

KASPERSKY LAB

Kaspersky Anti-Virus[®] 5.5 für
Linux /FreeBSD
Workstations und File Server

ADMINISTRATOR'S GUIDE

KASPERSKY ANTI-VIRUS® 5.5 FOR
LINUX/FREEBSD WORKSTATIONS AND FILE SERVERS

Handbuch für Administratoren

© Kaspersky Lab Ltd.
<http://www.kaspersky.com/de/>
Redaktionsdatum: September 2006

Inhalt

KAPITEL 1. EINFÜHRUNG	6
1.1. Viren und schädliche Programme	7
1.2. Funktionen von Kaspersky Anti-Virus.....	8
1.3. Was ist neu in Version 5.5.....	8
1.4. Lizenzierungspolitik	9
1.5. Hardware- und Softwarevoraussetzungen.....	10
1.6. Lieferumfang.....	11
1.7. Textgestaltung	12
KAPITEL 2. ARBEITSALGORITHMUS DER ANWENDUNG.....	14
KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-VIRUS.....	16
1.1. Installation der Anwendung auf einem Linux-Computer	16
3.1. Installation der Anwendung auf einem FreeBSD-Server.....	17
3.2. Installationsprozess	17
3.3. Update-Prozess zur Version 5.5.....	18
3.4. Installation des Lizenzschlüssels	18
3.5. Anordnung der Dateien in den Verzeichnissen.....	19
3.6. Abschluss der Installation.....	22
KAPITEL 4. KONFIGURATION DER ANWENDUNG NACH DER INSTALLATION.....	23
4.1. Standardeinstellungen der Anwendung	23
4.2. Installation der Antiviren-Datenbanken.....	24
4.3. Konfiguration der Zusammenarbeit mit Webmin.....	24
KAPITEL 5. ARBEITEN MIT KASPERSKY ANTI-VIRUS	26
5.1. Update der Antiviren-Datenbanken	26
5.1.1. Neue Optionen der Update-Komponente.....	27
5.1.2. Automatisches Updaten der Antiviren-Datenbanken.....	29
5.1.3. Update der Antiviren-Datenbanken auf Befehl.....	30
5.1.4. Erstellen eines Netzwerkordners zum Speichern und Kopieren der Antiviren-Datenbanken	31

5.2. Antivirenschutz des Dateisystems	32
5.2.1. Untersuchungsbereich	33
5.2.2. Modus zur Untersuchung und Desinfektion von Objekten	34
5.2.3. Aktionen für Objekte	35
5.2.4. Scan auf Befehl eines einzelnen Ordners	36
5.2.5. Zeitgesteuerte Untersuchung eines Ordners	37
5.2.6. Zusätzliche Optionen: Verwendung von Skriptdateien	37
5.2.6.1. Desinfektion von infizierten Objekten in einem Archiv.....	37
5.2.6.2. Senden von Benachrichtigungen an den Administrator.....	38
5.3. Echtzeit-Antivirenschutz	39
5.4. Verwaltung von Lizenzschlüsseln.....	40
5.4.1. Informationen über den Lizenzschlüssel ansehen.....	41
5.4.2. Lizenzverlängerung	42
KAPITEL 6. ERWEITERTE EINSTELLUNGEN.....	44
6.1. Optimierung der Arbeit von Kaspersky Anti-Virus.....	44
6.2. Verschieben von Objekten in Quarantäne-Ordner	46
6.3. Modus zum Erstellen von Sicherheitskopien (Backup).....	48
6.4. Lokalisierung der Datums- und Uhrzeitanzeige	48
6.5. Parameter für die Erstellung von Protokollen für Kaspersky Anti-Virus	49
KAPITEL 7. DEINSTALLATION VON KASPERSKY ANTI-VIRUS	51
KAPITEL 8. TESTEN DER FUNKTIONALITÄT VON KASPERSKY ANTI-VIRUS....	52
ANHANG A. ZUSÄTZLICHE ANWENDUNGSINFORMATIONEN	54
A.1. Konfigurationsdatei des Kaspersky Anti-Virus	54
A.2. Befehlszeilenoptionen der Komponente kavscanner	62
A.3. Rückgabewerte der Komponente kavscanner	65
A.4. Befehlszeilenoptionen der Komponente kavmonitor	66
A.5. Befehlszeilenoptionen der Komponente licensemanager.....	66
A.6. Rückgabewerte der Komponente licensemanager	67
A.7. Befehlszeilenoption der Komponente keepup2date.....	67
A.8. Rückgabewerte der Komponente keepup2date.....	69
ANHANG B. HÄUFIGE FRAGEN	70
ANHANG C. KASPERSKY LAB	75
C.1. Weitere Produkte und Services von Kaspersky Lab	76

C.2. Kontaktinformationen.....	81
ANHANG D. ENDBENUTZER-LIZENZVERTRAG.....	83

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 „nutzliche“ 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 Informationskanäle 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 und FreeBSD Workstation und File Server** (weiter auch Kaspersky Anti-Virus, *Anwendung*) ist zum Antiviren-Schutz der File-Server und Arbeitsstationen, die unter LINUX- und FreeBSD-Betriebssystemen arbeiten, bestimmt.

