

KASPERSKY LAB

Kaspersky Anti-Virus[®] 5.5
for Samba Servers

Handbuch
FÜR
ADMINISTRATOREN

KASPERSKY ANTI-VIRUS® 5.5 FOR SAMBA SERVERS

Handbuch für Administratoren

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

Redaktionsdatum: November 2006

Inhalt

KAPITEL 1. VORWORT	6
1.1. Computerviren und schädliche Programme.....	7
1.2. Grundfunktionen von Kaspersky Anti-Virus	8
1.3. Hardware- und Softwarevoraussetzungen für das System.....	9
1.4. Lieferumfang.....	11
1.5. Service für registrierte Benutzer.....	12
1.6. Textgestaltung.....	12
KAPITEL 2. INTERNE ARCHITEKTUR VON KASPERSKY ANTI-VIRUS	14
2.1. Komponenten	14
2.2. Funktionsalgorithmus	14
KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-VIRUS.....	16
3.1. Installation der Anwendung auf einem Server mit Linux.....	16
3.2. Installation der Anwendung auf einem Server mit FreeBSD	16
3.3. Installationsprozess	17
3.4. Konfiguration der Anwendung	18
3.5. Anordnungsschema der Dateien nach Verzeichnissen.....	19
3.6. Versionsupdate des Samba-Servers.....	21
3.7. Deinstallation von Kaspersky Anti-Virus.....	22
KAPITEL 4. KONFIGURATION NACH DER INSTALLATION.....	24
4.1. Standardeinstellungen der Anwendung	24
4.2. Installation der Antiviren-Datenbanken.....	25
4.3. Konfiguration der Zusammenarbeit mit Webmin.....	25
4.4. Empfohlene Funktionsmodi	26
4.4.1. Optimaler Funktionsmodus	26
4.4.2. Modus für maximales Arbeitstempo	28
4.4.3. Modus für maximale Sicherheit.....	28
4.4.4. Untersuchungsmodus für häufig aktualisierte Dateien.....	29
KAPITEL 5. ARBEIT MIT KASPERSKY ANTI-VIRUS FOR SAMBA SERVERS	32
5.1. Aktualisierung der Antiviren-Datenbanken	32

5.1.1. Automatisches Update der Antiviren-Datenbanken	34
5.1.2. Update der Antiviren-Datenbanken auf Befehl.....	35
5.1.3. Erstellen eines Netzwerkordners zum Speichern und Kopieren der Antiviren-Datenbanken	36
5.2. Antivirenschutz des Samba-Servers im Echtzeitmodus	37
5.2.1. Konfiguration der Benutzerbenachrichtigung	38
5.2.1.1. Monitoring mit Benachrichtigung durch smbclient	38
5.2.1.2. Monitoring mit Benachrichtigung durch E-Mails	39
5.3. Antivirenschutz für Dateisysteme.....	40
5.3.1. Dateiuntersuchung auf Befehl.....	40
5.3.2. Untersuchung eines Ordners nach Zeitplan (cron)	41
5.3.3. Zusätzliche Optionen: Verwendung von Skriptdateien	42
5.3.3.1. Senden einer Benachrichtigung an den Administrator.....	42
KAPITEL 6. ZUSÄTZLICHE EINSTELLUNGEN.....	43
6.1. Konfiguration des Echtzeit-Antivirenschutzes	43
6.1.1. Untersuchungsbereich	43
6.1.2. Modus zur Untersuchung und Desinfektion von Dateien.....	44
6.1.3. Aktionen für Dateien	45
6.1.4. Infizierte Objekte isolieren	46
6.1.5. Modus zum Erstellen von Sicherungskopien von Objekten	47
6.2. Konfiguration des Antivirenschutzes für Dateisysteme.....	47
6.2.1. Untersuchungsbereich	48
6.2.2. Modus zur Untersuchung und Desinfektion von Dateien.....	49
6.2.3. Aktionen für Dateien	50
6.2.4. Modus zum Erstellen von Sicherungskopien	51
6.3. Optimierung der Arbeit von Kaspersky Anti-Virus for Samba Servers.....	51
6.4. Neustart von Kaspersky Anti-Virus	54
6.5. Lokalisierung des Formats für Datums- und Uhrzeitanzeige.....	55
6.6. Parameter für die Berichtsführung von Kaspersky Anti-Virus	56
KAPITEL 7. VERWALTUNG VON LIZENZSCHLÜSSELN.....	58
7.1.1. Informationen zum Lizenzschlüssel anzeigen.....	59
7.1.2. Lizenz verlängern	60
7.1.3. Lizenzschlüssel löschen.....	61
KAPITEL 8. TESTEN DER KORREKTEN FUNKTION VON KASPERSKY ANTI- VIRUS.....	62

KAPITEL 9. MÖGLICHE FRAGEN BEI DER ARBEIT MIT DER ANWENDUNG.....	64
ANHANG A. ZUSÄTZLICHE ANGABEN ZU DER ANWENDUNG	69
A.1. Konfigurationsdatei von Kaspersky Anti-Virus	69
A.2. Befehlszeilenschlüssel der Komponente kavsamba	79
A.3. Rückgabewerte der Komponente kavsamba	79
A.4. Befehlszeilenschlüssel der Komponente kavscanner	80
A.5. Rückgabewerte der Komponente kavscanner	83
A.6. Befehlszeilenschlüssel der Komponente licensemanager	84
A.7. Rückgabewerte der Komponente licensemanager	85
A.8. Befehlszeilenschlüssel der Komponente keepup2date.....	85
A.9. Rückgabewerte der Komponente keepup2date.....	87
ANHANG B. KASPERSKY LAB.....	88
B.1. Andere Produkte von Kaspersky Lab	89
B.2. Kontaktinformationen	99
ANHANG C. ENDBENUTZER-LIZENZVERTRAG.....	100

KAPITEL 1. VORWORT

Mit der steigenden Zahl der Computeranwender und den wachsenden Möglichkeiten zum gegenseitigen Datenaustausch per E-Mail und über das Internet ist auch die Bedrohung einer Computerinfektion durch Viren sowie der Zerstörung und des Diebstahls von Informationen durch schädliche Programme gewachsen.

Die gefährlichsten Quellen für das Eindringen schädlicher Programme sind:

Internet

Das globale Informationsnetzwerk ist die Hauptquelle für die Verbreitung einer beliebigen Art von schädlichen Programmen. Viren und andere Schadprogramme können auf populären Webseiten im Internet platziert und als nützliche und kostenlose Software " maskiert " sein. Außerdem können viele Skripts, die beim Öffnen von Webseiten automatisch gestartet werden, schädliche Programme enthalten.

