var/opt/kaspersky/kav4ws/bases.backup – Verzeichnis zum Speichern der aktuellen Antivirus-Datenbanken bis zum letzten Update.

/var/opt/kaspersky/kav4ws/licenses – Verzeichnis zur Speicherung der Lizenzinformation.



Um das Hilfe-System des Kaspersky Antivirus zu installieren (manual pages) geben Sie der Variable **MANPATH** den Wert **/opt/kaspersky/kav4ws/man**.



Nachdem Administrationsagent auf einem Computer mit dem Linux-Betriebssystem installiert ist, werden die Dateien des Administrationsagenten wie folgt verteilt:

/opt/kaspersky/klnagent/ – Hauptverzeichnis des Administrationsagenten, welcher enthält:

/bin/ – Verzeichnis, welcher die ausführende Dateien der Werkzeuge für Administrationsagenten enthält, unter anderen:

klmover – dieses Werkzeug ist für die Verbindung mit dem Administrationsserver bestimmt ist (für Detaillierte Informationen s. «Handbuch für Kaspersky Administration Kit»);

klnagchk – dieses Werkzeug ist für die Überprüfung der Verbindung mit dem Administrationsserver bestimmt ist (für Detaillierte Informationen s. «Handbuch für Kaspersky Administration Kit»);

/lib/ – – Verzeichnis, welcher die zusätzliche Dateien des Administrationsagenten enthält.

/bin/setup – Verzeichnis, welcher Skripts zur Einstellung des Administrationsagenten enthält;

/share/man/ – Verzeichnis zum Speichern der man-Dateien.

/sbin/ – Verzeichnis, welcher die ausführende Datei des Dienstes für Administrationsagenten enthält.

3.9. Abschluss der Installation

Wenn alle oben beschriebenen Installationsschritte erfolgreich abgeschlossen wurden, erscheint eine entsprechende Meldung in der Konsole. Die Konfigurationsdatei, die zum Lieferumfang der Anwendung gehört, enthält alle erforderlichen Einstellungen für den Beginn der Arbeit.

Eine Reihe von Parametern wird nicht während des Installationsprozesses der Anwendung festgelegt. Diese Parameter helfen aber bei dem Benutzen von Kaspersky Anti-Virus im vollen Umfang. Wir empfehlen deswegen die Einstellungen nach der Installation vorzunehmen (s. **Error! Reference source not found.** auf S. **Error! Bookmark not defined.**).

KAPITEL 4. ARBEITEN MIT KASPERSKY ANTI-VIRUS

Mit Kaspersky Anti-Virus können Sie Ihren Computer schützen: von einer einzelnen Datei bis zum gesamten Dateisystem.

Die Funktionalität der Anwendung unterstützt den Administrator bei unterschiedlichen Aufgaben. Alle mit Hilfe von Kaspersky Anti-Virus realisierbaren Aufgaben können in drei Gruppen unterteilt werden:

- Update der Antiviren-Datenbanken, die zur Suche von Viren und zur Desinfektion infizierter Objekte verwendet werden. (Details s. Pkt. 4.1 auf S. 23).
- Antivirenschutz von Computerdateisystemen (Untersuchung nach Zeitplan und/oder auf Befehl) (Details s. Pkt. 4.2 auf S. 29)
- Echtzeit-Antivirenschutz (Schutz im Echtzeitmodus) (Details S.36).

In diesem Kapitel betrachten wir die typischen Aufgaben, die am häufigsten bei der Arbeit mit Kaspersky Anti-Virus auftauchen. Im Rahmen eines Unternehmens kann der Administrator diese kombinieren und komplexer gestalten.

4.1. Update der Antiviren-Datenbanken

Ein obligatorischer Faktor des vollwertigen Antivirenschutzes ist die Aktualisierung der Antiviren-Datenbanken, die von der Anwendungskomponente *keepup2date* ausgeführt wird. Als Quelle für die Updates der Antiviren-Datenbanken, die von Kaspersky Anti-Virus während des Such- und Desinfektionsprozesses infizierter Objekte verwendet werden, dienen u.a. folgende Kaspersky-Lab-Updateserver:

<http://downloads1.kaspersky-labs.com/>

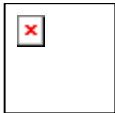
<http://downloads2.kaspersky-labs.com/>

<ftp://downloads1.kaspersky-labs.com/>

Eine Liste der Adressen, von denen die Updates kopiert werden können, befindet sich in der Datei */var/opt/kaspersky/kav4ws/bases/updcfg.xml*, die zum Lieferumfang der Anwendung gehört. Um die Liste der Update-Server anzuschauen, geben Sie in der Befehlszeile ein:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-keepup2date -s
```

Beim Updateprozess greift die Komponente *keepup2date* auf die genannte Liste zu, wählt eine Adresse aus und versucht, die Antiviren-Datenbanken vom Server herunterzuladen. Mit Hilfe des Parameters **RegionSettings** im Abschnitt **[updater.options]** der Konfigurationsdatei kann aktueller Region des Computers angegeben werden (als Buchstaben-Code, entsprechend ISO 3166-1). In dem Fall sucht die Komponente *keepup2date* neue Updates als erstes an den Servern, welche zur ausgewählten Region gehören. Wenn die Aktualisierung von der gewählten Adresse erfolglos ist, wendet sich die Komponente an die nächste Adresse und versucht erneut, die Datenbanken zu aktualisieren.

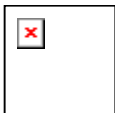


Updates für die Antiviren-Datenbanken werden jede Stunde auf den Servern des «Kaspersky Lab» veröffentlicht.



Sie können als Update-Quelle einen Server benutzen, welcher nicht «Kaspersky Lab» gehört. Antivirus-Datenbanken auf diesem Server können älter sein als die, welche auf dem Computer bereits installiert sind. Wenn Sie Update von so einem Server durchführen, werden alte Datenbanken die aktuellen ersetzen.

Nach einem erfolgreichen Update erfolgt standardmäßig der automatische Neustart der Anwendung (Parameter **PostUpdateCmd** im Abschnitt **[updater.options]**). Standardmäßig startet dieser Befehl die automatische Initialisation der Antiviren-Datenbanken. Inkorrekte Änderungen des Parameters können dazu führen, dass die Anwendung die Upgedateten Antiviren-Datenbanken nicht nutzen wird, oder inkorrekt funktionieren wird.



Alle Parameter der Komponente *keepup2date* befinden sich in den Optionen **[updater.*]** der Konfigurationsdatei.

Wenn die Struktur Ihres lokalen Netzwerks eine gewisse Komplexität aufweist, empfehlen wir, die Updates der Antiviren-Datenbanken von den Updateservern jede Stunde herunter zu laden, in einem speziellen Netzwerkordner zu speichern und für die lokalen Computer das Kopieren der Datenbanken aus diesem Ordner zu konfigurieren. Details über das Erstellen des Ordners s. Pkt. 4.1.3 auf S. 27.

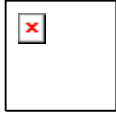
Die Aktualisierung lässt sich nach Zeitplan mit Hilfe des Programms **cron** (s. Pkt. 4.1.1 auf S. 25) oder auf Befehl des Administrators aus der Befehlszeile durchführen.



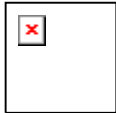
Es wird nachdrücklich empfohlen, die Antiviren-Datenbanken stündlich zu aktualisieren!

4.1.1. Automatisches Updaten der Antiviren-Datenbanken

Sie können die eine regelmäßige automatische Aktualisierung der Antiviren-Datenbanken durchführen, indem Sie einige Änderungen vornehmen.



Aufgabe: Stündliche automatische Updates der Antiviren-Datenbanken festlegen. Im Systemprotokoll sollen nur Programmfehler aufgezeichnet werden. In einem allgemeinen Protokoll werden alle Aufgabenstarts aufgezeichnet. Auf der Konsole werden keine Informationen angezeigt.



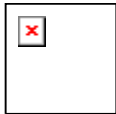
Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Legen Sie in der Konfigurationsdatei der Anwendung die entsprechenden Wert für die Parameter fest, z.B.:

```
[updater.options]
KeepSilent=yes
[updater.report]
Append=yes
ReportLevel=1
```

2. Ändern Sie die Datei, welche die Regeln für die Arbeit des Prozesses cron (**crontab -e**) festlegt. Geben Sie dazu folgende Zeile ein:

```
0 0-23/1 * * * /opt/kaspersky/ kav4ws/bin/kav4ws-keepup2date
```

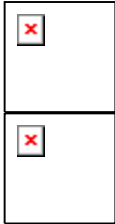


Aufgabe: Update der Antiviren-Datenbanken von den „Kaspersky Lab« Servern. Die Update-Quellen sollen aus der Liste entnommen werden, die zur Komponente *keepup2date* gehört.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

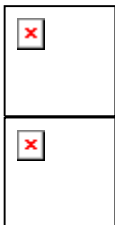
Vergeben Sie für den Parameter **UseUpdateServerUrl** im Abschnitt **[updater.options]** den Wert **No**.



Aufgabe: Ein Update der Antiviren-Datenbanken von einer vorgegebenen Adresse. Wenn das Updaten nicht möglich ist, soll der Update-Prozess angehalten werden.

Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

Vergeben Sie für die Parameter **UseUpdateServerUrl** und **UseUpdateServerUrlOnly** im Abschnitt **[updater.options]** den Wert **Yes**. Außerdem, soll der Parameter **UpdateServerUrl** die Adresse des Update-Servers enthalten.



Aufgabe: Ein Update der Antiviren-Datenbanken von einer vorgegebenen Adresse. Wenn das Updaten nicht möglich ist, sollen sie Server von «Kaspersky Lab» benutzt werden.

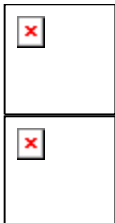
Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

Vergeben Sie für die Parameter **UseUpdateServerUrl** im Abschnitt **[updater.options]** den Wert **Yes** und dem Parameter **UseUpdateServerUrlOnly** den Wert **No**. Außerdem soll der Parameter **UpdateServerUrl** die Adresse des Update-Servers enthalten.

4.1.2. Update der Antiviren-Datenbanken auf Befehl

Die Aktualisierung der Antiviren-Datenbanken kann jederzeit aus der Befehlszeile gestartet mit Hilfe folgenden Befehls werden:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-keepup2date
```

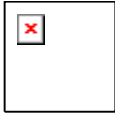


Aufgabe: Start des Updates der Antiviren-Datenbanken, Speichern der Prozessergebnisse in der Datei */tmp/updatesreport.log*.

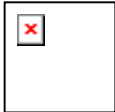
Lösung: Geben Sie zur Lösung dieser Aufgabe in der Befehlszeile ein:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-keepup2date -l /tmp/updatesreport.log
```

Wenn es erforderlich ist, die Antiviren-Datenbanken auf mehreren Computern zu aktualisieren, bietet sich an, anstelle des mehrmaligen Downloads der Datenbanken aus dem Internet, diese einmal von den Updateservern herunterzuladen, sie in einem speziellen Netzwerkordner zu speichern und die Datenbanken danach aus diesem Ordner zu aktualisieren.



Aufgabe: Das Update der Antiviren-Datenbanken aus dem Netzwerkordner **/home/bases**. Wenn dieser Ordner nicht verfügbar oder leer ist, erfolgt das Update von den Kaspersky-Lab-Servern. Die Prozessergebnisse werden in einer Protokolldatei **report.txt** aufgezeichnet.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Legen Sie in der Konfigurationsdatei der Anwendung die entsprechenden Wert für die Parameter fest:

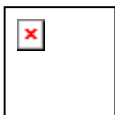
```
[updater.options]
UpdateServerUrl=/home/bases
UseUpdateServerUrl=yes
UseUpdateServerUrlOnly=no
```

2. Geben Sie in der Befehlszeile ein:

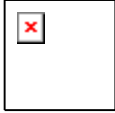
```
# /opt/kaspersky/kav4ws/bin/kav4ws -l
/tmp/report.txt
```

4.1.3. Erstellen eines Netzwerkordners zum Speichern und Kopieren der Antiviren-Datenbanken

Um die korrekte Weitergabe von Updates der Antiviren-Datenbanken aus einem bestimmten Ordner Ihres Netzwerks auf lokale Computer zu gewährleisten, muss in diesem eine Dateistruktur erstellt werden, die der Struktur der Kaspersky-Lab-Updateseiten entspricht. Folgend eine Beschreibung zum Erstellen dieses Netzwerkordners.



Aufgabe: Erstellen eines Netzwerkordners, aus dem die Antiviren-Datenbanken auf die Computer des lokalen Netzwerks kopiert werden.

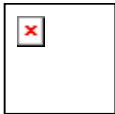


Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

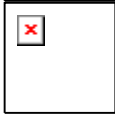
1. Erstellen Sie einen lokalen Ordner.
2. Starten Sie die Komponente *keepup2date* auf folgende Weise:

```
# kav4fs-keepup2date -u <dir>
```

wobei *dir* der vollständige Pfad des erstellten Ordners ist.
3. Erteilen Sie den lokalen Computern den Netzwerkzugriff auf diesen Ordner.



Aufgabe: Konfiguration des Updates der Antiviren-Datenbanken über einen Proxyserver.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Geben Sie im Abschnitt **[updater.options]** der Konfigurationsdatei für den Parameter **UseProxy** den Wert **Yes** an.
2. Vergewissern Sie sich, dass der Parameter **ProxyAddress** im Abschnitt **[updater.options]** der Konfigurationsdatei die Adresse des Proxyserver enthält. Die Adresse muss im folgenden Format angegeben werden:
http://username:password@ip_address:port. Dabei gelten die Werte **ip_address** und **port** als obligatorisch, **username** und **password** sind nur anzugeben, wenn die Autorisierung auf dem Proxyserver erforderlich ist.

Oder:

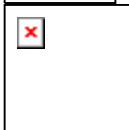
1. Geben Sie im Abschnitt **[updater.options]** der Konfigurationsdatei für den Parameter **UseProxy** den Wert **Yes** an.
2. Legen Sie die Umgebungsvariable **http_proxy** im Format **http://username:password@ip_address:port** fest. Beachten Sie, dass die Variable nur dann berücksichtigt wird, wenn der Parameter **UseProxy** im Abschnitt **[updater.options]** fehlt oder den Wert **Yes** besitzt.

4.2. Antivirenschutz des Dateisystems

Der Antivirenschutz von Dateisystemen erfolgt mit Hilfe der Komponente *kavscanner*, welche die Untersuchung ausführt und die Bearbeitung infizierter und verdächtiger Objekte entsprechend den Einstellungen vornimmt.



Alle Parameter der Komponente *kavscanner* befinden sich in den Optionen **[scanner.*]** der Konfigurationsdatei der Anwendung.



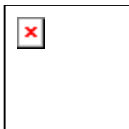
Standartmässig kann das Starten der Virensuche nach Befehl nur der Benutzer **root** ausführen.

Sie können sowohl den Scan des kompletten Dateisystems, wie auch eines einzelnen Ordners definieren. Volle Auswahl der Optionen kann man in Gruppen aufteilen, die folgendes definieren:

- Scan-Bereich.
- Modus zur Untersuchung und Desinfektion von Objekten (s. Pkt. 4.2.2 auf S. 31).
- Aktionen für Objekte (s. Pkt. 4.2.3 auf S. 32).
- Parameter zum erstellen der Protokolle. (s. Pkt. 5.6 auf S. 47).

Das Durchsuchen des Dateisystems kann folgendermaßen gestartet werden:

- Einmalig aus der Befehlszeile.
- Nach Zeitplan mit Hilfe des Programmes **cron** (s. Pkt. 4.2.5 auf S. 33).



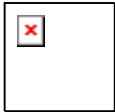
Das Scannen des ganzen Computers nach Viren ist eine sehr aufwendige Prozedur. Sie sollten daran denken, dass nach dem Starten des Scanvorgangs die Arbeitsgeschwindigkeit beeinträchtigt wird. Daher ist es nicht ratsam, irgendwelche Prozesse parallel zu starten. Um Probleme zu reduzieren, sollten Verzeichnisse einzeln gescannt werden.

4.2.1. Untersuchungsbereich

Scan-Bereich kann man in zwei Bereiche aufgeteilt werden:

- *Untersuchungspfad* – eine Liste der Ordner und Objekte, die untersucht werden;
- *Untersuchungsobjekte* – eine Auflistung der Objekt-Typen, die nach Viren untersucht werden (Archive u.s.w.).

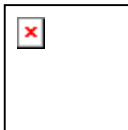
Standartmässig werden alle Objekte durchsucht, beginnend mit dem aktuellen Verzeichnis.



Zur Untersuchung des kompletten Dateisystems ist es erforderlich, in das Stammverzeichnis zu wechseln oder in der Befehlszeile den Untersuchungsbereich „/“ anzugeben.

Sie können den Scanbereich wie folgt definieren:

- Alle Verzeichnisse und Dateien, durch Leerzeichen getrennt, mit absolutem oder relativem Pfad direkt in der Befehlszeile beim Starten der Komponente aufzählen.
- Angabe des Untersuchungspfades in einer Textdatei und Festlegen der Verwendung dieser Datei in der Befehlszeile durch den Parameter **-@ <Dateiname>**. Jedes Objekt in dieser Datei wird in einer separaten Zeile und mit absoluter Pfadangabe angegeben.



Werden in der Befehlszeile sowohl der Untersuchungspfad als auch die Textdatei mit einer Liste von Untersuchungsobjekten angegeben, dann wird der in der Datei angegebene Bereich untersucht. Der in der Befehlszeile angegebene Pfad wird ignoriert.

- Einschränkung der Verzeichnisse, die standardmässig festgelegt sind (alle, beginnend mit dem aktuellen Verzeichnis) oder in der Befehlszeile aufgezählt werden. Dies kann in der Konfigurationsdatei **kav4ws.conf** festgelegt werden, indem Datei- und Ordnermasken angegeben werden, die aus dem Untersuchungsbereich ausgeschlossen werden sollen (Abschnitt **[scanner.options]**, Parameter **ExcludeMask** und **ExcludeDirs**).
- Deaktivieren der *rekursiven Untersuchung von Ordnern* (Abschnitt **[scanner.options]**, Parameter **Recursion** oder Befehlszeilenparameter **-r**).
- Erstellen einer alternativen Konfigurationsdatei und Festlegen der Verwendung dieser Datei durch den Befehlszeilenparameter **-c (-C) <Dateiname>** beim Start der Komponente.

Die standardmäßigen Untersuchungsobjekte werden ebenfalls in der Konfigurationsdatei **kav4ws.conf** (Abschnitt **[scanner.options]**) festgelegt und können geändert werden:

- direkt in dieser Datei;

- durch Befehlszeilenparameter beim Start der Komponente;
- durch Verwendung einer alternativen Konfigurationsdatei.

4.2.2. Modus zur Untersuchung und Desinfektion von Objekten

Das Anpassen dieser Untersuchungsoption ist sehr wichtig, da von ihr abhängt, ob die Desinfektion von infizierten Dateien, die bei der Untersuchung gefunden werden, erfolgt.

Diese Option ist standardmäßig deaktiviert. Das bedeutet, es erfolgt nur die Untersuchung von Objekten und die Benachrichtigung über den Fund von Viren und anderen verdächtigen oder beschädigten Dateien durch Meldungen auf der Konsole und im Protokoll (s. Pkt. 5.6 auf S. 47).

Als Ergebnis der Viruenuntersuchung erhält die Datei einen der folgenden Status:

- **Clean** – Es wurden keine Viren gefunden (Das Objekt ist nicht infiziert).
- **Infected** – Das Objekt ist infiziert.
- **Warning** – Der Code des Objekts besitzt Ähnlichkeit mit dem Code eines bekannten Virus.
- **Suspicious** – Der Code des Objekts ist verdächtig und könnte durch einen unbekanntes Virus infiziert sein.
- **Corrupted** – Das Objekt ist beschädigt.
- **Protected** – Das Objekt kann nicht untersucht werden, weil es verschlüsselt (durch Kennwort geschützt) ist.
- **Error** – Ein Fehler ist bei der Überprüfung aufgetreten.

Wenn der Desinfektionsmodus aktiviert ist (Abschnitt **[scanner.options]**, Parameter **Cure=yes**) werden nur Objekte mit dem Status **Infected** der Antivirenbearbeitung unterzogen. Als Ergebnis der Desinfektion erhält ein Objekt einen der folgenden Status:

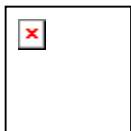
- **Cured** – Ein infiziertes Objekt wurde erfolgreich desinfiziert.
- **CureFailed** – Das Objekt konnte nicht desinfiziert werden. Eine Datei mit diesem Status wird nach den Regeln bearbeitet, die für infizierte Objekte gelten.
- **Error** – Beim Untersuchen ist ein Fehler aufgetreten.

4.2.3. Aktionen für Objekte

Abhängig vom Status eines Objektes (s. Pkt. 4.2.2 auf S. 31) können bestimmte Aktionen darauf angewandt werden. Standardmäßig erfolgt nur die Benachrichtigung über den Fund von Objekten mit einem bestimmten Status. Allerdings kann für Objekte mit den Status **Infected**, **Suspicious**, **Warning**, **Error**, **Protected** und **Corrupted** die Ausführung einer Reihe von Aktionen festgelegt werden:

- *Verschieben in einen bestimmten Ordner* – Verschieben von Objekten mit einem bestimmten Status in einen festgelegten Ordner. *Einfaches* und *rekursives Verschieben* ist möglich;
- *Löschen des Objektes* aus dem Dateisystem;
- *Ausführen eines bestimmten Befehls* – Bearbeitung von Dateien durch Unix-Standardbefehle, Skriptdateien usw.

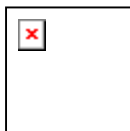
Es ist anzumerken, dass Kaspersky Anti-Virus zwischen einem gewöhnlichen Objekt (Datei) und einem Container-Objekt (das aus mehreren Objekten besteht, z.B. Archiv) unterscheidet. Auch die Aktionen, die mit solchen Objekten durchgeführt werden, werden unterschieden und in der Konfigurationsdatei in unterschiedlichen Abschnitten festgelegt: für einfache Objekte im Abschnitt **[scanner.object]**, für Container im Abschnitt **[scanner.container]**.



Die Aktionen für selbstextrahierende Archive sind nicht eindeutig: Ist das Archiv selbst infiziert, wird es als einfaches Objekt betrachtet, sind aber Objekte innerhalb des Archivs infiziert, als Container. Dementsprechend werden in solchen Fällen auch die Aktionen für Archive durch die Parameter unterschiedlicher Abschnitte der Konfigurationsdatei bestimmt!

Zur Auswahl der Aktion für bestimmte Objekte dienen folgende Methoden:

- Festlegen der Aktionen in der Konfigurationsdatei **kav4ws.conf**, wenn sie als Standardaktionen verwendet werden sollen (Abschnitte **[scanner.object]** und **[scanner.container]**).
- Festlegen der Aktionen in einer alternativen Konfigurationsdatei und Verwendung der Datei beim Start der Komponente.



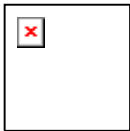
Wenn beim Start der Komponente in der Befehlszeile keine Konfigurationsdatei angegeben wird, dann werden die Funktionsparameter aus der Datei **kav4ws.conf** verwendet. Die Verwendung dieser Datei muss beim Start nicht gesondert angegeben werden!

- Festlegen der Aktionen für die laufende Session durch Befehlszeilenparameter beim Start der Komponente *kavscanner*.

Die Syntax der Aktionen ist für einfache Objekte und Container-Objekte identisch (Abschnitte **[scanner.object]** und **[scanner.container]**).

4.2.4. Scan auf Befehl eines einzelnen Ordners

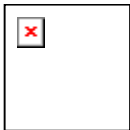
Eine der Aufgaben, die mit Kaspersky Anti-Virus gelöst werden können, ist die Untersuchung und Desinfektion eines bestimmten Verzeichnisses.



Aufgabe: Start der Untersuchung des Ordners */tmp* mit automatischer Desinfektion aller gefundenen infizierten Objekte. Alle Objekte, deren Desinfektion nicht möglich war, sollen gelöscht werden.

Im gleichen Ordner sollen die Dateien *infected.lst*, *suspicion.lst*, *corrupted.lst* und *warning.lst* erstellt werden, in denen in dieser Reihenfolge die Namen aller bei der Untersuchung gefundenen infizierten, verdächtigen oder beschädigten Objekte gespeichert werden.

Die Arbeitsergebnisse der Komponente (Startdatum, Informationen über alle Dateien außer virusfreien Objekten) sollen in der Protokolldatei *kav4w -kavscanner-aktuelles_Datum-pid.log* erscheinen, die im gleichen Ordner gespeichert wird.

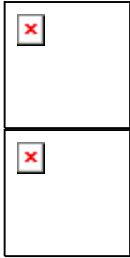


Lösung: Geben Sie zur Lösung dieser Aufgabe in der Befehlszeile ein:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-kavscanner -rlq -  
pi/tmp/infected.lst -ps/tmp/suspicion.lst -  
pc/tmp/corrupted.lst -pw/tmp/warning.lst -o  
/tmp/kav4ws-kavscanner-`date "+%Y-%m-%d-$$"` .log -i3  
-ePASBMe -j3 -mCn /tmp
```

4.2.5. Zeitgesteuerte Untersuchung eines Ordners

Der zeitgesteuerte Start von Programmen einschließlich der Aufgaben von Kaspersky Anti-Virus wird mit Hilfe des Programm **cron** durchgeführt.



Aufgabe: Die Viruenuntersuchung des Ordners **/home** soll jeden Tag um 0 Uhr 00 Minuten gestartet werden. Dabei sollen die Untersuchungsparameter verwendet werden, die in der Konfigurationsdatei `/etc/kav/scanhome.conf` angegeben sind.

Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Erstellen Sie die Konfigurationsdatei `/etc/kav/scanhome.conf` und geben Sie dort alle erforderlichen Untersuchungsparameter an.
2. Ändern Sie die Datei, welche die Regeln für die Arbeit des Prozesses cron (**crontab -e**) festlegt. Geben Sie dazu folgende Zeile ein:

```
0 0 * * * /opt/kaspersky/kav4ws/bin/kav4ws-
kavscanner -c /etc/kav/scanhome.conf /home
```

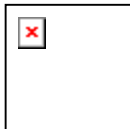
4.2.6. Zusätzliche Optionen: Verwendung von Skriptdateien

Kaspersky Anti-Virus bietet die Möglichkeit zur zusätzlichen Bearbeitung von Objekten, die der Antiviren-Analyse unterzogen wurden. Hierzu werden unterschiedliche Unix-Standardbefehle sowie Skriptdateien verwendet. Mit Hilfe solcher Werkzeuge können erfahrene Administratoren die Aktionen für Objekte mit unterschiedlichem Status selbständig festlegen und so die Funktionalität von Kaspersky Anti-Virus erweitern.

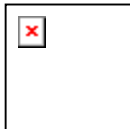
4.2.6.1. Desinfektion von infizierten Objekten in einem Archiv

Kaspersky Anti-Virus führt keine Desinfektion infizierter Dateien durch, die in Archive gepackt sind, erkennt aber die darin enthaltenen verdächtigen und infizierten Objekte. Allerdings kann die Desinfektion durch eine zusätzliche Skriptdatei realisiert werden. Im vorliegenden Handbuch wird ein Beispiel für die Desinfektion von Archiven des Typs `tar` und `zip` mit Hilfe der Skriptdatei `vox.sh` besprochen. Dieses Skript ist im Lieferumfang von Kaspersky Anti-Virus enthalten.

Das Skript entpackt die Datei, untersucht und bearbeitet einzelne Objekte und fügt diese anschließend wieder zu einem Archiv zusammen. Deswegen ist es erforderlich, dass im System Archivierungs-Programme installiert sind.



Aufgabe: mit Hilfe des Skripts `vox.sh` eine Archivuntersuchung eines `tar` oder `zip` Archives durchführen.



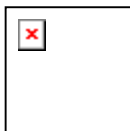
Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

In der Befehlszeile führen Sie aus:

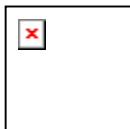
```
# /opt/kaspersky/kav4ws/share/contrib/vox.sh <Pfad zu  
der Archiv-Datei>
```

4.2.6.2. Senden von Benachrichtigungen an den Administrator

Durch die Verwendung von Unix-Standardwerkzeugen können Sie eine Benachrichtigung an den Administrator konfigurieren, die über den Fund von infizierten, verdächtigen und beschädigten Objekten informiert.



Aufgabe: Konfiguration einer Benachrichtigung des Administrators beim Fund infizierter Dateien und Archive bei jeder Untersuchung des Computers. Diese soll entsprechend der Parameter der Konfigurationsdatei `kav4ws.conf` ausgeführt werden. Bei der Untersuchung soll der Modus zur Öffnung von Symbolischen links eingeschaltet werden.

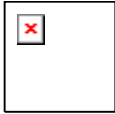


Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

Geben Sie in der Konfigurationsdatei `kav4ws.conf` die Bearbeitungsregeln für einfache Objekte und Container an:

```
[scanner.options]  
FollowSymlinks=yes  
[scanner.object]  
OnInfected=exec echo %FULLPATH%/%FILENAME% is  
infected by %VIRUSNAME% |  
mail -s kav4ws-kavscanner admin@localhost.ru
```

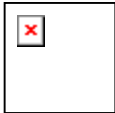
```
[scanner.container]
OnInfected=exec echo archive %FULLPATH%/%FILENAME% is
infected, viruses list is in the attached file %LIST%
| mail -s kav4ws-kavscanner -a %LIST% ad-
min@localhost.ru
```



Vor dem Starten muss der Benutzer sicherstellen, dass das Werkzeug **mail** sich im Standardmäßigen Pfad des Betriebssystems befindet.

4.3. Echtzeit-Antivirenschutz

Der Antivirenschutz im Echtzeitmodus wird durch die Komponente *kavmonitor* realisiert.



Alle Parameter der Funktion der Komponente *kavmonitor* sind in den Abschnitt **[monitor.*]** der Konfigurationsdatei zu finden.

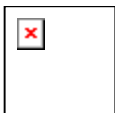
Die Komponente *kavmonitor* ist so konfiguriert, dass beim Zugriff auf Dateien (Öffnen, Schließen oder Starten) diese untersucht werden (beim Schließen wird die Datei nur untersucht, wenn Änderungen vorgenommen wurden). Standardmäßig werden alle angeforderten Objekte nach Viren und schädlichen Programmen untersucht, außer:

- Archive;
- Selbstentpackende Archive;
- Mail-Datenbanken;
- Email-Nachrichten.



Wenn ein symbolischer Link untersucht werden soll, wird das Objekt untersucht, zu dem dieser Link führt. Dies wird auch dann gemacht, wenn dieses Objekt aus der Überprüfung ausgeschlossen ist. Bei der Überprüfung der Verzeichnisse aus der Liste **IncludeDirs** werden die symbolischen Links nicht geöffnet.

Die Bearbeitung der Objekte wird, entsprechend der Parameter der Konfigurationsdatei, basierend auf den Ergebnissen durchgeführt.



Standardmäßig ist das Desinfizieren der gefundenen infizierten Objekte ausgeschaltet! Um die Option einzuschalten, geben Sie dem Parameter **Cure** im Abschnitt **[monitor.options]** der Konfigurationsdatei, den Wert **Yes**.

Für Objekte mit den Status **Infected**, **Suspicious**, **Warning**, **Error**, **Protected** und **CureFailed** kann die Ausführung einer Reihe von Aktionen festgelegt werden:

- *Verschieben in einen bestimmten Ordner* – Verschieben von Objekten mit einem bestimmten Status in einen festgelegten Ordner. *Einfaches* und *rekursives Verschieben* ist möglich;
- *Löschen des Objekts* aus dem Dateisystem;
- *Ein Befehl ausführen* – Dateien mit Hilfe von Unix-Standardbefehle, Skripte u.ä. bearbeiten.

Die Regeln der Bearbeitung der Objekte können in der Konfigurationsdatei festgelegt werden (Abschnitt **[monitor. actions]**).

Sie können auch weitere Einstellungen vornehmen:

- Mit Hilfe der Parameter **ExcludeDirs** und **ExcludeMask können** Ordner definiert werden, welche aus der Untersuchung ausgeschlossen werden.
- Die Benutzung der Technologien heuristischen Code-Analyse und iChecker.
- Die Auslastung des Servers verringern, indem Sie die maximale Anzahl der gleichzeitig zu untersuchenden Objekte begrenzen.



Wenn Sie die Anwendung mit Hilfe von Kaspersky Administration Kit verwalten werden, sollten Sie keine Änderungen an Abschnitten **[monitor.*]** der Konfigurationsdatei auf lokalem Computer vornehmen. Die Parameter dieser Abschnitte werden von den Einstellungen des Kaspersky Administration Kits überschrieben.

4.4. Verwaltung von Lizenzschlüsseln

Der Lizenzschlüssel gibt Ihnen das Recht zur Nutzung der Anwendung und enthält alle erforderlichen Informationen, die mit der von Ihnen erworbenen Lizenz verbunden sind. Dazu zählen: Typ der Lizenz, Ende der Gültigkeitsdauer der Lizenz, Händlerinformationen, usw.

Während der Gültigkeitsdauer der Lizenz bekommen Sie neben dem Recht zur Nutzung der Anwendung folgende Möglichkeiten:

- Technische Unterstützung (rund um die Uhr)
- stündliches Update der Antiviren-Datenbanken

- Aktualisierung der Anwendung (Patch)
- Download neuer Versionen der Anwendung (Upgrade)
- rechtzeitige Benachrichtigung über neue Viren

Bei Ablauf der Gültigkeitsdauer der Lizenz verlieren Sie automatisch das Recht auf die oben genannten Leistungen. Kaspersky Anti-Virus wird weiterhin die Antivirenbearbeitung der Dateien durchführen, dabei aber nur die Antiviren-Datenbanken verwenden, die am Ablaufdatum der Lizenzgültigkeit aktuell waren. Die Option des Updates der Antiviren-Datenbanken wird nicht mehr zugänglich sein.

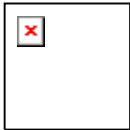
Aus diesem Grund ist es sehr wichtig, regelmäßig die im Lizenzschlüssel angegebenen Informationen zu überprüfen und das Ablaufdatum der Lizenzgültigkeit zu verfolgen.

4.4.1. Informationen über den Lizenzschlüssel ansehen

Sie können Informationen über die installierten Lizenzschlüssel in den Protokollen der Komponenten *kavscanner*, *kavmonitor* und *keepup2date* kontrollieren. Beim Start jeder dieser Komponenten werden Informationen über die Schlüssel geladen.

Ausserdem, verfügt Kaspersky Anti-Virus über die spezielle Komponente *licensemanager*, die es ermöglicht, nicht nur ausführliche Informationen über die Schlüssel, sondern auch bestimmte analytische Daten zu erhalten.

Alle Informationen können auf dem Bildschirm angezeigt werden.