Kaspersky Anti-Virus für Linux und FreeBSD ermöglicht Ihnen:

- Echtzeitschutz des Dateisystems gegen schädlichen Code: aufgerufene Dateien werden abfangen; diese werden analysieren; infizierte Objekte desinfiziert 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 lokalen Ordner oder interne Server benutzt werden.
- Die Verwaltung des Kaspersky Anti-Virus Produktes mit Hilfe der Konfigurationsdatei und des Web-Interfaces, basierend auf dem des Programm Webmin.

1.3. Was ist neu in Version 5.5

In der Version **Kaspersky Anti-Virus 5.5 für Linux/FreeBSD Workstation and File Server** wurden im Vergleich zu Version 5.0 folgende Änderungen vorgenommen:

- Die neue Komponente *kavmonitor* wurde dem Produkt hinzugefügt. Sie dient dem Antivirenschutz von Dateien im Echtzeitmodus.
- Neue Technologien zum Download von Updates der Antiviren-Datenbanken und Programmmodule der Anwendung wurden integriert. Dazu zählen die Integritätsprüfung und eine Option zur Verwendung bereits herunter geladener Datenbanken. Dadurch wird eine wesentliche Einsparung von Netzwerkressourcen erlaubt.

- Hinzugefügt wurde eine Option zur Auswahl des Typs der Antiviren-Datenbanken (Standard-Datenbanken, erweiterte oder redundante Datenbanken). Dabei kann der Typ der zu verwendenden Antiviren-Datenbanken für jede Komponente der Anwendung separat festgelegt werden.
- Der Installations- und Deinstallationsprozess für die Anwendung wurde wesentlich vereinfacht.
- Bei der Installation der Anwendung besteht nun die Möglichkeit zum Importieren der Einstellungen einer Vorgängerversion von Anti-Virus (Version 5.0). Dadurch ist ein einfacheres Upgrade von älteren Versionen möglich.
- Es besteht die Möglichkeit zum Anlegen eines Backup-Ordners, in dem Sicherheitskopien verdächtiger und infizierter Objekte vor der Desinfektion oder dem Löschen gespeichert werden. Dadurch kann der Verlust von Originaldaten vermieden werden, wenn während des Desinfektionsvorgangs unvorhergesehene Situationen eintreten.
- Zur Verringerung der Computerbelastung beim Durchführen einer Antivirenuntersuchung wurden die Technologien zur Verwendung der iChecker™-Datenbanken und zweistufigen Cache-Speicherung untersuchter Objekte integriert.
- Eine Option zur Generierung einer Liste der erkennbaren Viren wurde hinzugefügt.
- Es wurde eine Auswahl der möglichen Vorgehensweisen beim Erkennen eines Virus hinzugefügt.
- Unterstützung der 64-bit Betriebssysteme ist realisiert.
- Die Optionen der Virensuche nach Befehl wurden erweitert.

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:
- Eines der folgenden Betriebssysteme für die 32 bit Plattform:
 - RedHat Linux 9.0.
 - RedHat Enterprise Linux Advanced Server 4 UPD3.
 - RedHat Fedora Core 5.
 - SUSE Linux Enterprise Server 9.0 SP3.
 - Novell Linux Desktop 9.
 - SUSE Linux Professional 10.1.
 - Debian GNU/Linux Version 3.1 R2.
 - Mandriva 2006.
 - FreeBSD Version 4.11.
 - FreeBSD Version 5.4.
 - FreeBSD Version 6.1.
- Eines der folgenden Betriebssysteme für die 64 bit Plattform:
 - RedHat Enterprise Linux Advanced Server 4 UPD3.
 - RedHat Fedora Core 5.
 - SUSE Linux Professional 10.1.
 - SUSE LES 9 SP3.
 - 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 Betriebssystemkerns – zur Verwendung der Komponente *kavmonitor*.



Beachten Sie, dass Kaspersky Antivirus die gemeinsame Arbeit mit SELinux nicht unterstützt. Das Benutzen SELinux kann zum Auftauchen der 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.

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.

Lizenzvereinbarung





Die Lizenzvereinbarung 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 die Lizenzvereinbarung sorgfältig!