E-Mail-Korrespondenz

E-Mail-Nachrichten, die in der Mailbox des Benutzers eintreffen und in Maildatenbanken gespeichert werden, können Viren enthalten. Schädliche Programme können sich sowohl im Anhang als auch im Körper einer Nachricht befinden. Infizierte E-Mails enthalten in der Regel Viren oder Netzwerkwürmer. Die Daten auf Ihrem Computer können beim Öffnen einer Nachricht oder beim Speichern einer angehängten Datei auf der Festplatte infiziert werden.

Softwareschwachstellen

Die Hauptquelle für Hackerangriffe sind "Lücken" in der Software. Solche Schwachstellen erlauben einem Hacker den entfernten Zugriff auf Ihren Computer und damit auf Ihre Daten, die Ihnen zugänglichen Netzwerkressourcen und andere Informationsquellen.

In der Umgebung von Unix-Systemen sind Viren wesentlich geringer verbreitet als beispielsweise in der Windows-Umgebung. Die Ursache liegt in Besonderheiten dieser Plattformen. Das bedeutet aber nicht, dass für Benutzer von Unix-Betriebssystemen keine Gefahr im Hinblick auf die Informationssicherheit besteht. Im Folgenden betrachten wir die einzelnen Typen der Schadprogramme genauer.

1.1. Computerviren und schädliche Programme

Um zu beurteilen, welche Gefahrenart Ihre Daten bedrohen kann, ist es hilfreich, die Typen und Funktionsweise schädlicher Programme zu kennen. Schädliche Programme lassen sich generell in folgende Klassen unterteilen:

Würmer (Worms) – Diese Kategorie der schädlichen Programme benutzt Netzwerkressourcen, um sich auszubreiten. Die Klasse erhielt ihren Namen aufgrund ihrer wurmähnlichen Fähigkeit, von einem Computer auf einen anderen zu "kriechen", wobei Netzwerke, E-Mails und andere Informationskanäle benutzt werden. Deshalb besitzen Würmer eine überaus hohe Ausbreitungsgeschwindigkeit.

Würmer dringen in einen Computer ein, ermitteln die Netzwerkadressen anderer Computer und versenden ihre Kopien an diese Adressen. Neben Netzwerkadressen verwenden Würmer häufig auch Daten aus dem Adressbuch von Mailprogrammen. Vertreter dieser Klasse von Schadprogrammen erstellen teilweise Arbeitsdateien auf Systemlaufwerken, können aber auch völlig ohne Zugriff auf Computerressourcen (unter Ausnahme des Arbeitsspeichers) auskommen.

- **Viren (Viruses)** sind Programme, die andere Programme infizieren, indem sie ihnen den eigenen Code hinzufügen, um beim Start infizierter Dateien die Kontrolle zu übernehmen. Diese einfache Definition nennt die wichtigste Aktion, die von einem Virus ausgeführt wird: die Infektion. Die Ausbreitungsgeschwindigkeit von Viren ist etwas geringer als bei Würmern.
- **Trojanische Programme (Trojans)** – Programme, die auf infizierten Computern vom Benutzer nicht erlaubte Aktionen ausführen, d.h. abhängig von bestimmten Bedingungen Informationen auf Laufwerken vernichten, das System zum "Hängenbleiben" bringen, vertrauliche Informationen stehlen usw. Diese Klasse der schädlichen Programme fällt nicht unter die traditionelle Definition eines Virus (d.h. infiziert keine anderen Programme oder Daten). Trojanische Programme können nicht selbständig in einen Computer eindringen und werden von Angreifern als "nützliche" Software getarnt verbreitet. Dabei kann der von ihnen verursachte Schaden den eines traditionellen Virusangriffs erheblich übersteigen.

In letzter Zeit sind *Würmer* und *Trojanische Programme* zu den häufigsten Typen der Schadprogramme in der Umgebung von Unix-Systemen geworden.



Zur Bezeichnung von Viren, Trojanischen Programmen und Würmern wird im weiteren Text dieses Handbuchs der Begriff "Virus" verwendet. Die konkrete Art eines schädlichen Programms wird nur bei Bedarf genannt.

1.2. Grundfunktionen von Kaspersky Anti-Virus

Die Anwendung **Kaspersky Anti-Virus® 5.5 for Samba Servers** (im Folgenden auch **Kaspersky Anti-Virus** genannt) gewährleistet die Antivirenuntersuchung auf Samba-Servern, die mit dem Betriebssystem Linux und FreeBSD arbeiten.

Die Anwendung bietet die Untersuchung des Serverdateisystems auf zwei Ebenen: in Echtzeit und auf Befehl. Beim Fund schädlicher Programme erlaubt Kaspersky Anti-Virus die effektive Desinfektion oder das Sperren infizierter Objekte, um die weitere Ausbreitung einer Epidemie zu verhindern und den Systemadministrator umgehend über den Vorfall zu informieren.



Die Anwendung verwendet außerdem die intellektuelle Technologie iChecker™, die eine wesentliche Beschleunigung der Dateiuntersuchung erlaubt.

Kaspersky Anti-Virus for Samba Servers ist ein Paket von Antivirenkomponenten, die folgende Funktionen erfüllen:

- *Echtzeitschutz* des Samba-Dateiservers vor schädlichem Code (**On-Access Scanner**).
- *Suche und Desinfektion* von schädlichem Code im Serverdateisystem *auf Befehl* (**On-Demand Scanner**).
- *Benachrichtigung des Administrators* über den Fund infizierter oder verdächtiger Objekte.
- *Gewährleistung des aktuellen Zustands der Antiviren-Datenbanken* (**keepup2date**).
- *Lokale und entfernte Verwaltung* mit Hilfe des Moduls zur Web-Administration (**Webmin**).

Außerdem bietet Kaspersky Anti-Virus seinen Benutzern folgende Zusatzfunktionen:

- Möglichkeit zur Verwendung von benutzerdefinierten Skripts beim Eintritt eines Ereignisses vom Typ "infizierte Datei gefunden".