Um Informationen über alle Lizenzschlüssel anzusehen,

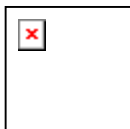
Geben Sie in der Befehlszeile ein:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-licensemanager -s
```

Auf dem Bildschirm erscheinen beispielsweise folgende Informationen:

```
Kaspersky license manager Version 5.7
Copyright (C) «Kaspersky Lab». 1997-2007.
Portions Copyright (C) Ian Crypto
License file 0003D3EA.key, serial 0038-000419-
0003D3EA, "Kaspersky Anti-Virus for Unix", expires
04-07-2003 in 28 days
```

```
License file 0003E3E8.key, serial 011E-000413-0003E3E8, "Kaspersky Anti-Virus for Linux File Srv (licence per e-mail address)", expires 25-01-2004 in 234 days
```



*Um Informationen über einen bestimmten Lizenzschlüssel anzu-
sehen,*

Geben Sie in der Befehlszeile ein:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-licensemanager -k <Name_der_Datei>  
Wo <Name_der_Datei> - Pfad und Dateiname des Schlüssels sind
```

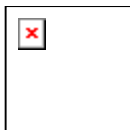
Auf dem Bildschirm erscheinen beispielsweise folgende Informationen:

```
Kaspersky license manager Version 5.7  
Copyright (C) «Kaspersky Lab». 1997-2007.  
Portions Copyright (C) Lan Crypto  
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus  
for Linux", expires 04-07-2003 in 28 days
```

4.4.2. Lizenzverlängerung

Die Verlängerung der Lizenz für die Nutzung von Kaspersky Anti-Virus gibt Ihnen das Recht auf die Wiederherstellung der vollen Funktionalität der Anwendung einschließlich der Aktualisierung der Antiviren-Datenbanken. Außerdem werden die Zusatzleistungen, die auf S. 37 genannt werden, erneuert.

Die Gültigkeitsdauer der Lizenz hängt vom Lizenzierungstyp ab, den Sie beim Erwerb der Anwendung gewählt haben.



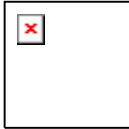
*Um die Lizenz für die Nutzung von Kaspersky Anti-Virus zu ver-
längern:*

setzen Sie sich mit der Firma in Verbindung, bei der Sie die Anwendung gekauft haben, und erwerben Sie eine Lizenzverlängerung für die Nutzung von Kaspersky Anti-Virus.

oder:

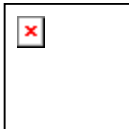
verlängern Sie die Lizenz direkt bei «Kaspersky Lab». Schreiben Sie dazu an die Verkaufsabteilung (sales@kaspersky.com) oder füllen Sie auf unserer Internetseite (www.kaspersky.com/de) im Abschnitt **PRO-**

DUKTE → Verlängern Sie Ihre Lizenz das entsprechende Formular aus. Nach Eingang der Bezahlung wird Ihnen der Lizenzschlüssel per E-Mail an die Adresse zugeschickt, die im Bestellformular angegeben wurde.



«Kaspersky Lab» führt regelmäßige Aktionen durch, die erlauben die Lizenzschlüssel für unsere Produkte mit erheblichen Nachlässen zu verlängern. Sie können über die Aktionen auf der «Kaspersky Lab» Internetseite in dem Abschnitt **Produkte→Aktionen und Sonderangebote** mehr erfahren.

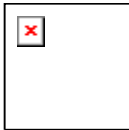
Nach dem Erwerb ist die Installation des neuen Lizenzschlüssels erforderlich.



Um den Lizenzschlüssel zu installieren, geben Sie in der Befehlszeile ein:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-licensemanager -a  
<Name der Schlüssel-Datei>
```

Es wird empfohlen, anschließend die Antiviren-Datenbanken zu aktualisieren (s. Pkt. 4.1 auf S. 23).



Um Lizenzschlüssel zu entfernen, Geben Sie in der Befehlszeile ein:

Um einen aktiven Lizenzschlüssel zu entfernen:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-licensemanager -da
```

Um zusätzlichen Lizenzschlüssel zu entfernen:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-licensemanager -dr.
```

KAPITEL 5. ERWEITERTE EINSTELLUNGEN

Dieses Kapitel beschreibt die zusätzlichen Funktionaleinstellungen von Kaspersky Anti-Virus. Sie dienen der Funktionalitätserweiterung der Anwendung und ihrer Anpassung an die Verwendungsbedingungen im Rahmen eines konkreten Unternehmens.

5.1. Zusammenarbeit mit Webmin einstellen

Wenn Sie vorhaben Kaspersky Anti-Virus fern zu administrieren, dann ist es ratsam die Zusammenarbeit mit dem Paket Webmin einzustellen.

Mit Hilfe von Webmin kann Zugang zum Programm begrenzt werden, indem Benutzerpasswörter vergeben werden.

Standardmäßig werden alle Einstellungen des Antivirus, welche mit Webmin gemacht wurden, in der Konfigurationsdatei der Anwendung gespeichert.



Wenn Sie eine alternative Konfigurationsdatei mit Hilfe von Webmin erstellen wollen, machen Sie folgendes:

1. Kopieren Sie die Daten aus der existierenden Konfigurationsdatei in eine neu, welche Sie unter einem anderen Namen speichern sollen. Danach verändern Sie die alternative Konfigurationsdatei entsprechend Ihren Bedürfnissen.
2. Den Namen der Konfigurationsdatei in der Registerkarte **Config edit** im Feld **Full path to KAV config** angeben.



Vollständige Information über unterschiedliche Einstellungen von Webmin sehen Sie in der Dokumentation zum diesen Produkt. Wenn Sie Fragen über die Fernadministration-Module haben, benutzen Sie das Hilfesystem des Programms Webmin.

Weiter im text beim Betrachten von Tasks wird die Arbeit über das Programm Webmin **nicht erwähnt!**

5.2. Optimierung der Arbeit von Kaspersky Anti-Virus

Zur Verringerung der Prozessorbelastung und zur Steigerung der Geschwindigkeit der Antivirenbearbeitung der Objekte, bietet Kaspersky Anti-Virus effektive Optimierungsmethoden für seine Arbeit.



Benutzung der Datenbank iChecker™ und der Technologie des zweistufigen Cashes der untersuchten Dateien.

Die Anwendung verwendet eine Reihe von Technologien, die es erlauben, die Antivirenuntersuchung einer Datei nicht bei jedem Zugriff auf die Datei durchzuführen, sondern möglichst auf eine Vergleichsoperation mit bereits darüber existierenden Daten zu beschränken. Der Algorithmus zur Untersuchung eines Objekts (einer Datei) auf Viren lässt sich folgendermaßen beschreiben:

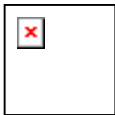
Bei der ersten Untersuchung einer beliebigen Datei werden Informationen darüber (Name, Kontrollsumme) in einer der folgenden Datenbanken gespeichert:

- Datenbank iChecker™ – Eine Datenbank, die Informationen über untersuchte **virusfreie** Dateien bestimmter Formate enthält. Diese Datenbank enthält Informationen über Objekte, die mit den Komponenten *kavmonitor* und *kavscanner* untersucht wurden.
- Cache der untersuchten Dateien – Eine Datenbank, die Informationen über die von der Komponente *kavmonitor* untersuchten Dateien enthält. Der Cache besteht aus zwei Stufen: Auf dem ersten Niveau werden Informationen über **virusfreie Dateien** gespeichert, auf die am häufigsten zugegriffen wird. Der Cache der ersten Stufe befindet sich im Kernmodul, wodurch die erforderliche Zugriffszeit wesentlich gesenkt wird. Wenn die Anwendung Daten über eine angeforderte Datei im ersten Cache findet, erhält es automatisch den Status **Clean** und es findet keine weitere Antivirenuntersuchung statt. Wenn der erste Cache die erforderlichen Informationen nicht enthält, erfolgt die Suche auf dem zweiten Niveau, das Daten **über alle untersuchten Dateien** enthält. Beide Cache-Datenbanken befinden sich im Arbeitsspeicher und werden beim Abschluss der Arbeit der Anwendung nicht gespeichert.

Daher, wenn bei der Untersuchung die Informationen über eine Datei nicht in die iChecker™-Datenbank aufgenommen werden (die Datei ist nicht virusfrei oder ihr Format wird von dieser Technologie nicht unterstützt), dann werden sie im Cache aufgenommen.

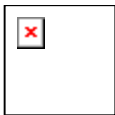
Bei jedem folgenden Zugriff eines Benutzers auf die Datei erfolgt die Suche zuerst im ersten Cache und dann (wenn das Objekt in der ersten Datenbank nicht gefunden wurde) in der iChecker™-Datenbank und auf der zweiten Cache-Stufe. Als Suchkriterium dient der Dateiname. Wird eine solche Datei in einer der Datenbanken gefunden, dann werden die Informationen über die Datei mit in der Datenbank vorhandenen verglichen. Unter der Voraussetzung der vollständigen Identität des aktuellen Objektzustands und seiner Beschreibung in der Datenbank wird die Datei als unverändert betrachtet und nicht auf das Vorhandensein von Viren untersucht.

Wenn weder in der iChecker-Datenbank noch im Cache Informationen über die angeforderte Datei gefunden werden, wird eine vollständige Antivirenuntersuchung der Datei durchgeführt.



Wenn Sie bei der Arbeit mit der Anwendung die Art der Antiviren-Datenbanken geändert haben, müssen Sie die Information aus der iChecker-Datenbank per Hand entfernen (kompletter Pfad zu der Datenbank wird durch den Parameter **IcheckerDbFile** im Abschnitt **[path]** in der Konfigurationsdatei bestimmt).

Das hängt damit zusammen, dass die Datenbank infizierte Objekte enthalten kann, die mit Standard-Versionen der Antiviren-Datenbanken nicht gefunden werden können, wurden aber mit den erweiterten erkannt. Wenn Informationen über Dateien in den iChecker Datenbanken gespeichert sind, werden diese Dateien nicht noch mal überprüft, was zur Infizierung des Computers führen kann.



Begrenzung der Prozessorbelastung.

Die Untersuchung des Dateisystems kann bei einem großen Datenvolumen viel Zeit beanspruchen, wobei die Prozessorbelastung wesentlich wächst. Gleichzeitig muss der Prozessor aber auch aktuelle Aufgaben ausführen, weshalb ein Mechanismus wünschenswert ist, welcher die Antivirenuntersuchung des Computers bei Überschreitung einer bestimmten Lastgrenze anhält.

Kaspersky Anti-Virus verfügt über einen solchen Mechanismus. In Version 5.7 der Anwendung wurde der Konfigurationsdatei der Parameter **MaxLoadAvg** im Abschnitt **[scanner.options]** hinzugefügt. Wenn der Parameter festgelegt wurde, überprüft *kavscanner* vor der Untersuchung jeder neuen Datei den aktuellen Wert der Prozessorbelastung **load average** und hält bei Überschreitung des in der Konfigurationsdatei angegebenen Werts die Arbeit von *kavscanner* an, bis der Wert auf den entsprechenden im Parameter **load average** sinkt.

Ausserdem, können Sie die Anzahl der gleichzeitig in Echtzeit zu überprüfenden Objekte mit Hilfe des Parameters **CheckFileLimit** im Abschnitt **[monitor.options]** der Konfigurationsdatei der Anwendung begrenzen. Das erlaubt Ihnen die Prozessorbelastung zu verringern und die Überprüfungsgeschwindigkeit für einzelne Objekte zu steigern.

Zusätzliche Maßnahme zur Entlastung des Systems ist das Abschalten von *kavmiddleware*. Dieser Dienst ist für Zusammenarbeit von Kaspersky Antivirus und Kaspersky Administration Kit bestimmt. Wenn Sie die Möglichkeit der Zusammenarbeit nicht benutzen, dann können Sie den Dienst *kavmiddleware* ausschalten. Dazu geben Sie in der Befehlszeile ein:

```
# /etc/init.d/kavmiddleware stop
```

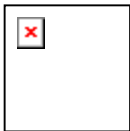
5.3. Verschieben von Objekten in Quarantäne-Ordner

Sie können die Arbeit von Kaspersky Anti-Virus so organisieren, dass alle infizierten Objekte des Dateisystems in einen separaten Ordner verschoben werden.

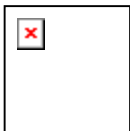
Diese Möglichkeit kann beispielsweise verwendet werden, wenn ein infiziertes Objekt nicht desinfiziert werden konnte. Beispielsweise wenn drei Viren, Dateien befallen haben, nur zwei entfernt werden konnten, die Datei aber wichtige Daten enthält.

Wenn der Ordner für isolierte Objekte in der Struktur des Dateisystems gespeichert werden soll, empfehlen wir, diesen für folgende Untersuchungen aus dem Scanbereich auszuschließen. Geben Sie dazu seinen vollständigen Pfad als Wert des Parameters **ExcludeDirs** im Abschnitt **[scanner.options]** der Konfigurationsdatei an.

Sehen wir uns eine Aufgabe zur Isolierung infizierter Objekte an, welche bei der Untersuchung auf Befehl oder beim Echtzeitschutz gefunden worden sind.



Aufgabe: Untersuchung aller Objekte, die in der Datei */tmp/download.lst* aufgezählt sind. Verschieben von gefundenen infizierten Objekten mit vollständigem Pfad in den Ordner */tmp/infected*. Informationen über infizierte, verdächtige und beschädigte Objekte werden in einer Protokolldatei aufgezeichnet.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Geben Sie als Aktionen für infizierte Objekte in den Abschnitten **[scanner.object]** und **[scanner.container]** der Konfigurationsdatei folgende Zeile an:

```
OnInfected=MovePath /tmp/infected
```

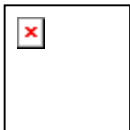
2. Deaktivieren Sie den Desinfektionsmodus (**Cure=no**), wenn dieser aktiviert war.
3. Geben Sie in der Befehlszeile ein:

```
# kav4fs-kavscanner -@/tmp/download.lst -ePASBME
-rq
-i0 -o /tmp/report.log -j3 -mCn
```

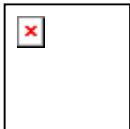
Diese Aufgabe lässt sich auch komplexer gestalten, indem gefordert wird, den Zugriff auf Dateien des Ordners */tmp/infected* auf Lesen und Schreiben zu beschränken. Dies kann mit Hilfe von Unix-Standardwerkzeugen (Befehl **chmod**) erreicht werden. Zur Lösung der Aufgabe sind folgende Änderungen erforderlich:

Geben Sie in den Abschnitten **[scanner.object]** und **[scanner.container]** der Konfigurationsdatei der Anwendung als Bearbeitungsregel für infizierte Objekte die folgende Zeile an:

```
OnInfected=exec mv %FULLPATH%/%FILENAME%
/tmp/infected/%FILENAME%; chmod -x
/tmp/infected/%FILENAME%
```



Aufgabe: Virusuntersuchung aller angeforderten Dateien; wenn ein Objekt von Viren befallen ist, soll die Desinfektion durchgeführt werden. Wenn diese misslingt, sollen die infizierten Objekte mit vollständigem Pfad in den Ordner ***/tmp/infected*** verschoben werden.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. In der Konfigurationsdatei der Anwendung aktivieren Sie den Desinfektionsmodus für infizierte Objekte (**Cure=yes** im Abschnitt **[monitor.options]**).
2. Geben Sie die Regeln der Isolation des infizierten Objekts. In dem Abschnitt **[monitor.actions]** der Konfigurationsdatei nehmen Sie folgende Einstellungen vor:

```
OnInfected=MovePath /tmp/infected
```

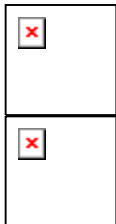
5.4. Modus zum Erstellen von Sicherheitskopien (Backup)

Wenn bei der Untersuchung infizierte Dateien gefunden werden und als Aktion für infizierte Objekte das Löschen der Dateien aus dem Dateisystem festgelegt wurden, besteht das Risiko des Verlusts wichtiger Daten. Um dies zu vermeiden, bietet Kaspersky Anti-Virus die Möglichkeit, Dateien in den Backup-Speicher zu kopieren.

Vor der Desinfektion oder dem Löschen eines Objekts wird im Backup-Speicher (Abschnitt **[path]**, Parameter **BackupPath**) automatisch eine Kopie angelegt. Die Sicherheitskopie bleibt auch dann erhalten (und bei Bedarf kann die ursprüngliche Datei wiederhergestellt werden), wenn das Objekt bei der Desinfektion beschädigt werden sollte. Das Objekt wird mit vollständigem Pfad im Backup gespeichert. Bei wiederholten Speichern im Backup-Speicher wird die ältere Kopie eines Objekts automatisch durch die neuere ersetzt.

Bitte beachten Sie: Der Modus zum Anlegen von Sicherheitskopien im Backup-Speicher ist nicht standardmäßig aktiviert und der Ordner, in dem die Sicherheitskopien gespeichert werden sollen, ist nicht festgelegt.

Um diese Option zu nutzen, muss dieser Pfad angegeben werden.



Wenn ein Objekt aus dem Dateisystem gelöscht wird, bleibt die Kopie im Backup solange erhalten, bis sie vom Administrator gelöscht wird.

Alle Handlungen, die in den Einstellungen der Konfigurationsdatei für infizierte Objekte festgelegt sind, werden nicht an den Dateien vorgenommen, die im Backup-Speicher liegen!

5.5. Lokalisierung der Datums- und Uhrzeitanzeige

Während der Arbeit von Kaspersky Anti-Virus wird für jede Komponente ein Protokoll erstellt. Außerdem werden unterschiedliche Benachrichtigungen für Benutzer und Administratoren generiert. Solche Informationen enthalten immer eine Datums- und Uhrzeitanzeige.

Standardmäßig verwendet Kaspersky Anti-Virus für Datum und Uhrzeit die Formate, die dem Standard `strftime` entsprechen:

%H:%M:%S – Format zur Anzeige der Uhrzeit

%d/%m/%y – Format zur Anzeige des Datums

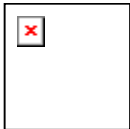
Der Administrator kann das Format für Datum und Uhrzeit ändern. Die Lokalisierung der Formate wird im Abschnitt **[locale]** der Konfigurationsdatei vorgenommen. Sie können beispielsweise folgende Formate festlegen:

%I:%M:%S %P – zur Anzeige der Uhrzeit im Zwölfstunden-Format (Parameter **TimeFormat**) mit Angabe von am/pm.

%y/%m/%d bzw. **%m/%d/%y** – zur Anzeige des Datums (Parameter **Date-Format**) im Format Jahr/Monat/Tag bzw. Monat/Tag/Jahr.

5.6. Parameter für die Erstellung von Protokollen für Kaspersky Anti-Virus

Die Ergebnisse aller Komponenten von Kaspersky Anti-Virus werden in einem Protokoll aufgezeichnet. Das Protokoll wird in einer Datei gespeichert.



Die Ergebnisse der Antivirenbearbeitung des Dateisystems werden auch auf der Konsole angezeigt. In der Grundeinstellung sind die Informationen, die im Protokoll aufgezeichnet und auf dem Bildschirm angezeigt werden, identisch.

Wenn Sie möchten, dass die Informationen in dem System-Log aufgezeichnet werden, vergeben Sie dem Parameter **ReportFileName** der Abschnitte **[monitor.report]**, **[scanner.report]**, **[updater.report]** den Wert **syslog**.

Der Umfang der angezeigten Informationen kann durch das Ändern der *Protokollgenauigkeit* reguliert werden.

Die **Protokollgenauigkeit** wird durch eine Ziffer angegeben, welche die Genauigkeit der Informationen über die Arbeit der Komponenten im Protokoll festlegt. Jede übergeordnete Stufe umfasst die Informationen der vorhergehenden sowie bestimmter Zusatzinformationen.

In der folgenden Tabelle werden alle vorhandenen Stufen der Protokollgenauigkeit aufgezählt.

Stufe	Bezeichnung der Stufe	Bedeutung
	Kritische Fehler	Nur Informationen über kritische Fehler (Fehler, die zum Beenden der Arbeit der Anwendung führen, weil bestimmte Aktionen nicht ausgeführt werden können). Beispiel: Eine Komponente ist infiziert oder bei der Untersuchung bzw. beim Laden von Datenbanken und Lizenzschlüsseln trat ein Fehler auf. In der Protokoll-Datei werden alle kritischen Fehler mit dem Buchstaben F gekennzeichnet.
1	Errors	Informationen über sonstige Fehler, einschließlich Fehlern, die nicht zum Beenden der Arbeit von Komponenten führten; z.B.: Informationen über einen Fehler bei der Untersuchung einer Datei. In der Protokoll-Datei werden alle nicht kritische Fehler mit dem Buchstaben E gekennzeichnet.
2	Warning	Informationen über Fehler, die zum Beenden der Arbeit des Produkts führen können (z.B. Informationen über unzureichenden Platz auf einem Laufwerk oder das Ablaufen des Lizenzschlüssels). In der Protokoll-Datei werden solche Fehler mit dem Buchstaben W gekennzeichnet.
3	Info, Notice	Wichtige Meldungen mit informativem Charakter; z.B.: Informationen darüber, ob eine Komponente gestartet wurde, Pfad der Konfigurationsdatei, Untersuchungsbereich, Informationen über die Antiviren-Datenbanken und über Lizenzschlüssel, Ergebnisstatistik. In der Protokoll-Datei werden Informationsmeldungen mit dem Buchstaben I gekennzeichnet.

Stufe	Bezeichnung der Stufe	Bedeutung
4	Activity	Meldungen über die aktuellen Aktivitäten der Anwendung (z.B., Name der untersuchenden Datei). In der Protokoll-Datei werden Informationsmeldungen mit dem Buchstaben A gekennzeichnet.
9	Debug	Meldungen, welche Debug-Informationen enthalten. In der Protokoll-Datei werden Informationsmeldungen mit dem Buchstaben D gekennzeichnet.

Informationen über kritische Fehler bei der Arbeit einer Komponente werden unabhängig von der gewählten Genauigkeitsstufe angezeigt. Die optimale Stufe für die Arbeit der Komponente ist Stufe **4**, das auch als Standard gilt.



Wenn die Tasks Untersuchung nach Befehl und Update der Antivirus-Datendanken mit Hilfe von Kaspersky Administration Kit gestartet werden, werden die Protokolldateien Standardmäßig nicht erstellt.

Um die Aufzeichnung der Protokolle einzuschalten, müssen Sie einen Verzeichnis und die Detaillierungsebene mit Hilfe der Parameter **ReportLevel** und **ReportsDir** im Abschnitt **[middleware.options]** der Konfigurationsdatei angeben.

KAPITEL 6. ANWENDUNG MIT HILFE VON KASPERSKY ADMINISTRATION KIT VERWALTEN

Kaspersky Administration Kit ist ein Verwaltungssystem für zentralisierte Administration der Computersicherheit in Ihrem Unternehmen, wenn die Sicherheit auf Basis von Produkten aufgebaut ist, welche zu Produktgruppe Kaspersky Anti-Virus Business Optimal gehören.

Kaspersky Antivirus 5.7 ist eins der Produkte von «Kaspersky Lab», welcher aus der Befehlszeile verwaltet werden kann (dies ist in dieser Dokumentation höher beschrieben), oder mit Hilfe von der Anwendung Kaspersky Administration Kit (wenn der Computer in das System der zentralen Fernverwaltung).

Die Installation der Anwendung wird in zwei Etappen durchgeführt:

- Installieren Sie ein *Administrationsserver* im Netzwerk; installieren Sie *Administrationskonsole* auf dem Arbeitsplatz des Administrator (Details sehe Einführungshandbuch von «Kaspersky Administration Kit»);
- Installieren Sie auf den Netzwerkcomputern Kaspersky Antivirus 5.7 und *Administrationsagenten*.

Zugang zur Verwaltung der Anwendung mit Hilfe von Kaspersky Administration Kit gewährleistet die *Administrationskonsole* (s. Abb. 1). Die Administrationskonsole ist ein Standardinterface, welcher in die MMC (Microsoft Management Konsole) integriert ist, und dem Administrator folgende Funktionen zur Verfügung stellt:

- Kaspersky Antivirus auf den Netzwerkcomputern Fern verwalten;
- Antivirusdatenbanken von Kaspersky Antivirus updaten;
- Informationen über Arbeit der Anwendung auf den Client-Computern ansehen.

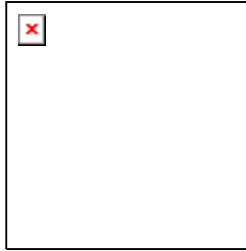


Abb. 1. Administrationskonsole von Kaspersky Administration Kit

Bei zentralisierter Verwaltung mit Hilfe von Kaspersky Administration Kit kann der Administrator die Richtlinienparameter, Taskparameter und Anwendungsparameter einstellen. Schutz des Netzwerkes wird auf Basis von diesen Parametern aufgebaut.

Anwendungsparameter – ein Satz von allgemeinen Parametern der Anwendung, welcher Schutz-, Schutzbereich- und andere Parameter enthält.

Task – eine Aktion, welche von der Anwendung ausgeführt wird. Entsprechend den Funktionen werden die Tasks von Kaspersky Antivirus nach Typen aufgeteilt:

- Task Scan auf Befehl;
- Updatetask für Antiviren-Datenbanken.

Jedem bestimmten Task entspricht ein Parametersatz des Kaspersky Antivirus – *Task Einstellungen*.

Eine Besonderheit der zentralen Verwaltung ist die Möglichkeit Computer in eine Gruppe zu organisieren und die Verwaltung der Gruppen mit Hilfe von Gruppenrichtlinien.

Richtlinie – ein Parametersatz für die Anwendung, welcher auf eine Computergruppe im logischen Netzwerk angewendet werden.

Richtlinie erlaubt Ihnen komplette Funktionalitäten der Anwendung zu verwalten, weil die Richtlinie Anwendungseinstellungen und Einstellungen für alle Tasktypen, außer Parameter, welche direkt beim Starten des Task definiert werden müssen (z.B., Zeitplan zum Starten des Tasks).

Zum Bestand der Richtlinie können auch Begrenzungen auf Änderungen vorgegebenen Parameter beim Einstellen der Anwendung oder Tasks.

6.1. Anwendung verwalten

Kaspersky Administration Kit gibt Ihnen eine Möglichkeit das Starten und Anhalten von Kaspersky Antivirus auf einem Client-Computer, wie auch Einstellung allgemeiner Parameter der Anwendung einstellen, z.B., Antivirusschutz des Computers Ein/Ausschalten, wie auch Einstellung der Protokoll-Parameter.



Um die Anwendungsparameter zu verwalten:

1. Im Ordner **Gruppen** (s. Abb. 1) wählen Sie den Ordner mit dem Gruppennamen, zur welcher der Client-Computer gehört.
2. Im Ergebnisfenster wählen Sie den Computer, für den Sie die Parameter ändern wollen. Im Kontextmenü oder im Menü **Aktionen** wählen Sie Befehl **Eigenschaften**.
3. Im Eigenschaften-Fenster des Client-Computers, auf der Registerkarte **Anwendungen** (s. Abb. 2) ist eine volle Liste der Anwendungen von «Kaspersky Lab» dargestellt, welche auf dem Client-Computer installiert sind. Wählen Sie die Anwendung **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server**.

Unter der Liste sind folgende Schaltflächen zu finden:

- **Ereignisse** – Liste der Ereignisse in der Arbeit der Anwendung, welche auf der Arbeitsstation statt fanden und auf dem Administrationsserver registriert wurden.
- **Statistik** – Statistik über die Arbeit der Anwendung ansehen.
- **Eigenschaften** – Einstellungen an der Anwendung vornehmen im Fenster **Anwendungsparameter «Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server»**.

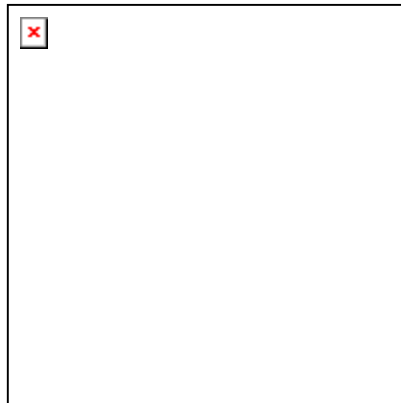


Abbildung 2. Liste der Anwendungen «Kaspersky Lab» »

6.1.1. Anwendungsparameter einstellen



Um die Arbeitsparameter der Anwendung zu sehen oder zu ändern:

1. Öffnen Sie das Fenster der Eigenschaften von Client-Computer auf der Registerkarte **Anwendungen** (s. Abb. 1).
2. Wählen Sie die Anwendung **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server**. Klicken Sie auf die Schaltfläche **Eigenschaften**, um zu den Einstellungen der Anwendungsparameter zu gelangen.

Alle Registerkarten (außer Registerkarte **Parameter**) sind für Anwendungen von Kaspersky Administration Kit gleich. Eine detaillierte Beschreibung von standardmäßigen Registerkarten sehen Sie im Handbuch für Administratoren.

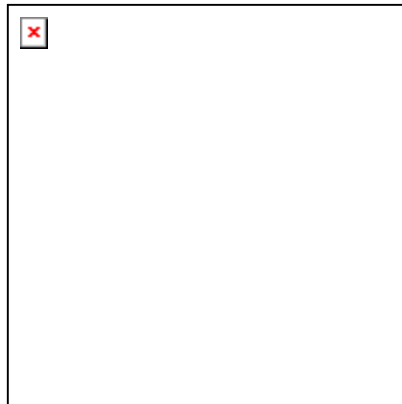


Abbildung 3. Parameter für Kaspersky Anti-Virus einstellen.
Registerkarte **Parameter**



Wenn eine Richtlinie für die Anwendung erstellt wurde (s. Pkt. 6.3.1 auf S. 62), welche die Vordefinierung einige Parameter verboten ist, werden diese Parameter beim Einstellen der Parameter nicht zugänglich sein.

Auf der Registerkarte **Parameter** können allgemeine Schutzparameter und Untersuchungsbereich-Parameter einstellen.

6.1.1.1. Registerkarte **Parameter**, Abschnitt **Echtzeitschutz: allgemeine Parameter**

Im Abschnitt **Allgemeine Parameter** können Sie:

- Echtzeitschutz des Computers Ein-/Ausschalten;
- Desinfizierung von infizierten Objekten Ein-/Ausschalten;
- Heuristische Analyse und Technologie iChecker Ein-/Ausschalten;
- Anwendungsparameter für Arbeitsproduktivität einstellen (Anzahl von gleichzeitig überprüfenden Dateien, Anzahl der Dateien im Casch von Kernel und UserSpace).

6.1.1.2. Registerkarte Parameter, Abschnitt Echtzeitschutz: Schutzbereich und geschützte Objekte

Auf der Registerkarte **Parameter** im Abschnitt **Schutzbereich und geschützte Objekte** können Sie:

- Vertraute Zone einstellen (eine Liste der Verzeichnisse, welche aus der Überprüfung ausgeschlossen werden);
- Ausschluss der Dateien aus der Überprüfung nach Maske einstellen (Masken werden im Form von standardmäßigen shell-Masken angegeben);
- Schutzbereich einstellen (Liste der Verzeichnisse, welche in die Überprüfung eingeschlossen sind);
- Typen von zu überprüfenden Objekten auswählen.

6.2. Tasks verwalten

In diesem Abschnitt finden Sie Information über das Erstellen von Tasks für Kaspersky Anti-Virus.

Als Teil der Verwaltung über Kaspersky Administration Kit können Sie folgende Tasks erstellen und benutzen:

- Task Scan auf Befehl;
- Updatetask für Antivirus-Datenbanken.

6.2.1. Task erstellen



Um die Liste der Tasks zu sehen, welche für einen Client-Computer erstellt wurde:

1. In dem Ordner **Gruppen** (s. Abb. 1) wählen Sie den Ordner mit dem Namen der Gruppe, zur welchen der Client-Computer gehört.
2. In dem Ergebnisfenster wählen Sie den Computer, an dem Sie die Liste der lokalen Tasks ansehen wollen. Benutzen Sie den Befehl **Tasks** aus dem Kontextmenü oder gleichen Punkt im Menü **Aktionen**. Darauf öffnet sich das Eigenschaftsfenster des Client-Computers.

Auf der Registerkarte **Tasks** (s. Abb. 4) ist eine volle Liste der Tasks zu sehen, welche für diesen Computer erstellt wurde.

Wenn Sie Kaspersky Administration Kit benutzen, können Sie erstellen:

- Lokale Tasks – werden für einzelne Computer definiert;
- Gruppentask – werden für Computer definiert, welche in eine logische Gruppe geschlossen wurden;
- Globale Tasks – werden für einen Satz der Computer aus unterschiedlichen Gruppen des logischen Netzwerkes definiert.

Sie können Änderungen an den Einstellungen des Tasks vornehmen, Taskausführung beobachten, Tasks kopieren und aus einer Gruppe in andere verschieben, wie auch Tasks löschen mit Hilfe der Befehle aus dem Kontextmenü **Kopieren/Einfügen, Ausschneiden/Einfügen** und **Löschen** oder gleiche Punkte aus dem Menü **Aktion** benutzen.

Arbeitsparameter der Anwendung beim Ausführen der Tasks auf einzelnen Computern werden entsprechend den Gruppenrichtlinien, Taskeinstellungen und Einstellungen der Anwendung auf diesem Computer eingestellt.

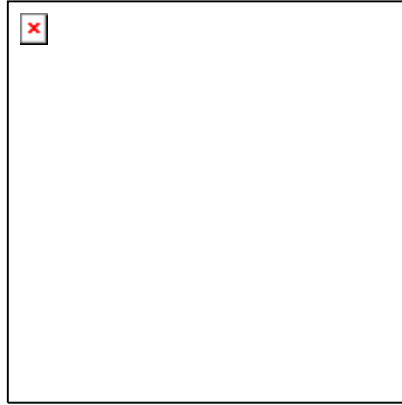


Abbildung 4. Taskliste der Anwendung

6.2.1.1. Lokale Tasks erstellen



Um einen lokalen Task zu erstellen:

1. Im Ordner **Gruppen** wählen Sie den Ordner mit dem Namen der Gruppe, zur welchen der Client-Computer gehört (s. Abb. 4).
2. In dem Ergebnisfenster wählen Sie den Computer, für welchen der lokale Task erstellt werden soll und benutzen Sie den Befehl **Eigenschaften** aus dem Kontextmenü oder den Punkt **Tasks** aus dem Menü **Aktion**. Darauf öffnet sich das Eigenschaftsfenster des Client-Computers **Eigenschaften: Computername**.
3. Auf der Registerkarte **Tasks** (s. Abb. 4) ist eine Liste der Tasks zu finden, welche für diesen Computer erstellt wurden. Einen neuen Task können Sie mit Hilfe der Schaltfläche **Hinzufügen** erstellen, Taskinstellungen können Sie mit Hilfe der Schaltfläche **Einstellungen** vornehmen. Mit Hilfe der Schaltfläche **Löschen** können Sie den Task aus der Liste löschen.

Wenn Sie auf die Schaltfläche **Hinzufügen** klicken, wird ein Assistent zum erstellen eines Task Microsoft Windows (Windows Wizard) gestartet, welcher aus eine Reihe von Schritten besteht, zwischen den Schritten bewegen Sie sich mit Hilfe von Schaltflächen **Zurück** und **Weiter**, beenden können Sie des Assistenten mit der Schaltfläche **Fertig**. Um die Arbeit des Assistenten abzubrechen dient die Schaltfläche **Abbrechen**.