1.7. 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.
 Um diese Aktion durchzuführen, 1. Schritt 1. 2. ...	Beschreibung einer Folge von Schritten und möglichen Aktionen, die vom Benutzer durchgeführt werden.
 Aufgabe, Beispiel	Aufgabenstellung, Beispiel für die Realisierung der Optionen des Softwareprodukts.

Formatierung	Bedeutung
 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*;
- 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.
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 Zugriffscode (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.

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). Sollten bestimmte Anwendungen (z.B. perl) nicht installiert sein, dann wird deren Installation empfohlen. Andernfalls ergibt sich eine teilweise Einschränkung der Anwendungsfunktionalität.
- 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>
```

3.2. Installation der Anwendung auf einem FreeBSD-Server

Für Server, die mit dem Betriebssystem FreeBSD arbeiten, wird die Distribution von Kaspersky Anti-Virus® als pkg-Paket geliefert.



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

```
pkg_add < Paketname >
```

3.3. Installationsprozess

Die Installation der Anwendung wird automatisch durchgeführt und umfasst folgende Etappen:

1. Kopieren der Distributionsdateien auf den Computer.
2. Installation des Lizenzschlüssels.
3. 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. Pnk. 5.5.4 auf S. 40)
4. Konfiguration der Komponente *keepup2date*.
5. Installation (Update) der Antiviren-Datenbanken.



Denken Sie daran, die Antiviren-Datenbanken zu installieren, bevor Sie mit der Verwendung der Anwendung beginnen. Ohne Antiviren-Datenbanken sind Untersuchung und Bearbeitung von Dateien nicht möglich!

6. Installation des Moduls Webmin.

Das Modul zur Fernverwaltung für Webmin wird nur unter der Bedingung installiert, dass sich Webmin im standardmäßigen Ordner befindet. Nach der Installation des Moduls erfolgen entsprechende Empfehlungen zur Konfiguration der gemeinsamen Arbeit mit der Anwendung.



Nach der Installation ist das Kompilieren und die Installation des Kernelmoduls für die Untersuchung im Echtzeitmodus erforderlich!



Bei der Arbeit mit dem Betriebssystem Linux müssen Sie beachten, dass beim Updaten des Kernels des Betriebssystems auch das Kernel-Modul kavmonitor upgedatet werden muss.

3.4. Update-Prozess zur Version 5.5

Während des Installationsprozesses erfolgt die Inspektion des Systems zur Suche nach einem bereits installierten Kaspersky Anti-Virus einer älteren Version als 5.5.

Wenn eine Vorgängerversion der Anwendung gefunden wird, werden bestimmte alten Einstellungen von Kaspersky Anti-Virus in die Konfigurationsdatei für die Version 5.5 importiert.



Die Distribution der älteren Version von Kaspersky Anti-Virus wird während des Installationsprozesses nicht entfernt. Diese Aufgabe bleibt dem Administrator überlassen.

Ein Teil der Standardparameter der Konfigurationsdatei (beispielsweise der Pfad des Ordners zum Speichern der Antiviren-Datenbanken) wird nicht exportiert, sondern während des Installationsprozesses festgelegt.

Außerdem wurden in der Version 5.5 der Anwendung im Vergleich zu den Versionen 5.0 und 4.0 einige Änderungen vorgenommen, welche sich auf die Logik der Arbeit einzelner Komponenten beziehen, sowie eine Reihe von Optionen hinzugefügt. Deshalb wird empfohlen, vor dem Beginn der Arbeit mit der Anwendung die Korrektheit der Konfigurationsdatei zu überprüfen.

3.5. 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 folgenden 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. 40).

3.6. 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.

`/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.

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

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

`kav4ws-kavmonitor` – ausführende Datei der Komponente des Antivirusschutzes.

`/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.

`/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.



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



Nachdem Kaspersky Antivirus auf einem Computer mit dem FreeBSD-Betriebssystem installiert ist, werden die Dateien der Distribution wie folgt verteilt:

`/usr/local/etc/kaspersky/` – Verzeichnis, in dem die Konfigurationsdatei des Kaspersky Antivirus liegt:

`kav4ws.conf` – Konfigurationsdatei.

`/usr/local/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.

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

`kav4ws-kavmonitor` – ausführende Datei der Komponente des Antivirusschutzes.