- Möglichkeit zum Verschieben infizierter (oder verdächtiger) Objekte in ein spezielles Verzeichnis (Quarantäne).
- Speichern des Originals eines infizierten Objekts (im Backup) vor der Desinfektion mit der Möglichkeit seiner Wiederherstellung im Fall des Eintritts unvorhersehbarer Ereignisse.
- Speichern von Daten über bereits untersuchte Dateien in einem temporären Cache. Dadurch wird bei nachfolgenden Zugriffen auf eine Datei eine wesentliche Verringerung der erforderlichen Untersuchungszeit erreicht (Die Daten bleiben bis zum Neustart der Anwendung im Cache gespeichert).
- Möglichkeit zur Begrenzung der maximalen Anzahl von im Echtzeitmodus gleichzeitig zu scannenden Dateien, wobei überzählige zur Untersuchung anstehende Dateien in eine Warteschlange eingereiht werden.
- Möglichkeit zum automatischen Anhalten der Antivirenuntersuchung von Dateien im Hintergrundmodus, wenn ein benutzerdefinierter Wert für die Belastungsgrenze auf dem Server überschritten wird, und zur Wiederaufnahme der Arbeit, wenn die Belastung auf das zulässige Niveau sinkt.
- Möglichkeit der Definition einer beliebigen Kombination der Modi "Untersuchung beim Öffnen" und "Untersuchung beim Speichern" für jeden gemeinsamen Ordner.
- Möglichkeit zum Vornehmen individueller Einstellungen für den Antivirenschutz für jeden separaten gemeinsamen Ordner.
- Bei der Aktualisierung der Antiviren-Datenbanken wird der Kaspersky-Lab-Updateserver mit der geringsten Belastung ermittelt. Außerdem nimmt der Updateprozess nach einem Verbindungsabbruch seine Arbeit nach der Verbindungswiederherstellung an der Stelle des Abbruchs wieder auf.
- Möglichkeit zum Rückgängigmachen von Updates der Antiviren-Datenbanken und Updates der Anwendung.

1.3. Hardware- und Softwarevoraussetzungen für das System

Für die Arbeit von **Kaspersky Anti-Virus for Samba Servers** sind erforderlich:

- Prozessor Intel Pentium® 133 MHz oder höher.
- 64 MB Arbeitsspeicher.
- 100 MB verfügbarer Festplattenspeicher zur Installation der Anwendung und zum Speichern von temporären Dateien.
- Softwarevoraussetzungen:
 - Für eine 32-Bit-Plattform eines der folgenden Betriebssysteme:
 - RedHat Linux 9.0.
 - RedHat Enterprise Linux Advanced Server 4 UPD3.
 - SUSE Linux Enterprise Server 9.0 SP3.
 - 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.
 - Für eine 64-Bit-Plattform eines der folgenden Betriebssysteme:
 - RedHat Enterprise Linux Advanced Server 4 UPD3.
 - RedHat Fedora Core 5.
 - SUSE Linux Professional 10.1.
 - SUSE Linux Enterprise Server 9 SP3.
 - Programm Webmin (www.webmin.com) – zur Remote-Verwaltung von Kaspersky Anti-Virus.
 - Perl-Interpreter Version 5.0 oder höher (www.perl.org).
 - Installiertes Dienstprogramm which.
 - Installierter Samba-Server Version 2.2.7 und höher oder Version von 3.0.0 bis 3.0.23c.



Beachten Sie, dass Kaspersky Anti-Virus die Zusammenarbeit mit SELinux nicht unterstützt. Die Verwendung SELinux kann zur Anzeige unterschiedlicher Warnungen im Systembericht der Anwendung führen.

Wenn auf Ihrem Server ein Schutz mit Hilfe von Listen zur Zugriffskontrolle auf das Dateisystem installiert ist (File System Access Control Lists, ACLs), müssen Sie den Samba Server anpassen damit diese Funktion unterstützt wird.

1.4. Lieferumfang

Kaspersky Anti-Virus kann bei unseren Vertriebspartnern oder in einem Online-Shop (z.B. www.kaspersky.com/de, Abschnitt **E-STORE**) erworben werden.

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

- Versiegelter Umschlag mit Installations-CD, auf der die Dateien des Softwareprodukts enthalten sind.
- Benutzerhandbuch.
- Lizenzschlüssel, der auf einer speziellen Diskette gespeichert ist.
- Registrierungskarte (mit Seriennummer des Produkts).
- Lizenzvertrag.



Bitte lesen Sie vor dem Öffnen des versiegelten Umschlags mit der Installations-CD (oder mit den Disketten) sorgfältig den Lizenzvertrag

Beim Erwerb von Kaspersky Anti-Virus in einem Online-Shop kopieren Sie das Produkt von der Kaspersky-Lab-Internetseite. Die Distribution enthält neben dem eigentlichen Produkt auch das vorliegende Handbuch. Ein Lizenzschlüssel wird Ihnen nach Eingang der Bezahlung per E-Mail zugesandt.

Lizenzvertrag

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

Bitte lesen Sie den Lizenzvertrag sorgfältig!

Wenn Sie den Bedingungen des Lizenzvertrags nicht zustimmen, können Sie die Packung mit dem Produkt an den Händler zurückgeben, bei dem Sie diese erworben haben, und der Kaufbetrag des Produkts wird Ihnen erstattet.

Voraussetzung dafür ist, dass der versiegelte Umschlag mit der Installations-CD (oder den Disketten) nicht geöffnet wurde.

Durch das Öffnen der versiegelten Packung mit der Installations-CD (oder den Disketten) stimmen Sie allen Bedingungen des Lizenzvertrags zu.

1.5. Service für registrierte Benutzer

Kaspersky Lab Ltd. bietet seinen registrierten Kunden ein breites Spektrum an Serviceleistungen, die eine gesteigerte Effektivität von Kaspersky Anti-Virus ermöglichen.

Durch den Erwerb einer Lizenz werden Sie zum registrierten Programmbenutzer und können während der Gültigkeitsdauer der Lizenz folgende Serviceleistungen in Anspruch nehmen:



- Nutzung neuer Versionen des betreffenden Softwareprodukts;
- Beratung bei Fragen zu Installation, Konfiguration und Benutzung des Softwareprodukts (per Telefon und E-Mail);
- Nachrichten über das Erscheinen neuer Softwareprodukte von Kaspersky Lab und über das Auftauchen neuer Viren (Dieser Service gilt für Benutzer, die den Newsletter von Kaspersky Lab Ltd. abonniert haben).






Die Beratung erstreckt sich nicht auf Fragen über Funktion und Benutzung von Betriebssystemen und anderen Technologien.

1.6. 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.