Schritt 1. Allgemeine Daten über den Task eingeben

Im ersten Fenster des Assistenten müssen Sie den Namen des Tasks angeben (Feld **Name**).

Schritt 2. Tasktyp und Anwendung auswählen

In der Liste **Anwendungsname** wählen Sie die Anwendung **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Servers**. Tasktyp wird aus der Liste **Tasktyp** ausgewählt. Für Kaspersky Anti-Virus können folgende Tasks erstellt werden:

- Scan auf Befehl.
- Antivirus-Datenbanken updaten.

Schritt 3. Einstellen der Parameter für ausgewählten Tasktyp

Abhängig von dem Tasktyp, welcher im Schritt 3 ausgewählt wurde, variiert sich der Inhalt von den folgenden Fenstern.

EINSTELLEN DER PARAMETER FÜR DEN TASK SCAN AUF BEFEHL

Für den Parameter Scan auf Befehl müssen Sie angeben:

- Typen zu untersuchenden Objekte;
- Untersuchungsbereich (im entsprechenden Feld, als Liste, getrennt durch Doppelpunkt);
- Aktionen an infizierten Objekten angeben, welche im Falle des Fundes an den Objekten vorgenommen werden;
- Zusätzliche Arbeitsparameter angeben: Benutzung von heuristischen Analyse, Technologie iChecker, erweiterten Antivirus-Datenbanken, Start des Tasks als Komplettüberprüfung des Computers.

EINSTELLEN DER PARAMETER FÜR DEN TASK ANTIVIRUS-DATENBANKEN UPDATEN

Für den Task Antivirus-Datenbanken updaten müssen Sie angeben:

- Updatequelle. Als Updatequelle kann entweder ein Updateserver von «Kaspersky Lab» sein, oder eine von dem Benutzer angegebene Quelle;
- Benutzung des passiven Betriebs bei FTP-Verbindung;

- Time-out der Verbindung, in sek.

Ein- und Ausschalten der Benutzung des Proxy-Servers und die Parameter der Verbindung können Sie im Fenster einstellen, welches sich nach dem Sie auf den Hyperlink **Parameter des Proxy-Servers einstellen** klicken.

Schritt 4. Zeitplan einstellen

In dem Fenster **Zeitplan für das Starten des Task** können Sie den Zeitplan einstellen, nach dem dieser Task funktionieren wird.

In der aufklappenden Liste **Start nach Zeitplan** wählen Sie gewünschte Betriebsart zum Starten des Tasks. Abhängig von den gewählten Variante, wird das zentrale Teil des Fensters sein aussehen verändern.

Details über das Einstellen des automatischen Taskstarts sehen Sie Administratorhandbuch «Kaspersky Administration Kit».

Schritt 5. Taskerstellung beenden

In dem letzten Fenster wird Assistent Sie über erfolgreiches beenden der Taskerstellung informieren.

6.2.1.2. Gruppentask erstellen



Um Gruppentask zu erstellen, führen Sie folgende Aktionen aus:

1. Wählen Sie in der Konsole die Gruppe, für welche Sie den Task erstellen werden.
2. Wählen Sie darin enthaltenen Ordner **Tasks**, rufen Sie das Kontextmenü auf und wählen Sie den Befehl **Erstellen → Task**, oder benutzen Sie den gleichen Punkt aus dem Menü **Aktion**. Darauf wird ein Assistent gestartet, welcher gleich dem Assistenten der Erstellung eines lokalen Task ist (Details s. Pkt. 6.2.1.1 auf S. 56). Folgen Sie den Anweisungen des Assistenten.

Nach dem die Arbeit des Assistenten beendet wird, wird der Task zum Ordner **Tasks** der entsprechenden Gruppe wie auch aller eingelegten Gruppen hinzugefügt, außerdem wird der Task in dem Ergebnisfenster angezeigt.

6.2.1.3. Globalen Task erstellen



Um einen globalen Task zu erstellen, führen Sie folgende Aktionen aus:

1. Wählen Sie in der Konsole den Knoten **Globale Tasks**, rufen Sie das Kontextmenü auf und wählen Sie den Befehl **Erstellen → Task**, oder benutzen Sie den gleichen Punkt aus dem Menü **Aktion**.
2. Darauf wird ein Assistent gestartet, welcher gleich dem Assistenten der Erstellung eines lokalen Task (Details s. Pkt. 6.2.1.1 auf S. 56). Eine Abweichung von der Erstellung eines lokalen Task ist eine Etappe, bei der eine Liste der Client-Computer aus dem logischen Netzwerk erstellt wird, für welche der globale Task erstellt wird.
3. Wählen Sie Computer aus dem logischen Netzwerk, auf welchen der Task gestartet werden soll. Es können Computer aus unterschiedlichen Ordnern gewählt werden, es kann auch ein kompletter Ordner ausgewählt werden (Details s. Administratorhandbuch «Kaspersky Administration Kit»).



Globale Tasks werden nur für einen definierten Satz der Computer ausgeführt. Wenn zu einer Gruppe, für welche ein Task der Installation erstellt wurde, neu Computer hinzugefügt werden, wird der Task für diese Computer nicht ausgeführt. Es muss ein neuer Task erstellt werden oder Änderungen an dem existierenden Task vorgenommen werden.

Nach dem die Arbeit des Assistenten beendet wird, wird der Task zum Bestand des Knotens **Globale Tasks** der Konsole hinzugefügt, außerdem wird der Task in dem Ergebnisfenster angezeigt.

6.2.2. Spezifische Taskparameter einstellen



Um Taskparameter des Client-Computers anzusehen und zu ändern:

1. Öffnen Sie das Eigenschaftenfenster des Client-Computers auf der Registerkarte **Tasks** (s. Abb. 4).
2. Wählen Sie den Task aus der Liste und klicken Sie auf die Schaltfläche **Eigenschaften**. Darauf öffnet sich das Fenster mit Einstellungen der Taskparameter (s. Abb. 6).

Folgende Registerkarten sind für alle Tasks gleich:

- **Allgemein** – allgemeine Informationen über Task ansehen, Starten und Beenden des Tasks.
- **Zeitplan** – Zeitplan zur Ausführung des Tasks erstellen.

- **Benachrichtigung** – Benachrichtigungen über Ergebnisse der Taskausführung einstellen (Details s. Administratorhandbuch «Kaspersky Administration Kit»).

Registerkarte **Parameter** enthält spezifische Parameter für Kaspersky Anti-Virus; Inhalt dieser Registerkarte ändert sich abhängig von dem Tasktyp.

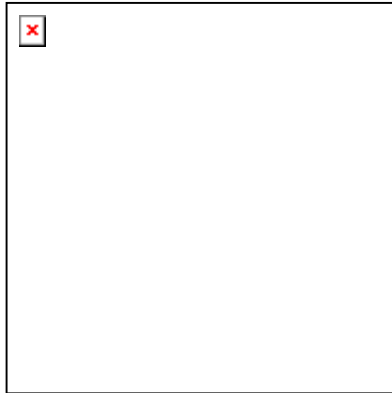


Abbildung 5. Einstellung der Taskparameter

6.2.2.1. Task Scan auf Befehl

Für den Task Scan auf Befehl außer Parameter, welche beim erstellen des Tasks angegeben wurden, können folgende Parameter hinzugefügt werden:

- Typ der untersuchenden Objekte angeben;
- Vertraute Zone angeben – Objekte und Maske der Dateinamen angeben, welche aus der Überprüfung ausgeschlossen werden (Masken werden in Form von Standardmäßigen shell-Masken angegeben),
- Betriebsart für Überprüfung der Dateisysteme des Computers angeben;
- Betriebsart für rekursive Überprüfung der Verzeichnisse angeben;
- Angeben, ob symbolische Links auf Verzeichnisse geöffnet werden sollen;
- Betriebsart der Kompletüberprüfung angeben.

6.2.2.2. Update-Task

Für Update-Task der Antivirus-Datenbanken sind folgende Einstellungen möglich:

- Updatequelle. Als Updatequelle kann entweder ein Updateserver von «Kaspersky Lab» benutzt werden, oder eine vom Benutzer definierte Quelle;
- Regionale Einstellungen. Bei der Auswahl der Region, in der sich der Computer befindet, werden die Updates in erster Reihe von den Servern bezogen, welche sich in der Region befinden;
- Passive Betriebsart für FTP benutzen;
- Timeout der Verbindung, in sek.

Proxy-Server Benutzung ein- und ausschalten, wie auch die Parameter der Verbindung einstellen, können Sie in dem Fenster, welches sich nach dem Klick auf den Hyperlink **Parameter des Proxy-Servers einstellen** öffnen.

6.2.3. Tasks Starten und Anhalten

Das Starten und Anhalten von Tasks erfolgt automatisch, entsprechend dem Zeitplan, wie auch per Hand mit Hilfe von Befehlen aus dem Kontextmenü und aus dem Fenster der Taskeinstellungen.



Um einen Task per Hand zu starten oder anzuhalten:

Wählen Sie den gewünschten Task in dem Ergebnisfenster aus, öffnen Sie das Kontextmenü und benutzen Sie Befehl **Starten / Anhalten** oder den Gleichen Punkt im Menü **Aktion**.

Gleiche Aktionen (für alle Tasktypen) können Sie aus dem Ergebnisfenster auf der Registerkarte **Allgemein** (s. Abb. 5) mit Hilfe der Schaltfläche **Starten / Anhalten** initiieren.



Das Starten der Tasks auf dem Client-Computer wird nur in dem Fall ausgeführt, wenn die Anwendung gestartet wird. Beim Anhalten der Anwendung wird das Ausführen aller gestarteten Tasks angehalten.

6.3. Richtlinien Verwalten

Das Bestimmen von Richtlinien erlaubt Ihnen einheitliche Parameter für Anwendungen und Tasks auf Client-Computer zu verbreiten, welche zum Inhalt einer logischen Gruppe gehören.

In diesem Abschnitt finden Sie Informationen über das Erstellen und Einstellen von Richtlinien für Kaspersky Anti-Virus.

6.3.1. Richtlinie erstellen




Um eine Richtlinie für Kaspersky Anti-Virus zu erstellen, führen Sie folgende Aktionen aus:

1. Im Ordner **Gruppen** (s. Abb. 1) wählen Sie die Computergruppe, für welche die Richtlinie erstellt werden soll.
2. Wählen Sie in der Gruppe enthaltenen Ordner **Richtlinien**, öffnen Sie das Kontextmenü und benutzen Sie das Befehl **Erstellen** → **Richtlinie**. Darauf folgt das Fenster der Erstellung einer neuen Richtlinie.

Das Erstellen der Richtlinie ist als Assistent für Microsoft Windows (Windows Wizard) ausgeführt und besteht aus einer Reihe von Fenstern (Stritte), zwischen den Schritten bewegen Sie sich mit Hilfe von Schaltflächen **Zurück** und **Weiter**, beenden können Sie des Assistenten mit der Schaltfläche **Fertig**. Um die Arbeit des Assistenten abzubrechen dient die Schaltfläche **Abbrechen**.



In jedem Schritt der Erstellung von Richtlinie (Schritt 3 - Schritt 5), können die angegebenen Parameter mit Hilfe von Schaltfläche  fixiert werden. Wenn das Schoss zu ist, werden auf den Client-Computern die Werte benutzt, welche von der erstellenden Richtlinie definiert werden.

Allgemeine Richtlinien-Daten angeben

Erster Schritt des Assistenten ist die Einführung. In dem ersten Fenster müssen Sie den Richtliniennamen angeben (Feld **Name**), in dem zweiten müssen Sie die Anwendung **Kaspersky Anti-Virus 5.7 for Linux Workstation and File Server** aus der aufklappenden Liste **Anwendungsname** auswählen.

Richtlinienstatus wählen

In diesem Fenster müssen Sie Richtlinienstatus wählen, stellen Sie dazu den Schalter in die gewünschte Position: aktive Richtlinie, inaktive Richtlinie oder Richtlinie für mobile Benutzer (wird nach der Trennung des Computers von Netzwerk getrennt).



Es können mehrere Richtlinien für eine Anwendung erstellt werden, es kann aber nur eine davon aktiv sein.

Richtlinienparameter einstellen

Anwendungseinstellungen sind in zwei Kategorien aufgeteilt:

- Allgemeine Parameter;

- Schutzbereich und Objekte.

Zur Kategorie **Allgemeine Parameter** gehören folgende Einstellungen:

- Betriebsart des ständigen Schutzes;
- Auswahl der Aktion für gefundene infizierte Objekte (Sie können das Desinfizieren der Objekte einschalten / ausschalten);
- Das benutzen des heuristischen Analysator und Technologie iChecker.

Zur Kategorie **Schutzbereich und Objekte** gehören folgende Einstellungen:


- Vertraute Zone (Liste der Verzeichnisse, welche aus der Überprüfung ausgeschlossen sind);
- Dateien nach einer Maske ausschließen (Masken werden als standardmäßige shell-Maske angegeben);
- Typ der geschützten Objekte auswählen.

Listen der Verzeichnisse und Masken werden durch Doppelpunkt geteilt.

Erstellen der Richtlinie beenden

Letztes Fenster des Assistenten informiert Sie über erfolgreiches Beenden der Richtlinien-Erstellung.

Nach dem Beenden des Assistenten wird die Richtlinie für Kaspersky Anti-Virus in den Ordner **Richtlinien** der entsprechenden Gruppe hinzugefügt und in dem Ergebnisfenster angezeigt.

Sie können die Einstellungen einer erstellten Richtlinie ändern und das Ändern der Parameter begrenzen mit Hilfe der Schaltfläche  für jede Gruppe der Einstellungen. Benutzer des Client-Computers kann die Einstellungen nicht ändern, wenn sie auf diese Art fixiert wurden. Das Verbreiten der Richtlinie auf die Client-Computer wird bei erster Synchronisation des Client-Computers mit dem Server. Sie können die Richtlinien kopieren, aus einer Gruppe in die Andere verschieben und löschen mit Hilfe von den standardmäßigen Befehlen des Kontextmenüs **Kopieren / Einfügen, Ausschneiden / Einfügen** und **Löschen** oder benutzen Sie gleiche Befehle aus dem Menü **Aktion**.

6.3.2. Richtlinienparameter ansehen und ändern

Sie können an der Richtlinie Änderungen vornehmen, das Ändern der Parameter der Richtlinien in den eingebeteten Gruppen, in den Anwendung-Parametern und in den Taskeinstellungen verbieten.

1. wählen Sie die Computergruppe in der Konsole im Ordner **Gruppen**, für welche die Einstellungen geändert werden sollen.
2. Wählen Sie den Ordner **Richtlinien**, welche zum Inhalt dieser Gruppe gehört; dabei werden in der Ergebnispanelle alle Richtlinien angezeigt, welche für diese Gruppe erstellt wurden.
3. Wählen Sie aus der Liste die gewünschte Richtlinie für **Kaspersky Anti-Virus 5.7 for Linux Workstation** (Name der Anwendung wird in dem Feld **Anwendung** angezeigt).
4. Wählen Sie aus dem Kontextmenü der gewählten Richtlinie Befehl **Eigenschaften**. Darauf öffnet sich das Fenster zum Einstellen der Anwendungsrichtlinie, welches mehrere Registerkarten enthält.

Registerkarten **Allgemein**, **Anwenden** und **Ereignisse** sind standardmäßige Registerkarten für Kaspersky Administration Kit (Details s. gleichnamiges Administratorhandbuch).

Registerkarte **Parameter** (s. Abb. 6) enthält Abschnitte mit den Einstellungen für Kaspersky Anti-Virus. Eine Beschreibung der Abschnitte ist im Dokument unten angeführt.

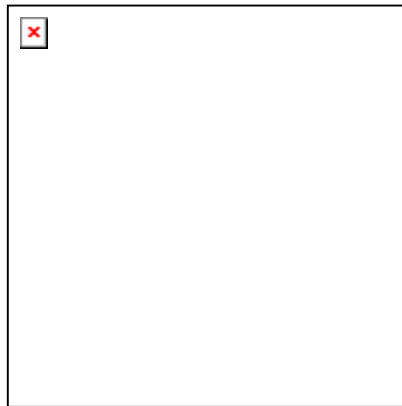



Abbildung 6. Richtlinienparameter einstellen



Beim Ändern der Richtlinienparameter Benutzen Sie die Schaltfläche  um die Daten über die Richtlinie fest zu legen. Später kann der Benutzer auf dem Client-Computer die Einstellungen der Richtlinie nicht ändern, wenn die Richtlinien so fest fixiert wurden.

6.3.2.1. Schutzbereich-Einstellungen

Auf der Registerkarte **Parameter** im Abschnitt **Echtzeitschutz: Schutzbereich und geschützte Objekte** können Sie:

- Vertraute Zone einstellen (Liste der Verzeichnisse, welche aus der Überprüfung ausgeschlossen sind);
- Ausschließen der Dateien aus der Überprüfung nach einer Maske (Masken werden in Form von standardmäßigen shell-Masken angegeben);
- Überprüfungsbereich angeben (Liste der Verzeichnisse, welche überprüft werden sollen).

Listen der Verzeichnisse und Masken werden durch Doppelpunkt geteilt.

6.3.2.2. Typ von den überprüfenden Dateien bestimmen

Auf der Registerkarte **Parameter** im Abschnitt **Echtzeitschutz: Schutzbereich und geschützte Objekte** schalten Sie den Schutz ein für:

- Gepackte Dateien;
- Archive;
- Selbstentpackende Archive;
- E-Mail-Datenbanken;
- Dateien in E-Mail-Format.

6.3.2.3. Aktionen an den Objekten einstellen

Auf der Registerkarte **Parameter** im Abschnitt **Echtzeitschutz: allgemeine Parameter** können Sie folgendes tun:

- Das Desinfizieren von infizierten Objekten Ein- / Ausschalten;
- Echtzeitschutz Ein- / Ausschalten;
- Heuristische Analyse Ein- / Ausschalten;
- Technologie iChecker Ein- / Ausschalten;
- Das Benutzen von erweiterten Antiviren-Datenbanken Ein- / Ausschalten.

6.3.2.4. Zusätzliche Parameter einstellen

Auf der Registerkarte **Parameter** im Abschnitt **Echtzeitschutz: allgemeine Parameter** können Sie folgendes tun:

- Anzahl von gleichzeitig zu überprüfenden Dateien angeben;
- Anzahl von Dateien angeben, welche im Cash von UserSpace gehalten werden;
- Anzahl von Dateien angeben, welche im Cash von Kernel gehalten werden.

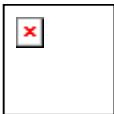
KAPITEL 7. DEINSTALLATION VON KASPERSKY ANTI- VIRUS

Für die Deinstallation von Kaspersky Anti-Virus sind erforderlich:

- Vorhandensein der Rechte eines privilegierten Benutzers (**root**). Wenn Sie im Moment der Deinstallation nicht über diese Rechte verfügen, ist die Anmeldung beim System als Benutzer **root** erforderlich.
- Vorhandensein der Protokolldatei über den Installationsprozess.
- Vollständige Übereinstimmung von Namen und Größen der installierten Dateien von Kaspersky Anti-Virus mit den Angaben in der Installations-Protokolldatei.
- Vor der Deinstallation muss die Komponente **kavmonitor** angehalten werden. . Geben Sie dazu in der Befehlszeile ein:

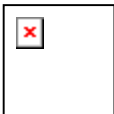
```
# /etc/init.d/kav4ws stop
```

- Danach müssen Sie die Anwendung und Administrationsagenten deinstallieren



Wenn Sie bei der Installation die rpm-Pakete für Kaspersky Anti-Virus und Administrationsagenten verwendet haben, geben Sie zum Start der Deinstallation in der Befehlszeile ein:

```
rpm -e <Paketname>
```




Wenn Sie bei der Installation das deb-Paket für Kaspersky Anti-Virus verwendet haben, geben Sie zum Start der Deinstallation in der Befehlszeile ein:

```
dpkg -r <Paketname>
```

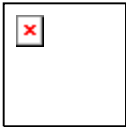
Die Deinstallationsprozedur wird automatisch ausgeführt. Nach dem Abschluss erscheint eine entsprechende Meldung auf der Konsole.

KAPITEL 8. TESTEN DER FUNKTIONALITÄT VON KASPERSKY ANTI-VIRUS

Wir empfehlen, nach der Installation und Konfiguration von Kaspersky Anti-Virus mittels eines "Test-Virus" und dessen Modifikationen zu überprüfen, ob die Anwendung richtig funktioniert.

Der "Test-Virus" wurde von der Organisation  (The European Institute for Computer Antivirus Research) speziell zum Testen von Antivirenprodukten entworfen.

Der "Test-Virus" IST KEIN VIRUS und enthält keinen Programmcode, der Ihrem Computer schaden könnte. Die meisten Antivirenprodukte der meisten Hersteller identifizieren diese Datei jedoch als Virus.



Verwenden Sie niemals einen echten Virus, um die Funktionsfähigkeit eines Antivirenprodukts zu testen!

Sie können den "Test-Virus" von der offiziellen Webseite der Organisation **EICAR** unter http://www.eicar.org/anti_virus_test_file.htm downloaden.

Die Datei, die Sie von der **EICAR**-Webseite heruntergeladen oder wie oben beschrieben hergestellt haben, enthält den Körper eines standardmäßigen "Test-Virus". Das Antivirenprogramm entdeckt diese Datei, markiert sie als **Infiziert** und irreparabel, und wendet die vom Administrator für diesen Objekttyp festgelegte Aktion darauf an.

Um die Reaktion des Antivirenprogramms auf den Fund anderer Objekttypen zu testen, verändern Sie den Inhalt des standardmäßigen "Test-Virus", indem Sie eines der Präfixe aus der unten folgenden Tabelle hinzufügen.

Tabelle. Modifikationen des "Test-Virus"

Präfix	Objekttyp
Kein Präfix, standardmäßiger "Test-Virus"	Infiziert. Objekt kann nicht desinfiziert werden.
CORR–	Unbekannt.
SUSP–	Verdächtig (unbekannter Viruscode).
WARN–	Verdächtig (veränderter Code eines bekannten Virus).
ERRO–	Nicht untersucht wegen Fehler.
CURE–	Desinfiziert. Objekt kann desinfiziert werden, wobei der Text des "Virus"-Körpers in CURE geändert wird.
DELE–	Objekt wird automatisch gelöscht.

In der ersten Spalte der Tabelle sind die Präfixe aufgeführt, die am Anfang der Zeichenkette des standardmäßigen "Test-Virus" angefügt werden können (zum Beispiel: CORR–X50!P%@AP[4\PZX54(P^)7CC)7}\$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!\$H+H*). Die zweite Spalte der Tabelle enthält die Typen von Objekten, die nach dem Hinzufügen der Präfixe von einem Antivirenprogramm identifiziert werden. Die Aktionen für jeden Objekttyp sind durch die vom Administrator angepassten Einstellungen des Antivirenprogramms festgelegt.

ANHANG A. ZUSÄTZLICHE ANWENDUNGSGEHEBENSINFORMATIONEN

Dieser Anhang beinhaltet eine Beschreibung der Ordnerstruktur der Distribution Kaspersky Anti-Virus nach dem Installieren, die Konfigurationsdatei, sowie Optionen der Komponenten in der Befehlszeile und dessen Rückgabewert, als Beispiel wurde ein Skript zur Desinfektion der Archive hinzugefügt.

A.1. Konfigurationsdatei des Kaspersky Anti-Virus

Zum Lieferumfang gehört eine Konfigurationsdatei **kav4fs.conf**, welche die Anwendungseinstellungen enthält. In diesem Abschnitt werden die Parameter näher erleutern. In den Beschreibungen der Parameter werden Standardwerte angegeben, wenn diese vorgesehen sind.

Abschnitt **[path]** enthält Parameter, die den Pfad zu den wichtigsten Dateien bestimmen, welche für die Funktionalität der Anwendung notwendig sind:

BasesPath – voller Pfad zu den Antiviren-Datenbanken.

LicensePath – voller Pfad zum Lizenzschlüssel-Ordner.

IcheckerDbFile – voller Pfad zur i-Checker Datenbank .

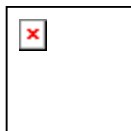
Abschnitt **[locale]** enthält Optionen, zur Datums- und Zeitformatierung:

TimeFormat=%H:%M:%S – Zeitformat nach strftime.



Sie können den Zeitformat auf Zwölfstündigen ändern (am, pm): **%I:%M:%S %P**

DateFormat=%d/%m/%y – Datum-Format nach strftime.



Sie können den Format des Datums ändern: **%y/%m/%d** или **%m/%d/%y**.

Abschnitt [network] enthält Einstellungen für die Verbindung des Dienstes kavmidware:



Den Wert des Parameters soll nicht geändert werden, wenn die Anwendung normal funktioniert.

MiddlewareAddress=/var/run/kav4ws/kavmidware.socket – Einstellungen der Verbindung von *kavmidware* mit dem Administrationsagenten und der Komponente *kavmonitor*.

Abschnitt [monitor.options] enthält Parameter der Untersuchung in Echtzeit:

ExcludeDirs= Maske1: Maske2:...: MaskeN – Maske der Ordner, welche von der Untersuchung ausgeschlossen werden; standardmäßig werden alle Ordner untersucht. Diese werden in Form der Standard shell-Masken eingegeben.

ExcludeMask=Maske1:Maske2:...:MaskeN – Maske der Dateien, welche von der Untersuchung ausgeschlossen werden; standardmäßig werden alle Dateien untersucht. Diese werden in Form der Standard shell-Masken eingegeben.

IncludeDirs=Maske1:Maske2:...:MaskeN – Maske der Ordner, die untersucht werden. Diese werden in Form der Standard shell-Masken eingegeben..

Packed=yes – Untersuchungsmodus für archivierte Dateien. Um diesen einzuschalten, setzen Sie den Wert auf **yes**.

Archives=no – Untersuchungsmodus für Archive. Um diesen einzuschalten, vergeben Sie dem Parameter den Wert **yes**.

SelfExtArchives=no – Untersuchungsmodus für selbstentpackende Archive. Um diesen einzuschalten, setzen Sie den Wert auf **no**. Wenn der Untersuchungsmodus für Archive eingeschaltet ist (**Archives=yes**), werden selbstentpackende Archive auch dann untersucht, wenn die Einstellung **SelfExtArchives** Wert **no** vergeben ist.

MailBases=no – Untersuchungsmodus der Post-Datenbanken. Um diesen einzuschalten, vergeben Sie dem Parameter den Wert **yes**.

MailPlain=no – Untersuchungsmodus für Emails in Form von plain text. Um diesen einzuschalten, vergeben Sie dem Parameter den Wert **yes**.

Heuristic=yes – Aktivierung für die heuristische Code-Analyse. Um diesen auszuschalten, vergeben Sie dem Parameter den Wert **no**.

Cure=no – Desinfektionsmodus für infizierten Objekte. Um diesen einzuschalten vergeben Sie dem Parameter den Wert **yes**.

Ichecker=yes – Benutzung der iChecker-Technologie bei der Untersuchung. Um diesen auszuschalten, vergeben Sie dem Parameter den Wert **no**.

FileCacheSize – Größe des Cache (in MB).

KernelCacheSize – Größe des Cache, für Einträge im Kernel-Speicher (in Einträgen).

CheckFileLimit=20 – Maximale Anzahl der gleichzeitig zu untersuchenden Objekte.

HashType=md5|crc32 – benutzter Hash-Typ. Standardmäßig wird **md5** benutzt.

UseAVbasesSet=standard|extended – Art der Anti-Viren Datenbanken, die von der Anwendung benutzt werden. Die **extended-Datenbank** beinhaltet außer den Einträgen aus der **standard**, zusätzliche Signaturen potenziell gefährlicher Programme, wie z.B.: Werbeprogramme, Fernverwaltungsprogramme u.s.w.

Abschnitt **[monitor.path]** enthält Parameter, die den Pfad zu den wichtigsten Dateien definieren, welche für die Funktion des Moduls kavmonitor notwendig sind:

BackupPath= Pfad – voller Pfad zu dem Ordner, in dem die Kopien der untersuchten Dateien gespeichert werden.

PidFile=Pfad – voller Pfad zur pid-Datei der Komponente kavmonitor.

Abschnitt **[monitor.actions]** enthält Parameter, die die Behandlung der unterschiedlichen Objekte beim Echtzeitschutz vorgeben:

OnInfected=Aktion – Aktionen im Fall des Fundes einer infizierten Datei. Wenn der Desinfektionsmodus eingeschaltet ist, wird diese Aktion auf Objekte angewendet, die nicht desinfiziert werden konnten.

OnSuspicion=Aktion – Aktionen im Fall des Fundes einer verdächtige Datei, deren Code einem Virus ähnelt, «Kaspersky Lab» aber noch nicht bekannt ist.

OnWarning=Aktion – Aktionen im Fall des Fundes einer Datei, deren Code einem Virus ähnelt, der «Kaspersky Lab» bekannt ist.

OnCured=Aktion – Aktionen im Fall nach erfolgreicher Desinfektion einer infizierten Datei.

OnProtected=Aktion – Aktionen im Fall eines Fundes eines passwortgeschütztes Objektes. Solche Objekte können nicht untersucht werden.

OnCorrupted=Aktion – Aktionen im Fall des Fundes einer beschädigten Datei.

OnError=Aktion – Aktionen im Fall, wenn bei der Untersuchung ein Systemfehler auftritt.

Schreibweise des Parameters **Aktion** besteht aus zwei Teilen: Aktion selbst und zusätzlichen Parameter, geteilt durch Leerzeichen. Wert des zusätzlichen Parameters wird in Einführungszeichen geschrieben. Zum Beispiel: `OnInfected=move "/tmp/infected"`

Die Aktion kann folgende Werte annehmen:

- *move* <Verzeichnis> – Datei in <Verzeichnis> verschieben.
- *movePath* <Verzeichnis> – Datei in den <Verzeichnis> rekursiv verschieben (mit dem vollen Pfad).
- *remove* – Datei löschen.
- *exec* <Parameter> – eine Aktion an der Datei vornehmen, welche im Wert <Parameter> bestimmt ist.

Als Makros des zusätzlichen Aktion-Parameters **exec** für Container werden benutzt:

- %VIRUSNAME% – Name des gefundenen gefährlichen Objektes oder Fehlername.
- %LIST% – Dateiname oder Liste der infizierten, verdächtigen oder fehlerhaften Dateien, welche im Container gefunden worden sind. Dateiformat sieht folgender Maassen aus: **<Virusname>\t<Dateiname>**.
- %FULLPATH% – kompletter Container-Pfad.
- %FILENAME% – Dateiname ohne Pfad.
- %CONTAINERTYPE% – Containertyp als eine Zeile.

Abschnitt **[monitor.report]** enthält Parameter für die Protokollfunktion der Komponente kavmonitor:

ReportLevel=4 – Stufe der Protokollgenauigkeit (s. Pkt. 5.6 auf S. 47).

ReportFileName – Name der Protokolldatei.

Append=yes – Gibt an, ob neue Meldungen der Protokolldatei hinzugefügt werden sollen. Um dies auszuschalten, vergeben Sie dem Parameter den Wert **no**.

ShowOK=yes – Eintragen von Informationen über nicht infizierte Dateien in die Protokolldatei. Um dies auszuschalten, vergeben Sie dem Parameter den Wert **no**.

Abschnitt **[scanner.options]** enthält Parameter für die Untersuchung Dateisysteme des Computers:

Archives=yes – Untersuchungsmodus für Archive. Um diesen auszuschalten, vergeben Sie dem Parameter den Wert **no**

Cure=no – Modus zum desinfizieren infizierter Objekte. Um dies zu aktivieren setzen Sie den Parameter auf den Wert **yes**.

ExcludeDirs=Maske1:Maske2:...:MaskeN – Maske der Ordner, welche von der Untersuchung ausgeschlossen werden; standardmäßig werden alle Ordner untersucht. Diese werden in Form der Standard shell-Masken eingegeben.

ExcludeMask=Maske1:Maske2:...:MaskeN – Maske der Dateien, welche von der Untersuchung ausgeschlossen werden; standardmäßig werden alle Dateien untersucht. Diese werden in Form der Standard shell-Masken eingegeben.

Heuristic=yes – Aktivierung für die heuristische Code-Analyse. Um diesen auszuschalten, vergeben Sie dem Parameter den Wert **no**.

LocalFS=no – Option, dass nur das lokale Dateisystem untersucht wird. Um dies einzuschalten, vergeben Sie dem Parameter den Wert **yes**.

MailBases=yes – Modus zur Untersuchung der Mail-Datenbanken. Um diesen auszuschalten, vergeben Sie dem Parameter den Wert **no**.

MailPlain=yes – Modus zur Untersuchung von Emails in Form von plain text. Um diesen auszuschalten, vergeben Sie dem Parameter den Wert **no**.

Packed=yes – Untersuchung archivierter Dateien. Um dies auszuschalten, setzen Sie den Wert auf **no**.

Recursion=yes – Rekursiv-Modus bei der Untersuchung von Ordnern. Um dies auszuschalten, setzen Sie den Wert auf **no**.

SelfExtArchives=yes – Untersuchung von selbstextrahierenden Archiven. Um dies auszuschalten, setzen Sie den Wert auf **no**. Wenn die Untersuchung von Archiven aktiviert ist (**Archives=yes**), werden selbstextrahierende Archive auch dann untersucht, wenn für diese Einstellung (**SelfExtArchives**) mit der Wert **no** vergeben ist.

Ichecker=yes – Benutzung der iChecker-Technologie bei der Untersuchung. Um diesen auszuschalten, vergeben Sie dem Parameter den Wert **no**.

UseAVbasesSet= standard |extended – Art der Anti-Viren Datenbanken, die von der Anwendung benutzt werden. Die **extended-Datenbank** beinhaltet außer den Einträgen aus der **standard**, zusätzliche Signaturen potenziell gefährlicher Programme, wie z.B.: Werbeprogramme, Fernverwaltungsprogramme u.s.w.

FollowSymlinks – Option zur Bearbeitung von symbolischen Links. Wenn diesem Parameter der Wert **yes** zugewiesen ist, werden bei der Untersuchung die Links geöffnet, die auf einen Ordner zeigen.

MaxLoadAvg – maximale Prozessorbelastung. Wenn der Wert überstiegen wird, wird die Komponente *kavscanner* angehalten.

Abschnitt **[scanner.report]** enthält Parameter für die Protokollfunktion der Komponente *kavscanner*:

Append=yes – Gibt an, ob neue Meldungen der Protokolldatei hinzugefügt werden sollen. Um dies auszuschalten, vergeben Sie dem Parameter den Wert **no**.

ReportFileName – Name der Protokolldatei.

ReportLevel=4 – Stufe der Protokollgenauigkeit (s. Pkt. 5.6 auf S. 47).

ShowOK=yes – Eintragen von Informationen über nicht infizierte Dateien in die Protokolldatei. Um dies auszuschalten, vergeben Sie dem Parameter den Wert **no**.

ShowContainerResultOnly=no – Eintragen von Informationen über die Untersuchung von Archiven in Kurzform. Zum aktivieren vergeben Sie dem Parameter den Wert **yes**.

ShowObjectResultOnly=no – Eintragen von Informationen über die Untersuchung von Objekten in Kurzform. Zum aktivieren vergeben Sie dem Parameter den Wert **yes**.

Abschnitt **[scanner.container]** enthält Parameter, die die Behandlung von Archiven beim Antivirenschutz der Computer-Dateisysteme definieren:

OnCorrupted=Aktion – Aktionen im Fall eines Fundes von beschädigten Containern.

OnInfected=Aktion – Aktionen im Fall des Fundes eines infizierten Objektes in einem Container. Wenn die Desinfektionsoption eingeschaltet ist, wird diese Aktion auf den Container angewendet, die nicht desinfiziert werden konnten, und wird nach dem Ausführen aller Aktionen mit Objekten des Containers.

OnSuspicion=Aktion Aktionen im Fall des Fundes eines verdächtigen Objektes in einem Container, dessen Code einem Virus ähnelt, welcher «Kaspersky Lab» noch nicht bekannt ist.

OnWarning=Aktion – Aktionen im Fall des Fundes eines verdächtigen Objektes in einem Container, dessen Code einem Virus ähnelt, der «Kaspersky Lab» bekannt ist.

OnCured=Aktion – Aktionen im Fall einer erfolgreichen Desinfektion eines infizierten Objektes in einem Container.

OnProtected=Aktion – Aktionen im Fall des Fundes eines Objekts in einem Container, der mit einem Passwort geschützt ist. Solche Objekte können nicht untersucht werden.

OnError=Aktion – Aktionen im Fall, wenn während der Untersuchung eines Containers ein Fehler auftritt.

Die Syntax der Aktionen an allen Objekttypen ist gleich der Syntax für Container im Abschnitt **[monitor.actions]**.

%CONTAINERTYPE% – Containertyp in Form einer Zeile. Der Abschnitt

[scanner.object] enthält Parameter, die die Behandlung der einfachen Objekte unterschiedlicher Typen beim Antivirenschutz der Arbeitsstation definieren:

OnCorrupted=Aktion – Aktionen im Fall eines Fundes einer beschädigten Datei.

OnInfected=Aktion – Aktionen im Fall eines Fundes einer infizierten Datei. Wenn die Desinfektionsoption eingeschaltet ist, wird diese Aktion auf Dateien angewendet, die nicht desinfiziert werden konnten.

OnSuspicion=Aktion – Aktionen im Fall des Fundes einer verdächtigen Datei, deren Code einem Virus ähnelt, der «Kaspersky Lab» noch nicht bekannt ist.

OnWarning=Aktion – Aktionen im Fall des Fundes einer verdächtigen Datei, deren Code einem Virus ähnelt, der «Kaspersky Lab» bekannt ist.

OnCured=Aktion – Aktionen im Fall einer erfolgreichen Desinfektion eines infizierten Objektes.

OnProtected=Aktion – Aktionen im Fall des Fundes eines Objekts, welches mit einem Passwort geschützt ist. Solche Objekte können nicht untersucht werden.

OnError=Aktion – Aktionen im Fall, wenn während der Untersuchung ein Fehler auftritt.

Die Syntax für Aktionen, welche auf Objekte anwendbar sind, ist der Syntax gleich, welche im Abschnitt **[monitor.actions]** für Container beschrieben ist.

Abschnitt **[scanner.display]** enthält Parameter der Protokollierung auf die Konsole:

ShowContainerResultOnly=no –Anzeigen von Untersuchungsergebnissen von Archiven in Kurzform. Zum aktivieren vergeben Sie dem Parameter den Wert **no**.

ShowObjectResultOnly=no – Anzeigen von Untersuchungsergebnissen von Objekten in Kurzform. Zum aktivieren vergeben Sie dem Parameter den Wert **yes**.

ShowOK=yes – Modus zum Anzeigen von Informationen über nicht infizierte Dateien. Um dies auszuschalten, vergeben Sie dem Parameter den Wert **no**.

ShowProgress=yes –Anzeigen der aktuellen Arbeit der Komponente (Updatedownload-Prozess der Antivirendatenbanken, Information über die Untersuchung der aktuellen Datei) in der Konsole. Um dies auszuschalten, vergeben Sie dem Parameter den Wert **no**.

Abschnitt **[scanner.path]** enthält Parameter, die den Pfad zu den Dateien definiert, ,

welche für die Funktion des Moduls kavscanner notwendig sind:

BackupPath= Pfad – voller Pfad zu dem Ordner, in dem die Kopien der untersuchten Dateien gespeichert werden.

Abschnitt **[updater.path]** enthält Parameter, die Pfade zu den Dateien definieren, welche für die Funktion des Moduls für das Update der Antivirendatenbanken nötig sind:

AVBasesTestPath – vollständiger Pfad zu dem Ordner, in dem die Antivirendatenbanken gespeichert werden.

BackUpPath – vollständiger Pfad zu dem Ordner, in dem die Reserve-Antivirendatenbanken liegen.

Abschnitt **[updater.report]** enthält Parameter für die Protokollfunktion der Komponente `keepup2date`:

Append=yes – Gibt an, ob neue Meldungen der Protokolldatei hinzugefügt werden sollen. Um dies auszuschalten, vergeben Sie dem Parameter den Wert **no**.

ReportFileName – Name der Protokolldatei.

ReportLevel=4 – Stufe der Protokollgenauigkeit(s. Pkt. 5.6 auf S. 47).

Abschnitt **[updater.options]** enthält Parameter für die Arbeit der Komponente `keepup2date`:

KeepSilent=no – Anzeigen von Information über Arbeit der Komponente `keepup2date` in der Konsole. Um dies auszuschalten, vergeben Sie dem Parameter den Wert **yes**.

ProxyAddress – Für die Verbindung zu benutzende Proxyserveradresse. Der Parameter wird in Form <http://username:password@url:port> angegeben. In der Adresse können **username** und/oder **password** fehlen. Wenn die Adresse nicht angegeben ist, wird ihr Wert aus der Umgebungsvariablen **http_proxy** übernommen.

UseProxy – Option zur Benutzung eines Proxy-Servers beim Verbinden mit dem Updateserver von «Kaspersky Lab». Wenn der Wert **no** ist, wird kein Proxy-Server benutzt. Wenn der Wert **yes** ist, wird der Proxy-Server benutzt, der im Parameter **ProxyAddress** definiert ist. Wenn der Wert des Parameters **ProxyAddress** nicht definiert ist, wird der Wert der Umgebungsvariablen **http_proxy** benutzt. Wenn diese Umgebungsvariable nicht definiert ist, wird kein Proxy-Server benutzt.

UseUpdateServerUrl=no Option zur Benutzung des Updateservers, welcher im Parameter **UpdateServerUrl** definiert ist.

UseUpdateServerUriOnly=no Option zur ausschliesslichen Benutzung des Updateservers, welcher in der Einstellung **UpdateServerUri** angegeben ist. Wenn dieser Option der Wert **no** vergeben wurde, wird im Fall eines nicht erfolgreichen Updateversuchs über die Adresse **UpdateServerUri**, die nächste Adresse aus der Serverliste benutzt.