`/usr/local/man/` – Verzeichnis zum Speichern der man-Dateien.

`/usr/local/src/kav4ws/` – Verzeichnis zum Speichern des Antivirus Kernel-Modules der Anwendung.

`/usr/local/share/kav4ws/contrib/kav4ws.wbm` – Plug-In für das Programm Webmin.

`/usr/local/share/kav4ws/contrib/vox.sh` – Skript `vox.sh`, wird zum säubern der Archive benutzt.

`/usr/local/share/doc/kav4ws/LICENSE` – Lizenzvereinbarung.

`/var/db/kaspersky/kav4ws/bases` – Verzeichnis zum Speichern der Antivirus-Datenbanken;

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



Nach dem Kaspersky Antivirus auf einem Linux-Server 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.

`/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.

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

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

`kav4ws-kavmonitor` – ausführende Datei der Komponente des Antivirusschutzes.

`/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.

`/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.



Um das Hilfe-System des Kaspersky Antivirus zu installieren (manual pages) geben Sie der Variable **MANPATH** den Wert **`/opt/kaspersky/kav4fs/man`**.



Nach dem Kaspersky Antivirus auf ein Computer mit dem FreeBSD-Server Betriebssystem installiert ist, werden die Dateien der Distribution wie folgt verteilt:

`/usr/local/etc/kaspersky/` – Verzeichnis, in dem die Konfigurationsdatei des Kaspersky Antivirus liegt:

`kav4ws.conf` – Konfigurationsdatei.

/usr/local/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.

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

kav4ws-kavmonitor – ausführende Datei der Komponente des Antivirusschutzes.

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

/usr/local/src/kav4ws/ – Verzeichnis zum Speichern des Antivirus Kernel-Modules der Anwendung.

/usr/local/share/kav4ws/contrib/kav4ws.wbm – Plug-In für das Programm Webmin.

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

/usr/local/share/doc/kav4ws/LICENSE – Lizenzvereinbarung.

/var/db/kaspersky/kav4ws/bases – Verzeichnis zum Speichern der Antivirus-Datenbanken;

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



Weiter werden die Bezeichnungen der Komponente benutzt, die in der Linux-Server Umgebung üblich sind!

3.7. 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 der Datei 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. Kapitel 4 auf S. 23).

KAPITEL 4. KONFIGURATION DER ANWENDUNG NACH DER INSTALLATION

Während des Installationsprozesses erfolgt eine Analyse des Systems, auf dem Kaspersky Anti-Virus installiert wird, und bestimmte Konfigurationsparameter werden automatisch festgelegt. Für eine Reihe von Parametern der Konfigurationsdatei der Anwendung gelten Standardwerte, welche die Arbeit mit Anti-Virus möglichst komfortabel gestalten (s. Pkt. 4.1 auf S. 23).

In diesem Kapitel beschreiben wir, welche Einstellungen für Kaspersky Anti-Virus als Standard gelten, und erläutern welche Parameter vor der Arbeit mit der Anwendung definiert werden sollen.

4.1. Standardeinstellungen der Anwendung

Alle Funktionsparameter von Kaspersky Anti-Virus sind in der Konfigurationsdatei *kav4fs.conf* gespeichert, welche standardmäßig verwendet wird.

Die Konfiguration wird folgendermaßen ausgeführt:

- Beim Starten des Betriebssystems nimmt Kaspersky Anti-Virus automatisch seine Arbeit auf. Das Programm fängt alle Aktivitäten innerhalb des Dateisystems ab und analysiert diese. Beim Auffinden von infizierten, verdächtigen oder beschädigten Dateien, schreibt Kaspersky Anti-Virus eine Meldung in die Bericht-Datei **kavmonitor.log**.
- Beim Starten der Suche auf Befehl, in der Befehlszeile, wird kann das komplette Dateisystem durchsucht werden. Meldungen werden von Kaspersky Anti-Virus in der Konsole angezeigt und in die Bericht-Datei **kavscanner.log** geschrieben.



Beachten Sie, dass als Standard die infizierten Objekte nicht desinfiziert oder isoliert werden!

4.2. Installation der Antiviren-Datenbanken

Die Suche und Desinfektion von infizierten Objekten wird auf Basis der Einträge der Antiviren-Datenbanken ausgeführt. Diese enthalten Beschreibungen aller bisher bekannten Viren und Methoden zur Reparatur infizierter Objekte. Es ist überaus wichtig, die Antiviren-Datenbanken auf aktuellem Stand zu halten.



Jeden Tag tauchen neue Virenauf. Es wird empfohlen, das Update der Antiviren-Datenbanken unbedingt **sofort** nach der Installation der Anwendung vorzunehmen.

Das Update der Datenbanken wird von Kaspersky Anti-Virus mit Hilfe der Komponente *keepup2date* durchgeführt. Geben Sie in der Befehlszeile ein:

```
/Pfad/von/ kav4fs-keepup2date
```

Die Antiviren-Datenbanken werden von den Kaspersky-Lab-Updateservern kopiert und in einem speziellen Ordner gespeichert, der in der Konfigurationsdatei festgelegt ist.

4.3. Konfiguration der Zusammenarbeit mit Webmin

Wird die Fern-Administration von Kaspersky Anti-Virus gewünscht, dann ist die Konfiguration der Zusammenarbeit mit dem Paket Webmin zu empfehlen.

Alle Einstellungen, die mit Hilfe des Programms Webmin vorgenommen wurden, werden in der standardmäßig verwendeten Konfigurationsdatei der Anwendung gespeichert.



Wenn Sie mit Hilfe des Programms Webmin eine alternative Konfigurationsdatei anlegen wollen:

1. Kopieren Sie die Daten aus der bestehenden Konfigurationsdatei in die neue Konfigurationsdatei, die unter einem anderen Namen gespeichert wird. Nehmen Sie dann die für Ihre Aufgaben erforderlichen Korrekturen der neuen (alternativen) Konfigurationsdatei vor.
2. Geben Sie den Namen der alternativen Konfigurationsdatei auf der Registerkarte **Config edit** im Eingabefeld des Parameters **Full path to KAV config** an.



Ausführliche Informationen zu den verschiedenen Einstellungen von **Webmin** erhalten Sie im Handbuch dieses Produktes. Bei Fragen über das Modul zur Fernadministration von Kaspersky Anti-Virus können Sie auch das Hilfesystem des Programmes Webmin verwenden.

Bei der Beschreibung von Einstellungen und Start bestimmter Aufgaben wird im Folgenden die Verwaltung über Webmin **nicht erwähnt!**

KAPITEL 5. 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. 5.1 auf S. 26).
- Antivirenschutz von Computerdateisystemen (Untersuchung nach Zeitplan und/oder auf Befehl) (Details s. Pkt. 5.2 auf S. 32)
- Echtzeit-Antivirenschutz (Schutz im Echtzeitmodus) (Details S.39).

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.

5.1. 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 *updcfg.xml*, die zum Lieferumfang der Anwendung gehört.

Beim Updateprozess greift die Komponente *keepup2date* auf die genannte Liste zu, wählt eine Adresse aus und versucht, die Antiviren-Datenbanken vom Server herunterzuladen. 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.

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. 5.1.4 auf S. 31.

Die Aktualisierung lässt sich nach Zeitplan mit Hilfe des Programms **cron** (s. Pkt. 5.1.2 auf S. 29) oder auf Befehl des Administrators aus der Befehlszeile durchführen.



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

5.1.1. Neue Optionen der Update-Komponente

In Version 5.5 von Kaspersky Anti-Virus wurde *im Unterschied zu den vorigen Versionen* die Komponente zum Update der Antiviren-Datenbanken ersetzt. In der neuen Komponente wurden bestehende Funktionen optimiert und neue Optionen hinzugefügt:

- Option zur automatischen Auswahl des geographisch nächsten Updateservers, basierend auf der in der Konfigurationsdatei angegebenen Region;
- Option zum Download und zur Installation von inkrementellen Updates beim Erscheinen eines kumulativen Updates. Dadurch können Netzwerkressourcen eingespart werden;

- Wenn die Verbindung während des Kopierens der Antiviren-Datenbanken getrennt wird oder nach dem Wiederherstellen der Verbindung der Updateserver gewechselt wird, lädt die Komponente automatisch den verbleibenden Teil der Antiviren-Datenbanken herunter und beginnt den Download nicht von vorne;
- Überprüfung der Vollständigkeit von heruntergeladenen Datenbanken;
- Das Analysieren der Vollständigkeit der installierten Datenbanken und das Herunterladen nur der geänderten Datenbanken oder hinzugekommenen Elemente der Datenbank. Dies hilft auch beim einsparen der Netzwerkressourcen;
- Option zum Starten eines benutzerdefinierten Befehls zum erneuten Laden der Antiviren-Datenbanken direkt nach dem erfolgreichen Update;
- Unterstützung der Option zur Rückkehr zu der vorigen Version der Antiviren-Datenbanken (rollbacks);
- Für die Arbeit der neuen Komponente ist das Programm wget nicht erforderlich;
- Option zur Auswahl der zu kopierenden Datenbanken (Standard-Datenbanken oder erweiterte Datenbanken).

Standard-Datenbanken – Antiviren-Datenbanken, die Beschreibung aller zurzeit existierende Viren enthalten, Methoden zur dessen Suche und Desinfektion. Diese Datenbanken werden Standardmässig benutzt.

Erweiterte Datenbanken – Antiviren-Datenbanken, die ausser Viren-Informationen auch die Informationen über Programme aus den Risiko-Gruppen (RiskWare) und Werbungs-Programme (AdWare) enthalten.

Programme aus der Risiko-Gruppe enthalten Schwachstellen, die für Hacker-Angriffe oder zum Einschleusen von unautorisierten Programmen benutzt werden.

Werbungs-Programme werden mit irgendeiner Software installiert und zeigen Werbungsinformationen an, in dem sie entweder zusätzliche Fenster öffnen, oder den Benutzer dazu zwingen, den Web-Site des Werbungsgeber zu besuchen. Außerdem, dass die Werbung aufgezwungen wird, verbrauchen solche Programme eine beachtliche Menge der Netzwerkressourcen.

Für die normale Arbeit genügt es, die Standard-Datenbanken zu wählen. Erweiterte Datenbanken dienen zum Sicherstellen einer höheren Schutzstufe. Das Benutzen dieser führt zu höherem Ressourcenverbrauch.

5.1.2. Automatisches Updaten der Antiviren-Datenbanken

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



Aufgabe: Festlegen eines automatischen Updates der Antiviren-Datenbanken alle drei Stunden. 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 0-23/3 * * * /opt/kaspersky/bin/kav4fs-
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 **UseUpdateServerUri** und **UseUpdateServerUriOnly** im Abschnitt **[updater.options]** den Wert **Yes**. Ausserdem, soll der Parameter **UpdateServerUri** 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 **UseUpdateServerUri** im Abschnitt **[updater.options]** den Wert **Yes** und dem Parameter **UseUpdateServerUriOnly** den Wert **No**. Außerdem soll der Parameter **UpdateServerUri** die Adresse des Update-Servers enthalten.

5.1.3. Update der Antiviren-Datenbanken auf Befehl

Die Aktualisierung der Antiviren-Datenbanken kann jederzeit aus der Befehlszeile gestartet werden.



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:

```
# kav4fs-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 herunter - zuladen, 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:

```
# kav4fs-keepup2date -l /tmp/report.txt
```

5.1.4. 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 Proxyservers 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.

5.2. 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. 5.2.2 auf S. 34).
- Aktionen für Objekte (s. Pkt. 5.2.3 auf S. 35).
- Parameter zum erstellen der Protokolle. (s. Pkt. 6.5 auf S. 49).

Das Durchsuchen des Dateisystems kann folgendermaßen gestartet werden:

- Einmalig aus der Befehlszeile.
- Nach Zeitplan mit Hilfe des Programmes **cron** (s. Pkt. 5.2.5 auf S. 37).



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

5.2.1. 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.).

Standardmässig 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 Scan-Pfad auf folgenden Möglichkeiten 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 *kav4fs.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 <Dateiname>** beim Start der Komponente.

Die standardmäßigen Untersuchungsobjekte werden ebenfalls in der Konfigurationsdatei *kav4fs.conf* (Abschnitt **[scanner.options]**) festgelegt und können geändert werden:

- direkt in dieser Datei;
- durch Befehlszeilenparameter beim Start der Komponente;
- durch Verwendung einer alternativen Konfigurationsdatei.

5.2.2. 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. 6.5 auf S. 49).

Als Ergebnis der Viruenuntersuchung erhält eine 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.

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.

5.2.3. Aktionen für Objekte

Abhängig vom Status eines Objektes (s. Pkt. 5.2.2 auf S. 34) 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 *kav4fs.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 *kav4fs.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]**).

5.2.4. 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 nur in der Protokolldatei *kavscanner-aktuelles_Datum-pid.log* erscheinen, die im gleichen Ordner gespeichert wird.



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

```
# kav4fs-kavscanner -rlq -pi/tmp/infected.lst
-ps/tmp/suspicion.lst -pc/tmp/corrupted.lst
-pw/tmp/warning.lst -o /tmp/kav4fs-kavscanner-`date
"+%Y-%m-%d-$$"` .log -i3 -ePASBMe -j3 -mCn /tmp
```

5.2.5. 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 * * * /path/to/kav4fs-kavscanner -c  
/etc/kav/scanhome.conf /home
```

5.2.6. 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.

5.2.6.1. 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/kav4fs/share/contrib/vox.sh <Pfad zu  
der Archiv-Datei>
```

5.2.6.2. 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 **`kav4fs.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 **`kav4fs.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 kav4fs-kavscanner admin@localhost.ru
```

```
[scanner.container]
OnInfected=exec echo archive %FULLPATH%/%FILENAME% is
infected, viruses list is in the attached file %LIST%
| mail -s kav4fs-kavscanner -a %LIST%
admin@localhost.ru
```



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

5.3. Echtzeit-Antivirenschutz

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



Alle Parameter der Funktion der Komponente *kavmonitor* sind im 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 vom Benutzer angeforderten Objekte nach Viren und schädlichen Programmen untersucht:

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

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;

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.

5.4. 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.

5.4.1. 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:

```
kav4fs-licensemanager -s
```

Auf dem Bildschirm erscheinen beispielsweise folgende Informationen:

```
Kaspersky license manager Version 5.5  
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 anzusehen,

Geben Sie in der Befehlszeile ein:

```
kav4fs-licensemanager -k 0003D3EA.key
```

Auf dem Bildschirm erscheinen beispielsweise folgende Informationen:

```
Kaspersky license manager Version 5.5  
Copyright (C) Kaspersky Lab. 1997-2007.  
Portions Copyright (C) Ian Crypto  
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus  
for Linux", expires 04-07-2003 in 28 days
```

5.4.2. 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. 40 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 verlängern:

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 **PRODUKTE → 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:

```
kav4fs-licensemanager -a <Name der Schlüssel-Datei>
```

Es wird empfohlen, anschließend die Antiviren-Datenbanken zu aktualisieren (s. Pkt. 5.1 auf S. 26).