Formatierung	Bedeutung
 <p><i>Um diese Aktion durchzuführen,</i></p> <ol style="list-style-type: none"> 1. Schritt 1. 2. ... 	Beschreibung einer Folge von Schritten und möglichen Aktionen, die vom Benutzer durchgeführt werden.
 <p>Aufgabe, Beispiel</p>	Aufgabenstellung, Beispiel für die Realisierung der Optionen des Softwareprodukts
 <p>Lösung</p>	Lösung der vorhergehenden Aufgabe
<p>[Parameter] – Funktion des Parameters.</p>	Befehlszeilenparameter.
<p>Text von Meldungen und Befehlszeilen</p>	Text von Konfigurationsdateien, Informationsmeldungen des Programms und Befehlszeilen.

KAPITEL 2. INTERNE ARCHITEKTUR VON KASPERSKY ANTI-VIRUS

Vor der Erklärung der funktionellen Möglichkeiten von Kaspersky Anti-Virus for Samba Servers werfen wir einen ausführlichen Blick auf seine interne Architektur. Dadurch wird ein besseres Verständnis des Funktionsalgorithmus von Anti-Virus ermöglicht

2.1. Komponenten

Kaspersky Anti-Virus for Samba Servers besteht aus folgenden Komponenten:

- *kavsamba (On-Access-Scanner)*
- *kavscanner (On-Demand-Scanner)*
- *keepup2date*

Die Komponente *kavsamba* umfasst die Module *kavsamba.so* und *kavsamba*. Das Modul *kavsamba.so* besitzt die Form einer dynamischen Bibliothek, die in den Samba-Server integriert wird und dem Abfangen von Dateiaufrufen über den Samba-Server dient. Das Modul *kavsamba* ist ein Prozess-Daemon, der die von *kavsamba.so* übergebenen Dateien analysiert und entsprechend der aktuellen Einstellungen bearbeitet. Der Datenaustausch zwischen Modul und Prozess-Daemon erfolgt über ein lokales Socket (Unix Domain sockets).

Die Komponente *kavscanner* dient dem Antivirenschutz von Dateisystemen. Die Untersuchung von Serverdateisystemen oder von Dateien bestimmter Verzeichnisse erfolgt nach Aufforderung durch den Administrator oder nach Zeitplan (abhängig von den gewählten Einstellungen).

Die Komponente *keepup2date* aktualisiert die Antiviren-Datenbanken, die zur Suche und Desinfektion von Viren verwendet werden, und lädt außerdem Programmpatches für die Anwendung.

2.2. Funktionsalgorithmus

In diesem Abschnitt betrachten wir die interne Architektur der Anwendung im Kontext des Echtzeit-Antivirenschutzes. Der Prozess zur Untersuchung auf Befehl ist relativ einfach und bedarf keiner separaten Erklärung.

Der Funktionsalgorithmus lässt sich folgendermaßen beschreiben:

1. Versucht ein Benutzer über den Samba-Server auf eine beliebige Datei zuzugreifen, dann wird der Aufruf vom Server abgefangen und an das Modul *kavsamba.so* weitergegeben.
2. Das Modul *kavsamba.so* sendet Daten über den Aufruf (Dateiname, vollständiger Pfad der Datei, Identifikationsnummer (ID) des Benutzers, der die Datei aufgerufen hat, Domänenname des Computers) über IPC nach binärem Protokoll an das Modul *kavsamba*.
3. Das Modul *kavsamba* führt übereinstimmend mit den Einstellungen der Konfigurationsdatei die Virusuntersuchung und –bearbeitung des aufgerufenen Objekts durch (dazu zählt auch die Desinfektion mit Hilfe der Antiviren-Datenbanken, wenn diese Option aktiviert wurde).
4. Nach Abschluss der Untersuchung und der Aktionen mit der Datei erhält *kavsamba.so* von *kavsamba* einen Zugriffscode (erlaubt/verboten), der den Status der Datei festlegt.
5. Abhängig vom Status des Objekts erteilt *kavsamba.so* dem Samba-Server die Zugriffserlaubnis für das Objekt oder blockiert es.

Der Zugriff auf eine Datei wird blockiert, wenn sie infiziert oder verdächtig ist (Infected, CureFailed, Warning, Suspicion). In allen anderen Fällen wird der Zugriff auf die Datei erlaubt.

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. 1.3 auf S. 9).
- Melden Sie sich als Benutzer **root** am System an.

3.1. Installation der Anwendung auf einem Server mit Linux

Kaspersky Anti-Virus für Computer mit Linux-Betriebssystem wird in zwei Formaten geliefert.

- **.rpm** – für Systeme, die RPM Package Manager unterstützen
- **.deb** – für Debian-Distributionen.



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

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



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

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

3.2. Installation der Anwendung auf einem Server mit FreeBSD

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 einem pkg-Paket geben Sie in der Befehlszeile ein:

```
pkg_add <Paketname>
```

3.3. Installationsprozess



Aus einer Reihe von Gründen kann beim Abschluss des Installationsprozesses ein Fehlercode erscheinen. Vergewissern Sie sich in diesem Fall, dass Ihr Computer den Hardware- und Softwarevoraussetzungen entspricht (s. Pkt. 1.3 auf S. 9) und dass Sie mit den Rechten des Benutzers root am System angemeldet sind.

Die Installation der Anwendung auf dem Server umfasst mehrere Etappen:

1. Kopieren der Distributionsdateien auf den Server;
2. Konfiguration der Komponente *keepup2date*;
3. Installation (Update) der Antiviren-Datenbanken;



Vergessen Sie nicht, die Antiviren-Datenbanken zu installieren, bevor Sie beginnen, die Anwendung zu verwenden. Die Prozedur zur Suche und Desinfektion von Viren basiert auf den Einträgen der Antiviren-Datenbanken, die eine Beschreibung aller momentan bekannten Viren und Methoden zur Desinfektion infizierter Objekte enthalten. Ohne die Antiviren-Datenbanken ist die Untersuchung und Bearbeitung von Dateien nicht möglich!

Beachten Sie außerdem, dass die automatische Konfiguration der Anwendung nicht ausgeführt wird, wenn die Antiviren-Datenbanken nicht installiert wurden.

4. Installation des Lizenzschlüssels.

Wenn kein Lizenzschlüssel installiert wird, dann wird der Konfigurationsprozess nicht ausgeführt und die Arbeit mit der Anwendung ist nicht möglich. Bei vorübergehendem Fehlen des Schlüssels (z.B. wenn die Anwendung über das Internet erworben wurde und der Lizenzschlüssel noch nicht per E-Mail eingetroffen ist) besteht die Möglichkeit, den Schlüssel nicht während des Installationsprozesses, sondern später, unmittelbar bevor die Anwendung verwendet wird, zu installieren.