UpdateServerUri=no **http://url/ | ftp://url/ | /local_path/** – Adresse zum Updaten der Antiviren-Datenbanken.

PostUpdateCmd – Befehl, welcher nach dem erfolgreichen Update der Antivirendatenbanken ausgeführt wird. Der Wert, der in der Konfigurationsdatei angegeben ist, wird automatisch nach dem herunterladen der neuen Antivirendatenbanken gestartet. Es wird nicht empfohlen diesen Parameter zu ändern.

RegionSettings=ru Region Code, wird zum Auswählen des optimalsten Updateservers von «Kaspersky Lab» benutzt.

ConnectTimeout=30 Timeout für das Update der Datenbanken (in Sekunden). Wenn in der angegebenen Zeit keine Daten vom Server kommen, wird ein neuer Server von «Kaspersky Lab» aus der Liste ausgewählt.

PassiveFtp=no passiver FTP-Modus.

Abschnitt **[middleware.options]** enthält Einstellungen des Dienstes *kavmidware*:



Die Werte der Parameter sollen nicht geändert werden, wenn die Anwendung normal funktioniert.

ScannerExe=/opt/kaspersky/kav4ws/bin/kav4ws-kavscanner – Pfad zur ausführenden Datei der Komponente *kavscanner*.

Keepup2dateExe=/opt/kaspersky/kav4ws/bin/kav4ws-keepup2date – Pfad zur ausführenden Datei der Komponente *keepup2date*.

LicenseManagerExe=/opt/kaspersky/kav4ws/bin/kav4ws-licensemanager – Pfad zur ausführenden Datei der Komponente *licensemanager*.

MonitorInitdScript=/etc/init.d/kav4ws – Pfad zum Verwaltungs-Skript des Dienstes *kavmonitor*.

DirToStoreFiles=/var/opt/kaspersky/kav4ws/middleware – Pfad zur Dateien des Dienstes *kavmidware*.

ReportLevel=0 – Detaillierungsstufe des Protokolls (s. Pkt. 5.6 auf S. 47).

ReportsDir=/var/log/kaspersky/kav4ws – Pfad zur Dateien des Komponenten-Protokoll.

A.2. Befehlszeilenoptionen der Komponente kavscanner

Die Parameter der Konfigurationsdatei können Sie beim Starten des Programms aus der Befehlszeile mit Hilfe der Optionen neu definieren.

Hilfeoptionen:

- h** Hilfe zur Komponente kavscanner in der Konsole anzeigen;
- v** Programmversion anzeigen.

Konfigurationsoptionen:

- c (-C) <Dateipfad>** Alternative Konfigurationsdatei benutzen **<Dateipfad>**;
- g<Dateipfad>** In die Datei **<Dateipfad>** eine Liste aller bekannten Viren schreiben, die in der Antivirendatenbanken enthalten sind.
- f** Die beschädigte Signatur der Komponente kavscanner ignorieren und versuchen, die Komponente zu desinfizieren.

Untersuchungsoptionen:

- e <Option>** Standardmäßige Untersuchungsoptionen ändern. Als **<Option>** können folgende Modi benutzt werden:
- P/p** Ein/ausschalten der Untersuchung der gepackten Dateien;
- A/a** Ein/ausschalten der Untersuchung von Archiven;
- S/s** Ein/ausschalten der Untersuchung der selbstentpackenden Archive;
- B/b** Ein/ausschalten der Untersuchung der Maildatenbanken;
- M/m** Ein/ausschalten der Untersuchung der E-Mails im plain text Format;

E/e	Ein/ausschalten der heuristischen Code-Analyse
-R/r	Ein/ausschalten der rekursiven Untersuchung;
-S/s	Ein/ausschalten der Option zum Öffnen von Symbolischen Links;
-l	Nur lokale Dateisysteme untersuchen.

Optionen der Protokollerstellung:

-q	Nichts in der Konsole ausgeben;
-o <Name>	Dateiname angeben, in die das Protokoll der Komponente geschrieben wird; wenn der Name nicht angegeben ist, wird kein Protokoll geschrieben. Außer Datei wird die Information über Arbeit der Komponente in der Console angezeigt. Um die Informationen in den Systemjournal zu schreiben, geben Sie <code>syslog</code> als Parameter <Name> ein.
-j<Zahl>	Stufe der Protokollgenauigkeit. Als <Option> können folgende Stufen benutzt werden:
1	anzeigen/nicht anzeigen von Fehlermeldungen;
2	anzeigen/nicht anzeigen von informativen Meldungen;
3	anzeigen/nicht anzeigen von Untersuchungsbenachrichtigungen.
-x<Option>	Protokollgenauigkeit für die Ausgabe der Untersuchung vorgeben, welche auf der Konsole angezeigt wird. Als <Option> können folgende Stufen benutzt werden:
O/o	Kurze/erweiterte Ausgabe von Meldungen über die Untersuchung einfacher Objekte;
C/c	Kurze/erweiterte Ausgabe von Meldungen über die Untersuchung von Archiven;
N/n	Ein/ausschalten der Anzeigen von Information über nicht infizierte Dateien;
P/p	Ein/ausschalten der Anzeigen von Information über die aktuelle

Arbeit der Komponente.

- m<Option>** Protokollgenauigkeit für die Untersuchung vorgeben (Benutzung einer Protokolldatei). Als **<Option>** können benutzt werden:
- O/o** Kurze/erweiterte Ausgabe von Meldungen über die Untersuchung einfacher Objekte;
- C/c** Kurze/erweiterte Ausgabe von Meldungen über die Untersuchung von Archiven;
- N/n** Ein/ausschalten der Protokollierung von Informationen über nicht infizierte Dateien.

Datei-Optionen:

- p<Option>
<Dateiname>** Liste der Objekte in eine Datei speichern; alle Objekte mit dem vollständigen Pfad in einer neuen Zeile speichern. Als **<Option>** können folgende eingetragen sein:
- i** In der Datei **<Dateiname>** die Liste der infizierten Objekte speichern;
- s** In der Datei **<Dateiname>** die Liste der verdächtigen Objekte speichern;
- c** In der Datei **<Dateiname>** die Liste der beschädigten Objekte speichern;
- w** In der Datei **<Dateiname>** die Liste der Objekte speichern, deren Code dem Code von bekannten Viren ähnelt.
- @ <filelist.lst>** Objekte untersuchen, welche in der Datei vorgegeben wird **<filelist.lst>**.

Optionen zur Bearbeitung von Dateien (Angabe der Dateien in der Befehlszeile setzt Vorgaben der Konfigurationsdatei außer Kraft):

- i0** Nur auf Viren untersuchen;
- i1** Objekte desinfizieren; falls desinfizieren nicht möglich ist - durchlassen
- i2** Objekte desinfizieren; falls desinfizieren nicht möglich ist und es ist ein einfaches Objekt – löschen; infiziertes Objekt aus einem Container nicht

- löschen;
- i3 Objekte desinfizieren; falls desinfizieren nicht möglich ist und es ist ein einfaches Objekt – löschen; falls infiziertes Objekt in einem Container ist – den ganzen Container löschen;
- i4 Alle infizierten Objekte und Container löschen.

A.3. Rückgabewerte der Komponente kavscanner

Während der Arbeit kann die Komponente kavscanner folgenden Rückgabewerte ausgeben:

- 0 Viren nicht gefunden;
- 5 Alle infizierten Objekte sind desinfiziert;
- 10 Es sind Archive gefunden worden, die mit einem Passwort geschützt sind;
- 15 Es wurden beschädigte Dateien gefunden;
- 20 Es wurden verdächtige Dateien gefunden;
- 21 Es wurden Dateien gefunden, deren Code einem bekannten Virus ähnelt;
- 25 Es wurden infizierte Dateien gefunden;
- 30 Bei der Untersuchung ist ein Systemfehler aufgetreten;
- 50 Antivirendatenbanken können nicht geladen werden (Pfad aus der Konfigurationsdatei konnte nicht gefunden werden);
- 55 Antivirendatenbanken sind beschädigt;
- 60 Datum der Antivirendatenbanken überschreitet das Zeitlimit des Lizenzschlüssels

- 64 Lizenzinformationen sind nicht vorhanden, kein Lizenzschlüssel im vorgegebenen Pfad aus der Konfigurationsdatei gefunden;
- 65 Konfigurationsdatei kann nicht geladen werden;
- 66 Falsche Einträge in der Konfigurationsdatei;
- 70 Komponente kavscanner ist beschädigt;
- 75 Komponente kavscanner ist beschädigt und kann nicht repariert werden.

A.4. Befehlszeilenoptionen der Komponente kavmonitor

Hilfeoptionen:

- h Hilfe über die Komponente auf der Konsole anzeigen;
- v Die Version der Anwendung anzeigen.

Konfigurationsoptionen:

- c<Dateipfad> Alternative Konfigurationsdatei benutzen <Dateipfad>.

A.5. Befehlszeilenoptionen der Komponente licensemanager

Hilfeoptionen:

- h Hilfe über die Komponente auf der Konsole anzeigen *licensemanager*.

Arbeitsoptionen für Lizenzschlüsseln:

- s Information über alle installierten Lizenzschlüssel in der Konsole anzeigen;

- c (-C) <Dateipfad>** Alternative Konfigurationsdatei benutzen
<Lizenzschlüsselpfad>;
- k <Dateipfad>** Information über Schlüssel in der Konsole anzeigen
<Lizenzschlüsselpfad>;
- a <Dateipfad>** Lizenzschlüssel installieren <Lizenzschlüsselpfad>;
- d(a|r)** Aktiven (Option **-da**) oder zusätzlichen Lizenzschlüssel
(Option **-dr**) entfernen.

A.6. Rückgabewerte der Komponente licensemanager

Während der Arbeit kann die Komponente licensemanager folgende Rückgabewerte ausgeben:

- 0** Komponente hat erfolgreich die Information über Lizenzschlüssel geladen und seine Arbeit beendet;
- 30** Ein Systemfehler trat bei der Arbeit der Komponente auf;
- 64** Lizenzinformation ist nicht vorhanden, kein Lizenzschlüssel im vorgegebenen Pfad aus der Konfigurationsdatei gefunden;
- 65** Konfigurationsdatei kann nicht geladen werden;
- 66** Falsche Einträge in der Konfigurationsdatei.
- 70** Die Komponente licensemanager ist fehlerhaft.

A.7. Befehlszeilenoption der Komponente keepup2date

Hilfeoptionen:

-v	Versionsinformation der Anwendung in der Konsole anzeigen und Arbeit beenden;
-h	Hilfe über Befehlszeilenoptionen in der Konsole anzeigen und die Arbeit beenden;
Arbeitsoptionen:	
-r	Rollback des Updates zu der vorigen Version;
-s	Liste der Updateserver in der Konsole anzeigen;
-k	Befehl PostUpdateCmd nicht ausführen nach dem erfolgreichen Update der Antivirendatenbanken;
-q	keine Meldungen in der Konsole anzeigen.
-e	nur Meldungen über kritische Fehler anzeigen.
-b <Pfad>	Beim Update eine Kopie der vorhandenen Antivirendatenbanken im Ordner <Pfad> erstellen.
-x Pfad_zum_Ordner <	Alle Updates der Antivirendatenbanken in den lokalen Ordner kopieren <Pfad_zum_Ordner> .
-t <Pfad>	Ordner <Pfad> zum Speichern der temporären Dateien benutzen.
-u Pfad_zum_Ordner <	Letzte Updates der Antivirendatenbanken in den Ordner kopieren < Pfad_zum_Ordner > ;
-c < Pfad_zur_Datei >	Alternative Konfigurationsdateien benutzen <Pfad_zur_Datei > .
-g <URL>	Adresse zum Updaten der Antivirendatenbanken. Beim vorgeben dieses Schlüssels wird das Update von der vorgegebenen Adresse geholt.
-d < Pfad_zur_Datei >	pid-Datei der Komponente benutzen, welche im lokalen Ordner < Pfad_zur_Datei > liegt.
Optionen der Protokollerstellung:	

<code>-l</code> <code><Pfad_zur_Datei></code>	Ergebnisse in die Datei <code><Pfad_zur_Datei ></code> speichern.
--	---

A.8. Rückgabewerte der Komponente `keepup2date`

Während der Arbeit kann die Komponente `keepup2date` folgende Rückgabewerte ausgeben:

0	Kein Update notwendig;
1	Update der Antivirendatenbanken erfolgreich abgeschlossen;
10	Kritischer Fehler ist aufgetreten, Update wird abgebrochen;
12	Beim Rollback zur letzten Version der Antivirendatenbanken ist ein Fehler aufgetreten;
30	Befehl <code>PostUpdateCmd</code> konnte nicht nach dem Update gestartet werden;
60	Lizenzinformation ist nicht vorhanden, kein Lizenzschlüssel im vorgegebenen Pfad aus der Konfigurationsdatei gefunden;
75	Konfigurationsdatei kann nicht geladen werden oder Fehler in dessen Parametern.

A.1. Schlüssel der Befehlszeile der Komponente `kavmiddleware`

Hilfe-Optionen:	
<code>-v</code>	Version in der Konsole anzeigen und Arbeit der Komponente beenden;
<code>-h</code>	Hilfeinformation über Schlüssel der Befehlszeile in der Konsole anzeigen und Arbeit der Komponente beenden;

ANHANG B. HÄUFIGE FRAGEN

In diesem Kapitel beantworten wir ausführlich die von Benutzern häufig gestellten Fragen über Installation, Konfiguration und Funktion von Kaspersky Anti-Virus.



Frage: Kann Kaspersky Anti-Virus gleichzeitig mit Antivirenprodukten anderer Hersteller verwendet werden?

Um Konflikte zu vermeiden, empfehlen wir, die Antivirenprodukte anderer Hersteller vor der Installation von Kaspersky Anti-Virus zu entfernen.



Frage: Kaspersky Anti-Virus untersucht eine Datei nicht wiederholt. Warum?

Tatsächlich untersucht Kaspersky Anti-Virus Dateien nicht erneut, die sich seit der letzten Untersuchung nicht verändert haben.

Möglich ist dies durch die Verwendung der neuen Technologie iChecker. Dabei werden Datenbanken mit Kontrollsummen von Objekten verwendet.



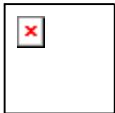
Frage: Warum ruft Kaspersky Anti-Virus eine gewisse Senkung der Leistungsfähigkeit des Computers hervor und führt zu bemerkbarer Prozessorbelastung?

Das Erkennen von Viren ist eine rechnerische (mathematische) Aufgabe, die mit Strukturanalyse, Berechnung von Kontrollsummen und mathematischer Datenumformung zusammenhängt. Deshalb ist die Hauptressource, die bei der Arbeit von Kaspersky Anti-Virus verbraucht wird, die Prozessorzeit. Dabei erhöht jeder neue Virus, der den Antiviren-Datenbanken hinzugefügt wird, die Gesamtzeit der Untersuchung.

Andere Antivirenprogramme verkürzen die Untersuchungszeit, indem schwierig zu erkennende oder (in geografischer Hinsicht) seltene Viren, sowie kompliziert zu analysierende Dateiformate (z.B. pdf) nicht in die Antiviren-Datenbanken aufgenommen werden. Im Unterschied dazu ist sich «Kaspersky Lab» sicher, dass die Aufgabe eines Antivirenprogramms darin besteht, den Benutzern reale Antivirensicherheit zu garantieren.

Kaspersky Anti-Virus erlaubt erfahrenen Benutzern, die Antivirenuntersuchung zu beschleunigen, indem bestimmte Dateitypen von der Antivirenuntersuchung ausgeschlossen werden.

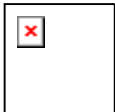
Kaspersky Anti-Virus erkennt über 2000 Formate von archivierten und komprimierten Dateien. Für die Antivirensicherheit ist das sehr wichtig, weil jedes der erkennbaren Formate einen ausführbaren schädlichen Code enthalten kann. Trotzdem arbeitet die neue Version des Produkts im Vergleich zur vorhergehenden schneller, obwohl sich die Gesamtzahl der von Kaspersky Anti-Virus erkennbaren Viren täglich erhöht (ungefähr 200 neue Viren pro Tag) und die Anzahl der unterstützten Formate ständig steigt. Das wird durch die Verwendung neuer Technologien wie iChecker™ und iStreams™ erreicht, die von «Kaspersky Lab» entwickelt wurden.



Frage: Wozu wird der Lizenzschlüssel benötigt? Funktioniert mein Anti-Virus ohne Lizenzschlüssel?

Kaspersky Anti-Virus funktioniert nicht ohne Lizenzschlüssel.

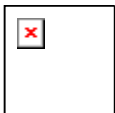
Wenn Sie sich noch nicht zum Erwerb von Kaspersky Anti-Virus entschlossen haben, können wir Ihnen einen Probeschlüssel (Evaluierungsschlüssel) anbieten, der für zwei Wochen oder einen Monat gültig ist. Nach Ablauf der Gültigkeitsdauer wird der Schlüssel gesperrt.



Frage: Was passiert, wenn die Lizenz zur Produktnutzung abläuft?

Bei Ablauf der Gültigkeitsdauer der Lizenz für die Nutzung von Kaspersky Anti-Virus setzt das Produkt seine Arbeit fort, aber die Verwendung neuer Antiviren-Datenbanken ist nicht mehr möglich. Kaspersky Anti-Virus wird weiterhin die Desinfektion infizierter Objekte durchführen, dabei jedoch die alten Antiviren-Datenbanken benutzen.

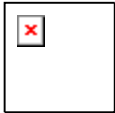
Sollte diese Situation eintreten, dann informieren Sie Ihren Systemadministrator oder wenden Sie sich zur Lizenzverlängerung an die Firma, bei der Kaspersky Anti-Virus erworben wurde, oder direkt an «Kaspersky Lab» Ltd.



Frage: Mein Anti-Virus funktioniert nicht.
Wie soll ich vorgehen?

Als Erstes, vergewissern Sie sich, dass Ihr Problem nicht in dieser Dokumentation oder auf Unserer Internet-Seite beschrieben ist.

Ausserdem, empfehlen wir Verbindung mit unserem Vertriebshändler aufzunehmen, bei dem Sie die Software erworben haben oder in dem Abschnitt Wissensdatenbank auf unserer Internet-Seite nach einer Lösung zu suchen (<http://www.kaspersky.com/faq>).



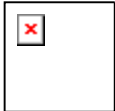
Frage: Was hat sich im Update-Dienst seit Version 5.0 geändert?

«Kaspersky Lab»s Produktlinie wurde ab Version 5.0 mit einem neuen Update-Dienst ausgestattet. Die Neuentwicklung beruht auf den Anregungen von Anwendern und auf Marketingüberlegungen. Daneben stellte sich die Aufgabe, die Technologie der gesamten Updateprozedur zu optimieren, die mit der Vorbereitung der Datenbanken bei «Kaspersky Lab» beginnt und mit dem Update der Benutzerdateien endet.

Vorteile des neuen Update-Dienstes:

- Vervollständigung des Datei-Downloads bei Verbindungsunterbrechung. Bereits heruntergeladene Updates müssen nach dem Wiederaufbau der Verbindung nicht mehr wiederholt geladen werden.
- Halbierung der Größe des kumulativen Updates. Ein kumulatives Update enthält die gesamte Antiviren-Datenbank, weshalb die Größe des Kumulativen jene eines gewöhnlichen Updates wesentlich übersteigt. Im neuen Update-Dienst kommt eine spezielle Technologie zum Einsatz, die es erlaubt, die bereits vorhandenen Antiviren-Datenbanken für das kumulative Update zu verwenden.
- Beschleunigter Download aus dem Internet. Kaspersky Anti-Virus wählt den Kaspersky-Lab-Updateserver, der in Ihrer Nähe liegt. Außerdem wird die Belastung der Server entsprechend ihrer Leistungsfähigkeit bestimmt, d.h. es wird kein überlasteter Server für den Download verwendet, wenn gleichzeitig ein anderer Server freie Ressourcen besitzt.
- Verwendung von "schwarzen Listen" für die Schlüssel. Dadurch können Benutzer, die keine Lizenz für die Nutzung von Kaspersky Anti-Virus besitzen, vom Update ausgeschlossen werden. Damit wird vermieden, dass lizenzierte Benutzer unter überlasteten Updateservern zu leiden haben.

- Für Unternehmens-Produkte wurde eine Option zum Erstellen eines lokalen Updateservers realisiert. Diese Funktion ist für Unternehmen erforderlich, in denen in einem lokalen Netzwerk Computer zusammengefasst sind, die durch Kaspersky-Lab-Anwendungen geschützt werden. In diesem Fall kann ein beliebiger Computer die Funktion des Updateservers übernehmen, der die Updates aus dem Internet empfängt, diese in einem lokalen Ordner ablegt und den anderen Netzwerkcomputern Zugriff darauf gewährt.



Frage: Kann ein Angreifer die Antiviren-Datenbanken verändern?

Alle Antiviren-Datenbanken besitzen eine eindeutige Signatur, die beim Zugriff auf die Datenbanken von Kaspersky Anti-Virus überprüft wird. Stimmt die Signatur nicht mit der von «Kaspersky Lab» vergebenen überein und das Datum einer Datenbank liegt nach dem Tag der Lizenzgültigkeit für die Produktbenutzung, dann wird Kaspersky Anti-Virus diese Datenbanken nicht verwenden.



Frage: Funktioniert Kaspersky Anti-Virus für Unix auf meiner Distribution des Betriebssystems Linux?

Kaspersky Anti-Virus für Unix Version 5.7 wurde auf Distributionen von RedHat, Debian und SuSE getestet und die Distributionen von Kaspersky Anti-Virus wurden speziell für diese erstellt.

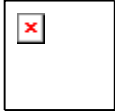
Auf den Distributionen, die nicht in der Liste der unterstützten von «Kaspersky Lab» stehen, können Fehler während Arbeit auftreten. Das hängt mit der Eigenart der Betriebssysteme zusammen. Ihre Distribution kann, z.B., eine andere Version einer Bibliothek benutzen oder der Pfad der Skripte zur Systeminitialisierung kann vom Standard abweichen. In dem Fall wird der Support von «Kaspersky Lab» keine Hilfe anbieten.



Frage: Warum startet die Komponente kavmonitor mehrere Prozesse gleichzeitig?

Maximale Anzahl der gestartete Prozesse wird von dem Parameter **CheckFileLimit** der Konfigurationsdatei begrenzt und bestimmt die Anzahl der gleichzeitig zu bearbeitenden Dateien. Deswegen ist die An-

zahl der Prozesse des Monitors immer mehr, als einer (standardmässig sind 20 Prozesse gestartet). Wenn keine Datei zum untersucht wird, werden keine Systemressourcen verbraucht.



Frage: Wie können die auf der Konsole angezeigten Meldungen des Programms in einer Datei gespeichert werden?

Um die Informationen, die während der Arbeit von Kaspersky Anti-Virus auf der Konsole angezeigt werden, zu speichern, müssen entweder entsprechende Einstellungen in der Konfigurationsdatei vorgenommen werden oder folgende Eingabe in der Befehlszeile erfolgen:

```
$ some_app > ./text_file 2>&1
```

wobei:

`some_app` – Anwendung, deren standardmäßige Ein- und Ausgabemeldungen über Fehler bei der Arbeit Sie in einer Datei speichern möchten.

`text_file` – vollständiger Pfad der Datei, in welcher die Informationen gespeichert werden sollen.

Beispiel:

```
# /opt/kaspersky/kav4ws/bin/kav4ws-keepup2date
> ./updater.log 2>&1
```

In diesem Fall werden in der Datei `updater.log` des aktuellen Ordners die ausgegebenen Standardmeldungen über Fehler der Komponente `keepup2date` aufgezeichnet.



Frage: Wo kann ich die Ergebnisse der Anwendungsarbeit nach dem Starten mit Hilfe von Kaspersky Administration Kit ansehen?

Standardmäßig wird keine Aufzeichnung der Anwendungsarbeit beim Starten mit Hilfe von Administration Kit geführt.

Um die Aufzeichnung der Anwendungsarbeit in einer Datei verändern Sie die Konfigurationsdatei wie folgt:

- Geben Sie die Detaillierungsebene des Protokolls ein (s. Pkt. 5.6 auf S. 47) mit Hilfe des Parameters **ReportLevel** im Abschnitt **[middleware.options]**.
- Geben Sie ein Verzeichnis an, in dem das Protokoll gespeichert wird.

Nach dem Beenden des Tasks wird im Verzeichnis eine der Dateien erstellt:

- *kavscanner_middleware.log* – nach dem Beenden des Tasks Scan auf Befehl;
- *keepup2date_middleware.log* – nach dem Beenden des Tasks Update der Antivirus-Datenbanken.

ANHANG C. «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 weitreichenden 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 der heuristischen Analyse-Engine 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: unsere 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.

C.1. Weitere Produkte und Services von «Kaspersky Lab»

Kaspersky Anti-Virus® 6.0

Kaspersky Anti-Virus 6.0 dient dem Schutz eines Personalcomputers vor schädlichen Programmen. Dabei werden traditionelle Virenschutzmethoden auf optimale Weise mit neuen proaktiven Technologien vereinigt.

Das Programm erlaubt eine komplexe Antivirenuntersuchung, die folgende Optionen umfasst:

- Antivirenuntersuchung 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.
- Antivirenuntersuchung des Internet-Datenstroms, der per HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.
- Antivirenuntersuchung 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 Betriebssystems 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 6.0 warnt den Benutzer rechtzeitig, wenn gefährliche, verdächtige oder versteckte Prozesse auftreten oder wenn normale Prozesse auf unerlaubte Weise verändert werden.
- **Überwachung von Veränderungen in der Registrierung des Betriebssystemes** durch die Kontrolle des Zustands der Systemregistrierung.
- **Sperren gefährlicher Makros** des Typs Visual Basic for Applications in Microsoft Office Dokumenten.
- **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 Lab» News Agent

Das Programm News Agent dient der schnellen Zustellung von Nachrichten von «Kaspersky Lab», über das "Viren-Wetter" und über neu erschienene Meldungen. 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 Stati.
- Öffnen der Webseite mit dem vollständigen Nachrichtentext im Browser.

Der News Agent funktioniert unter dem Betriebssystem Microsoft Windows. Er kann als separates Produkt 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 Antivirenuntersuchung des Computers im Online-Modus erlaubt. Kaspersky OnLine Scanner wird direkt im Browser ausgeführt und verwendet die Technologie Microsoft ActiveX®. Dadurch kann der Benutzer auf schnelle Weise herausfinden, ob sein Computer von einer Infektion durch schädliche Programme bedroht ist. Im Rahmen der Untersuchung kann der Benutzer:

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Datenbanken für die Untersuchung wählen.
- Gefundene infizierte Objekte desinfizieren.
- die Untersuchungsergebnisse in Berichten mit dem Format txt und html speichern.

Kaspersky® OnLine Scanner Pro

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

- Archive und Mail-Datenbanken von der Untersuchung ausschließen.
- standardmäßige oder erweiterte Antiviren-Datenbanken für die Untersuchung wählen.
- die Untersuchungsergebnisse in Berichten mit dem Format txt und html speichern.

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 Popupfenstern 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, Tro-

janern 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 PDA

Kaspersky® Security für PDA gewährleistet zuverlässigen Virenschutz für Daten auf Handheld-PCs unter Palm OS oder Microsoft Windows CE sowie für Daten, die von einem gewöhnlichen PC oder Erweiterungsspeicher, von CD-ROM oder aus Datenbanken übernommen werden. Das Programm umfasst eine optimale Auswahl an Virenschutz-Komponenten:

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

Weiterhin schützt das Programm die auf dem PDA gespeicherten Informationen vor unberechtigtem Zugriff durch Verschlüsselung im Speicher des PDA und auf Speicherkarten.

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*
- *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® Business Optimal

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

Kaspersky Anti-Virus® Business Optimal bietet Rundumschutz¹ vor Viren für:

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

Kaspersky Anti-Virus® Business Optimal beinhaltet außerdem das zentrale 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 Nachrichten auf Spam überprüft. Das Programm ist kompatibel mit jedem beliebigen Mail-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. Die Datenbank-Updates erscheinen alle 20 Minuten.

Kaspersky® SMTP Gateway

Kaspersky® SMTP-Gateway for Linux / Unix dient dem Antivirenschutz von E-Mails, die per SMTP-Protokoll weitergeleitet werden. Die Anwendung umfasst eine Reihe von zusätzlichen Filterinstrumenten für den Mailverkehr (Filterung nach Namen und MIME-Typen von Attachments) sowie eine Reihe von Mitteln, die es erlauben, die Belastung des Mailsystems zu verringern und Hackerangriffe abzuwehren. Dazu zählen die Begrenzung der maximalen

¹ Je nach Lieferumfang

Mailgröße, der Anzahl von Adressaten usw. Die Unterstützung der Technologie DNS Black List schützt vor dem Empfang von Mails, die von Servern stammen, die auf diesen Listen stehen und als Verbreitungsquellen für Spam gelten.

Kaspersky® Anti-Virus für MIMESweeper

Kaspersky® Anti-Virus für MIMESweeper bietet eine Hochgeschwindigkeit-Anitivirusüberprüfung des Netzwerkverkehrs auf den Servern, welche Clearswift MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web benutzen.

Das Programm ist als PlugIn ausgeführt (Erweiterungsmodule) und überprüft in Echtzeit ein- und ausgehende E-Mails nach Viren.

C.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 Lab»s GmbH
 Steinheilstraße 13
 85053 Ingolstadt

Technischer Support	Tel.: +49 (0) 841 98 18 90 Fax: +49 (0) 841 98 18 918 E-Mail: support@kaspersky.de
Allgemeine Informationen	WWW: http://www.kaspersky.de http://www.viruslist.de/
Feedback zu unseren Benutzerhandbüchern	docfeedback@kaspersky.com (Diese Adresse ist für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.)

ANHANG D. 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 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 des Landes, indem das Produkt erworben wurde