Um Lizenzschlüssel zu entfernen,

Geben Sie in der Befehlszeile ein:

```
kav4fs-licensemanager -d <Name der Schlüssel-Datei>
```

KAPITEL 6. 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.

6.1. 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 **lcheckerDbFile** 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 5.5 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.

6.2. 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
```

6.3. 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!

6.4. 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 Uhrzeitangabe.

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 **DateFormat**) im Format Jahr/Monat/Tag bzw. Monat/Tag/Jahr.

6.5. 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.
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.
2	Warning	Informationen über Fehler, die zum Beenden der Arbeit des Produkts führen können (z.B. Informationen über unzureichenden Platz auf einem Laufwerk).
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.
4	Activity	Meldungen über die Untersuchung von Objekten entsprechend dem Niveau der Protokollgenauigkeit.

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.

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.



Wenn Sie bei der Installation das rpm-Paket für Kaspersky Anti-Virus 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>
```




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

```
pkg_delete <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. Falls keine Internetverbindung besteht, können Sie selbst einen "Test-Virus" herstellen. Geben Sie dazu in einen beliebigen Texteditor folgende Zeichenkette ein und speichern Sie die Datei als **eicar.com**:

```
X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*
```

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-X5O!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 ANWENDUNGSINFORMATIONEN

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 **[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 auszuschalten, setzen Sie den Wert auf **no**.

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

SelfExtArchives=yes – Untersuchungsmodus für selbstentpackende Archive. Um diesen auszuschalten, 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=yes – Untersuchungsmodus der Post-Datenbanken. Um diesen auszuschalten, vergeben Sie dem Parameter den Wert **no**.

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

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 – Gösse des Cache (in MB).

KernelCacheSize – Gösse des Cache, für Einträge im Kernel-Speicher (in MB).

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-Datenbank**, 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 angeben:

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 passwortgeschützten 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.

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

ReportLevel=4 – Stufe der Protokollgenauigkeit.

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 der Server-Dateisysteme:

- 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.
- lchecker=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-Datenbank**, 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.

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.
- 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 Server-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 des Parameters **Aktion** besteht aus zwei Teile: aus der Aktion selbst und aus einem Parameter, welche durch Leerzeichen geteilt sind. Der Wert des zusätzlichen Parameters wird in Anführungszeichen geschrieben. Z.B.: **OnInfected=move "/tmp/infected"**

Aktion kann einen der folgenden Werte annehmen:

- *move* <Ordner> – Datei verschieben in < Ordner >.
- *movePath* <Ordner> – Datei rekursiv verschieben in <Ordner> (mit dem absoluten Pfad).
- *remove* – Datei löschen.
- *exec* <Parameter> – Aktion am Objekt vornehmen, welche mit <Parameter> definiert ist.

Als Makros des Zusätzlichen Parameters der Aktion **exec** können für Container benutzt werden:

- %LIST% – Dateiname oder Auflistung der infizierten, verdächtigen und beschädigten Dateien in dem Container. Das Dateiformat hat folgende Form: **<Virusname>|<Dateiname>**.
- %FULLPATH% – voller Pfad zum Container.
- %FILENAME% – Dateiname ohne Pfad.

%CONTAINERTYPE% – Containertyp in Form einer Zeile. Der Abschnitt **[scanner.object]** enthält Parameter, die die Behandlung der einfachen Objekte unterschiedlicher Typen beim Antivirenschutz des Fileservers 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 der Aktionen welche auf Objekte anwendbar sind ist der gleich, welche im Abschnitt **[scanner.container]** 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.

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 Proxyserver beim Verbinden mit dem Updateserver von Kaspersky Lab. Wenn der Wert **no** ist, wird kein Proxyserver benutzt. Wenn der Wert **yes** ist, wird der Proxyserver 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 Proxyserver benutzt.

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

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

UpdateServerUrl=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.

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;
-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:

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*.
- v Die Version der Anwendung anzeigen.

Arbeitsoptionen für Lizenzschlüssel:

- 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 <Dateipfad>** Lizenzschlüssel 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.

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;
-s	Liste der Updateserver in der Konsole anzeigen;
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 Konfigurationsdatei benutzen <Pfad_zur_Datei > . Option funktioniert, wenn auf dem Server nur eine Anwendung von Kaspersky Lab installiert ist oder wenn die Update-Anwendung mit dem Schlüssel -p definiert ist (sonst wird eine Systemmeldung über mehrere Anwendungen angezeigt);
-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:	
-l <Pfad_zur_Datei>	Ergebnisse in die Datei < Pfad_zur_Datei > 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 PostUpdateCmd 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.

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/fag>).



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

Kaspersky Labs 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 5.5 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?*

Anzahl der gestartete Prozesse wird mit dem Parameter **CheckFileLimit** der Konfigurationsdatei definiert und bestimmt die Anzahl der gleichzeitig zu bearbeitenden Dateien. Deswegen ist die Anzahl 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:

```
$kav4fs-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.

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: Die Antiviren-Datenbanken werden stündlich aktualisiert, die Anti-Spam-Dateien 12 bis 24 Mal pro Tag. Zudem steht allen Anwendern ein rund-um-die-Uhr-Support zur Verfügung: Telefonisch oder per E-Mail – in deutscher, englischer, russischer und französischer Sprache.

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 Betriebssystem Microsoft Windows gestartet werden, vorhanden.

Der Proaktive Schutz umfasst:

- **Kontrolle über Veränderungen im Dateisystem.** Das Programm erlaubt es, eine Liste der Anwendungen anzulegen, deren Komponentenbestand kontrolliert werden soll. Dadurch lässt sich die Verletzung der Integrität von Anwendungen durch Schadprogramme verhindern.
- **Überwachung von Prozessen im Arbeitsspeicher.** Kaspersky Anti-Virus 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 Webbrowser 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 Antiviren-Datenbanken für die Untersuchung wählen.
- 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[®] 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 HotSync[™] und während des Datenaustausches mit anderen PDA Virenprogramme blockiert.

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

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® Corporate Suite

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

Kaspersky® Corporate Suite bietet Rundumschutz² vor Viren für:

- *Computerarbeitsplätze* unter Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstation und Linux.

¹ Je nach Lieferumfang

² Je nach Lieferumfang

- *Dateiserver* unter Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD, Linux und Samba Servers.
- *Mailsysteme* vom Typ Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim und Qmail.
- *Internet-Firewalls*: Microsoft ISA Server 2004 Enterprise Edition.
- Handheld-PCs, die unter Microsoft Windows CE und Palm OS arbeiten, sowie Smartphones, die unter Microsoft Windows Mobile 2003 for Smartphone und Microsoft Smartphone 2002 arbeiten.

Kaspersky® Corporate Suite 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 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 Security® for Microsoft Exchange 2003

Kaspersky Security® for Microsoft Exchange bietet die Antivirenuntersuchung der eingehenden, ausgehenden und auf dem Server gespeicherten E-Mail-Nachrichten einschließlich der Nachrichten in gemeinsamen Ordnern. Außerdem führt er die Filterung unerwünschter Korrespondenz aus, wobei intelligente Technologien zur Spam-Erkennung in Verbindung mit den Technologien der Firma Microsoft verwendet werden. Die Anwendung untersucht alle mit dem SMTP-Protokoll auf dem Exchange-Server eingehenden Nachrichten auf Viren, wobei Antivirentechnologien von Kaspersky Lab verwendet werden, und auf Spam-Merkmale, wozu die Filterung nach formalen Kennzeichen (E-Mail-Adresse, IP-Adresse, Größe der Mail, Kopfzeile) dient. Außerdem analysiert er den Inhalt der Mails und seiner Anhänge mit Hilfe von intelligenten Technologien, wie eindeutige grafische Signaturen zum Erkennen von Spam in grafischer Form. Der Untersuchung werden sowohl der Nachrichtenkörper als auch angehängte Dateien unterzogen.

Kaspersky® Mail Gateway

Kaspersky® Mail Gateway ist eine universelle Lösung für den komplexen Schutz der Benutzer von Mailsystemen. Die Anwendung wird zwischen dem Unternehmensnetzwerk und dem Internet installiert und führt die Untersuchung aller Elemente einer E-Mail auf Viren und andere schädliche Programme (Spyware, Adware usw.) durch. Außerdem erfolgt die zentralisierte Filterung des E-Mail-Nachrichtenstroms auf Spam-Merkmale. Die Lösung enthält ferner eine Reihe zusätzlicher Optionen für die Filterung des E-Mail-Stroms.

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 Labs 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 In-formationen	WWW: http://www.kaspersky.de http://www.viruslist.de/
Feedback zu unseren nutzerhand-büchern	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 vorgesehene 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, INDIRECTEN, 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 HAFTUNGS AUSSCHLUSS 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