5. Installation des Webmin-Moduls.

Das Modul zur Remote-Administration für Webmin wird nur unter der Bedingung installiert, dass Webmin sich am Standardpfad befindet.

Nach der Installation des Moduls folgen entsprechende Empfehlungen für die Konfiguration der Zusammenarbeit mit der Anwendung.

3.4. Konfiguration der Anwendung

Gleich nachdem die Distributionsdateien auf den Server kopiert worden sind, wird die Konfiguration des Systems ausgeführt. Abhängig vom Paket-Manager wird die Konfigurationsetappe entweder automatisch gestartet oder erfordert einige zusätzliche Aktionen des Benutzers (wenn der Paket-Manager die Verwendung interaktiver Skripts nicht zulässt, wie z.B. rpm). In diesem Fall werden entsprechende Meldungen auf dem Bildschirm angezeigt.

Der Konfigurationsprozess der Anwendung umfasst:

- Suche eines installierten Samba-Servers und Überprüfung seiner Version auf Übereinstimmung mit den Softwarevoraussetzungen.
- Suche und Änderung der Konfigurationsdatei des Samba-Servers.
- Überprüfung der Konfigurationsdatei des Samba-Servers auf das Vorhandensein von VFS-Objekten. Wenn die Konfigurationsdatei des Samba-Servers bereits Zeilen mit zu verwendenden VFS-Objekten enthält, erfolgt die Auskommentierung dieser Zeilen.



Wenn Sie das Betriebssystem FreeBSD und Samba-Server Version von 3.0 bis 3.0.9 verwenden, besteht aufgrund von Besonderheiten des Betriebssystems die Wahrscheinlichkeit, dass bei der Arbeit mit VFS-Modulen Fehler auftreten.

Um die korrekte Funktion der Anwendung mit VFS-Objekten zu gewährleisten, wird empfohlen, die Version des Samba-Servers zu aktualisieren oder ein Patch für den Samba-Server zu installieren (Details über den Patch s.

https://bugzilla.samba.org/show_bug.cgi?id=2100).

Wenn bei der Konfiguration des Systems bestimmte Zusatzangaben (z.B. Pfad der Konfigurationsdatei des Samba-Servers) erforderlich sind, werden auf der Serverkonsole entsprechende Anfragen angezeigt. Werden inkorrekte Antworten eingegeben, dann wird der Konfigurationsprozess abgebrochen.

Wenn alle oben beschriebenen Konfigurationsschritte erfolgreich abgeschlossen wurden, ist die Anwendung zur Arbeit bereit und es erfolgt keine zusätzliche Meldung. Die Konfigurationsdatei, die zum Lieferumfang der Anwendung gehört, enthält alle Einstellungen, die für den Beginn der Arbeit erforderlich sind.



Vergessen Sie nicht, vor dem Beginn der Arbeit den Neustart des Samba-Servers vorzunehmen.

3.5. Anordnungsschema der Dateien nach Verzeichnissen

Unter der Bedingung, dass alle während der Installation standardmäßig vorgeschlagenen Pfade übernommen wurden, sind die Dateien der Distribution nach der Installation von Kaspersky Anti-Virus folgendermaßen angeordnet:

Wenn Sie das Betriebssystem Linux installiert haben:

/etc/opt/kaspersky/ – Dieses Verzeichnis enthält die Konfigurationsdatei von Kaspersky Anti-Virus und andere Konfigurationsdateien:

kav4samba.conf – Konfigurationsdatei.

/var/opt/kaspersky/kav4samba/bases und */var/opt/kaspersky/kav4samba/licenses* – Diese Verzeichnisse enthalten die Antiviren-Datenbanken und Lizenzschlüssel.

/opt/kaspersky/kav4samba – Das Hauptverzeichnis von Anti-Virus, das folgende Elemente enthält:

/bin/ – Verzeichnis der ausführbaren Dateien aller Komponenten von Kaspersky Anti-Virus for Samba Servers:

kav4samba-kavscanner – ausführbare Datei der Komponente für den Antivirenschutz von Dateiservern kavscanner (On-Demand Scanner).

kav4samba-licensemanager – ausführbare Datei der Komponente für die Arbeit mit Lizenzschlüssel licensemanager.

kav4samba-keepup2date – ausführbare Datei der Komponente keepup2date, die dem Update der Antiviren-Datenbanken dient.

/sbin/kav4samba-kavsamba – ausführbare Datei der Komponente für den Antivirenschutz im Echtzeitmodus kavsamba (On-Access Scanner).

/lib/bin/setup/kavsamba_setup.pl – Skript, das die Integration mit dem Samba-Server ausführt.

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



Um das Hilfesystem von Kaspersky Anti-Virus (manual pages) einzubinden, fügen Sie der Umgebungsvariablen **MANPATH** den Wert ***/opt/kaspersky/kav4samba/share/man*** hinzu.

/opt/kaspersky/kav4samba/lib/ – Verzeichnis mit Samba-Modulen für 32-Bit-Betriebssysteme.

/opt/kaspersky/kav4samba/lib64/ – Verzeichnis mit Samba-Modulen für 64-Bit-Betriebssysteme.

/opt/kaspersky/kav4samba/share/contrib/kavsamba.wbm – Verzeichnis zum Speichern des Webmin-Moduls.

/opt/kaspersky/kav4samba/share/contrib/vox.sh – Skript zur Desinfektion von Archiven.

/opt/kaspersky/kav4samba/share/doc/ – Verzeichnis zum Speichern von Lizenzen und der Samba-Dokumentation.

/opt/kaspersky/kav4samba/src/ – Verzeichnis mit dem Quellcode des Moduls für Samba-Server.

/var/opt/kaspersky/kav4samba/bases/ – Verzeichnis zum Speichern der Antiviren-Datenbanken.

/var/opt/kaspersky/kav4samba/bases.backup/ – Verzeichnis mit Sicherungskopien der Antiviren-Datenbanken (falls die Rückkehr zur vorherige Version der Datenbanken erforderlich wird).

/var/log/kaspersky/ – Verzeichnis zum Speichern von Berichtsdateien (log-Dateien) über die Arbeit der Anwendungskomponenten.

Wenn Sie das Betriebssystem FreeBSD installiert haben:

/usr/local/etc/kaspersky/ – Dieses Verzeichnis enthält die Konfigurationsdatei von Kaspersky Anti-Virus und andere Konfigurationsdateien:

kav4samba.conf – Konfigurationsdatei.

kav4samba.conf.default – Konfigurationsdatei mit standardmäßigen Einstellungen.

/var/db/kaspersky/kav4samba/bases/ und
/var/db/kaspersky/kav4samba/licenses/ – Diese Verzeichnisse enthalten die Antiviren-Datenbanken und Lizenzschlüssel.

/usr/local/ – Systemverzeichnis, das zur Installation von Programmen durch den Administrator vorgesehen ist. Diesem Ordner fügt Kaspersky Anti-Virus die ausführbaren Dateien aller Komponenten hinzu:

kav4samba-kavscanner – ausführbare Datei der Komponente für den Antivirenschutz von Dateiservern kavscanner (On-Demand Scanner).

kav4samba-licensemanager – ausführbare Datei der Komponente für die Arbeit mit Lizenzschlüsseln licensemanager.

kav4samba-keepup2date – ausführbare Datei der Komponente keepup2date, die dem Update der Antiviren-Datenbanken dient.

/usr/local/sbin/kav4samba-kavsamba – ausführbare Datei der Komponente für den Antivirenschutz im Echtzeitmodus kavsamba (On-Access Scanner).

/usr/local/libexec/kaspersky/kav4samba/setup/kavsamba_setup.pl – Skript, das die Integration mit dem Samba-Server ausführt.

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

/usr/local/lib/kaspersky/kav4samba/ – Verzeichnis mit Samba-Modulen für 32-Bit-Betriebssysteme.

`/usr/local/share/kav4samba/contrib/kavsamba.wbm` – Verzeichnis zum Speichern des Webmin-Moduls.

`/usr/local/share/kav4samba/contrib/vox.sh` – Skript zur Desinfektion von Archiven.

`/usr/local/share/doc/kav4samba/` – Verzeichnis zum Speichern von Lizenzen und der Samba-Dokumentation.

`/usr/local/src/kav4samba/` – Verzeichnis mit dem Quellcode des Moduls für Samba-Server.

`/var/db/kaspersky/kav4samba/bases.backup/` – Verzeichnis mit Sicherungskopien der Antiviren-Datenbanken (falls die Rückkehr zur vorigen Version der Datenbanken erforderlich wird).

`/var/log/kaspersky/` – Verzeichnis zum Speichern von Berichtsdateien (log-Dateien) über die Arbeit der Anwendungskomponenten.



Bei den folgenden Beispielen wird davon ausgegangen, dass Kaspersky Anti-Virus auf einem Server mit Linux-Betriebssystem installiert ist.

3.6. Versionsupdate des Samba-Servers



Die Distribution von Kaspersky Anti-Virus enthält binäre vfs-Module für die unterstützten Samba-Versionen.

Wenn eine neue Version von Samba Servers installiert ist, die nicht von Kaspersky Anti-Virus unterstützt wird, kann das vfs-Modul der Anwendung manuell angepasst werden.

Gehen Sie dazu folgendermaßen vor:

Wenn Sie ein Linux-Betriebssystem installiert haben, geben Sie in der Befehlszeile ein:

```
cd /opt/kaspersky/kav4samba/src
./configure --with-sambasrc=<path_to_samba> && make
```

wobei `<path_to_samba>` – Pfad der Quellmodule des Samba-Servers.

Wenn Sie ein FreeBSD-Betriebssystem installiert haben, geben Sie in der Befehlszeile ein:

```
cd /usr/local/src/kav4samba
./configure --with-sambasrc=<path_to_samba> && make
```

wobei `<path_to_samba>` = Pfad der Quellmodule des Samba-Servers.

Der Unterordner **/lib** wird die aktualisierte Version des vfs-Moduls enthalten. Konfiguration und Installation dieses Moduls sind Aufgabe des Administrators.

3.7. Deinstallation von Kaspersky Anti-Virus

Die Deinstallationsprozedur von Kaspersky Anti-Virus for Samba Servers setzt voraus:

- das Vorhandensein der Rechte eines privilegierten Benutzers (**root** oder anderer Benutzer mit UID=0). Wenn Sie im Moment der Deinstallation nicht über diese Rechte verfügen, ist die Anmeldung beim System als Benutzer **root** erforderlich.
- das Beenden des Samba-Servers.



Der Deinstallationsprozess beendet die Arbeit des Samba-Servers nicht selbständig!

Der Prozess zur Deinstallation von Kaspersky Anti-Virus wird im automatischen Modus ausgeführt. Der Prozess wird in Abhängigkeit von der verwendeten Distribution auf unterschiedliche Art gestartet.



Wenn Sie bei der Installation das rpm-Paket von Kaspersky Anti-Virus for Samba Servers verwendet haben, geben Sie zum Start der Deinstallationsprozedur in der Befehlszeile ein:

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



Wenn Sie bei der Installation das deb-Paket von Kaspersky Anti-Virus for Samba Servers verwendet haben, geben Sie zum Start der Deinstallationsprozedur in der Befehlszeile ein:

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



In Verbindung mit Besonderheiten des Betriebssystems Debian GNU/Linux ist das automatische Löschen der Verwaltungsskripts von Kaspersky Anti-Virus nicht möglich. Das Skript **/opt/kaspersky/kav4samba/lib/bin/kav4samba** muss nach Abschluss der Deinstallation manuell vom Administrator gelöscht werden.



Wenn Sie bei der Installation das *pkg*-Paket von Kaspersky Anti-Virus for Samba Servers verwendet haben, geben Sie zum Start der Deinstallationsprozedur in der Befehlszeile ein:

```
pkg_delete <Paketname>
```

Bei erfolgreichem Abschluss der Deinstallationsprozedur erfolgen keine zusätzlichen Meldungen.



Wenn bei der Installation der Anwendung das **Webmin-Modul** zur Remote-Verwaltung installiert wurde, muss es manuell entfernt werden.

Gehen Sie dazu im Hauptfenster des Programms Webmin auf die Registerkarte **Webmin Modules**, wählen Sie in der Liste **Delete Modules** die Zeile **KAV for Samba Servers** und klicken Sie auf die Schaltfläche **Delete Selected Modules**.

KAPITEL 4.

KONFIGURATION NACH DER INSTALLATION

Während des Installationsprozesses wird eine Analyse des Systems durchgeführt, auf dem Kaspersky Anti-Virus installiert wird, und bestimmte Parameter für seine Konfiguration werden automatisch festgelegt. Für eine Reihe von Parametern der Konfigurationsdatei der Anwendung sind Standardwerte vordefiniert, um die Arbeit mit der Anwendung möglichst komfortabel zu gestalten (s. Pkt. 4.1 auf S. 24).



Es wird empfohlen, vor Beginn der Arbeit mit der Anwendung die Antiviren-Datenbanken zu installieren oder zu aktualisieren, falls dies nicht bereits während der Installation gemacht wurde!

Zusätzlich sollten Sie Kaspersky Anti-Virus für die Arbeit mit Webmin konfigurieren.

In diesem Kapitel beschreiben wir, welche Einstellungen für Kaspersky Anti-Virus als Standard gelten, und untersuchen die für die Arbeit mit der Anwendung erforderliche Konfiguration.

4.1. Standardeinstellungen der Anwendung

Alle Funktionsparameter von Kaspersky Anti-Virus werden in der standardmäßig verwendeten Konfigurationsdatei der Anwendung gespeichert.



Sie können eigene Konfigurationsdateien anlegen und diese sowohl beim Ausführen einer aktuellen Aufgabe wie auch als Standard-Konfigurationsdatei verwenden.

Betrachten wir genauer, welche Parameter in dieser Datei als Standard gelten. Ausgehend von den Angaben dieses Abschnitts können Sie feststellen, ob zur optimalen Anpassung an die Anforderungen Ihres Unternehmens eine zusätzliche Konfiguration von Kaspersky Anti-Virus erforderlich ist (s. Kapitel 6 auf S. 43).

Als Standard ist in den Einstellungen von Kaspersky Anti-Virus festgelegt, dass die Komponente zum Antivirenschutz im Echtzeitmodus (*kavsamba*) ihre Arbeit beim Start des Betriebssystems beginnt. Beim Start der Komponente zum Scan auf Befehl (*kavscanner*) erfolgt ohne zusätzliche Befehlszeilenparameter die

Antivirenuntersuchung der Verzeichnisse und Dateisysteme des Servers, wobei mit dem aktuellen Verzeichnis begonnen wird.

Beim Fund infizierter, verdächtiger oder beschädigter Dateien werden auf der Konsole und in der Berichtsdatei entsprechende Meldungen angezeigt.



Beachten Sie, dass **IN DER GRUNDEINSTELLUNG DIE DESINFZEKTION** von gefundenen infizierten Dateien **NICHT AUSGEFÜHRT WIRD!**

4.2. Installation der Antiviren-Datenbanken

Die Virensuche und die Desinfektion infizierter Objekte durch Kaspersky Anti-Virus basiert auf den Einträgen der Antiviren-Datenbanken. Die Antiviren-Datenbanken enthalten eine Beschreibung aller momentan bekannten Schadprogramme und Methoden zur Desinfektion infizierter Objekte. Deshalb ist es äußerst wichtig, den aktuellen Zustand der Antiviren-Datenbanken zu pflegen.



Jeden Tag tauchen neue Viren auf. Es wird empfohlen, die Antiviren-Datenbanken **sofort** nach der Installation der Anwendung zu aktualisieren, weil die im Lieferumfang der Distribution enthaltenen Datenbanken zum Zeitpunkt der Installation bereits veraltet sind.

Das Update der Datenbanken wird von Kaspersky Anti-Virus mit Hilfe der Komponente *keepup2date* vorgenommen. Um das Update zu starten, geben Sie in der Befehlszeile ein:

```
/Pfad/für/ kav4samba-keepup2date
```

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

4.3. Konfiguration der Zusammenarbeit mit Webmin

Wenn Sie beabsichtigen, Kaspersky Anti-Virus entfernt zu verwalten, dann ist die Konfiguration der Zusammenarbeit mit dem Webmin-Paket zu empfehlen.

Mit den Werkzeugen von Webmin können beispielsweise die Kontrolle der Zugriffsrechte auf das Programm und die Organisation des Systems der Benutzerkennwörter vorgenommen werden.

Standardmäßig werden alle Einstellungen von Anti-Virus, die entfernt mit Hilfe des Programms Webmin vorgenommen wurden, in der Konfigurationsdatei der Anwendung gespeichert, die standardmäßig verwendet wird.



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

1. Kopieren Sie die Daten aus der bestehenden Konfigurationsdatei in die neue Datei, die unter einem anderen Namen gespeichert werden muss. Korrigieren Sie danach Ihren Aufgaben entsprechend die neue (alternative) Konfigurationsdatei.
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 über die einzelnen Einstellungen des Programms Webmin finden Sie in der Dokumentation dieses Produkts. Bei Fragen zum Modul für die Remote-Administration der Anwendung steht Ihnen außerdem das Hilfesystem des Programms Webmin zur Verfügung.

Im Folgenden wird bei der Beschreibung von Einstellungen und Start beliebiger Aufgaben die Arbeit im entfernten Modus über das Programm Webmin **nicht erläutert!**

4.4. Empfohlene Funktionsmodi

In Abhängigkeit der Serverauslastung empfiehlt Kaspersky Lab verschiedene Varianten zur Konfiguration der optimalen Arbeit von Kaspersky Anti-Virus. Diese Varianten werden unten ausführlich beschrieben.

4.4.1. Optimaler Funktionsmodus

Bei der Verwendung dieses Modus wird eine optimale Balance zwischen Arbeitstempo des Servers und gewährleitetem Sicherheitsniveau erreicht.



Nehmen Sie zur Konfiguration des optimalen Funktionsmodus folgende Änderungen in der Konfigurationsdatei vor:

- Wählen Sie als Wert für die Größe des Dateicache ungefähr die entsprechende Anzahl der Dateien, die über den Samba-Server zugänglich sind. Bei der Berechnung kann davon ausgegangen werden, dass ein Eintrag über eine virusfreie Datei im Cache ungefähr 50 Byte umfasst (Abschnitt [**samba.options**] Parameter **FileCacheSize**).

- Geben Sie im Abschnitt **[path]** folgenden Parameterwert an:
`IcheckerDbFile=/var/opt/kaspersky/kav4samba/ichecker.db`
- Geben Sie im Abschnitt **[samba.options]** folgende Werte für die Parameter an:
`Packed=yes`
`Archives=yes`
`SelfExtArchives=yes`
`MailBases=yes`
`MailPlain=yes`
`Heuristic=yes`
`Cure=yes`
`Ichecker=yes`
`CheckFilesLimit=20`
`BgCheckFilesLimit=5`
`BgSheduleTime=10`
`HashType=md5`
- Geben Sie im Abschnitt **[samba.path]** folgende Werte für die Parameter an:
`BackupPath=/var/opt/kaspersky/kav4samba/infected`
`SambaConfigFile=/etc/samba/smb.conf`
- Geben Sie im Abschnitt **[samba.actions]** folgende Werte für die Parameter an:
`OnInfected= MovePath /tmp/infected`
`OnSuspicion=MovePath /tmp/suspicious`
`OnWarning=MovePath /tmp/warning`
- Geben Sie im Abschnitt **[samba.shares]** folgende Werte für die Parameter an:
`CheckOnOpen=yes`
`CheckOnClose=yes`



Stellen Sie außerdem sicher, dass in *kavscanner* die Verwendung der Technologie **iChecker** aktiviert ist (Abschnitt **[scanner.options]** Parameter **IChecker=yes**). Außerdem müssen die Komponenten *kavsamba* und *kavscanner* übereinstimmende Optionen für die Konfigurationsparameter **Packed**, **Archives**, **SelfExtArchives**, **MailBases**, **MailPlain**, **Heuristic** (Abschnitt **[scanner.options]** und **[samba.options]**) verwenden.

4.4.2. Modus für maximales Arbeitstempo

Dieser Modus ist daraufhin orientiert, die maximale Arbeitsgeschwindigkeit der Anwendung zu gewährleisten. In diesem Fall wird die Sicherheit des Antivirenschutzes geringfügig vermindert.

Es wird empfohlen, die Untersuchung von Archiven zu deaktivieren und keine Untersuchung beim Schließen von Dateien durchzuführen. Dementsprechend untersucht die Anwendung Archive nicht, die möglicherweise infiziert sind. Außerdem können infizierte Objekte auf dem Server abgelegt werden, die nur beim Öffnen untersucht werden (Lesezugriff durch die Benutzer).



Nehmen Sie zur Konfiguration dieses Modus folgende Änderungen in der Konfigurationsdatei vor:

- Geben Sie im Abschnitt **[samba.options]** folgende Parameterwerte an:

```
Ichecker=no  
FileCacheSize=15000  
CheckFilesLimit=0  
HashType=crc32
```

- Geben Sie im Abschnitt **[samba.shares]** folgende Parameterwerte an:

```
CheckOnOpen=yes  
CheckOnClose=no
```

4.4.3. Modus für maximale Sicherheit

Bei dieser Konfigurationsvariante wird die maximale Sicherheit des Serverschutzes erreicht, da Dateien beim Lesen und beim Schreiben untersucht werden. Allerdings wird die Arbeit der Anwendung geringfügig verlangsamt.



Nehmen Sie zur Konfiguration dieses Modus folgende Änderungen in der Konfigurationsdatei vor:

- Geben Sie im Abschnitt **[samba.options]** folgende Parameterwerte an:

```
Packed=yes
Archives=yes
SelfExtArchives=yes
MailBases=yes
MailPlain=yes
Heuristic=yes
Cure=yes
FileCacheSize=0
CheckFilesLimit=0
BgCheckFilesLimit=0
BgSheduleTime=0
HashType=md5
```

- Geben Sie im Abschnitt **[samba.path]** folgenden Parameterwert an:

```
BackupPath=/var/opt/kaspersky/kav4samba/infected
```

- Geben Sie im Abschnitt **[samba.actions]** folgende Parameterwerte an:

```
OnInfected=remove
OnSuspicion=remove
OnWarning=remove
```



Stellen Sie sicher, dass die Verwendung der Technologie **iChecker** nicht nur in den Optionen von *kavsamba* (Abschnitt **[samba.options]** Parameter **lchecker=yes**), sondern auch für *kavscanner* (Abschnitt **[scanner.options]** Parameter **lchecker=yes**) aktiviert ist.

Stellen Sie außerdem sicher, dass in *kavscanner* die Verwendung der Technologie **iChecker** aktiviert ist (Abschnitt **[scanner.options]** Parameter **lChecker=yes**). Außerdem müssen die Komponenten *kavsamba* und *kavscanner* übereinstimmende Optionen für die Konfigurationsparameter **Packed**, **Archives**, **SelfExtArchives**, **MailBases**, **MailPlain**, **Heuristic** (Abschnitte **[scanner.options]** und **[samba.options]**) verwenden.

4.4.4. Untersuchungsmodus für häufig aktualisierte Dateien

Dieser Modus wird zur Konfiguration des Antivirenschutzes für gemeinsame Ordner empfohlen, deren Dateien häufig aktualisiert werden.

Der Modus zur Untersuchung von häufig aktualisierten Dateien unterscheidet sich von einem **empfohlenen Modus** (s. Pkt. 4.4.1 auf S. 26) dadurch, dass die Dateien in bestimmten gemeinsamen Ordnern nach dem Schreiben nicht untersucht werden, um die Arbeitsgeschwindigkeit zu erhöhen (im unten beschriebenen Beispiel ist dies der Ordner *public*).

Es wird empfohlen, für solche Ordner die Untersuchung der darin enthaltenen Ordner beim Schließen zu deaktivieren. Der Ordnerinhalt wird dann entweder untersucht, wenn ein Benutzer darauf zugreift oder wenn die Untersuchung im Hintergrundmodus stattfindet.

Die allgemeinen Einstellungen für alle übrigen Ordner entsprechen dem **empfohlenen Modus**.



Nehmen Sie zur Konfiguration dieses Modus folgende Änderungen in der Konfigurationsdatei vor:

- Geben Sie im Abschnitt **[path]** folgenden Parameterwert an:

```
IcheckerDbFile=  
/var/opt/kaspersky/kav4samba/ichecker.db
```

- Geben Sie im Abschnitt **[samba.options]** folgende Parameterwerte an:

```
Packed=yes  
Archives=yes  
SelfExtArchives=yes  
MailBases=yes  
MailPlain=yes  
Heuristic=yes  
Cure=yes  
Ichecker=yes  
FileCacheSize=20000  
CheckFilesLimit=20  
BgCheckFilesLimit=5  
BgSheduleTime=10  
HashType=md5
```

- Geben Sie im Abschnitt **[samba.path]** folgende Parameterwerte an:

```
BackupPath=/var/opt/kaspersky/kav4samba/infected  
SambaConfigFile=/etc/samba/smb.conf
```

- Geben Sie im Abschnitt **[samba.actions]** folgende Parameterwerte an:

```
OnInfected=remove
OnSuspicion=remove
OnWarning=remove
```

- Geben Sie im Abschnitt **[samba.shares]** folgende Parameterwerte an:

```
CheckOnOpen=yes
CheckOnClose=yes
```

- Geben Sie im Abschnitt **[samba.shares:public]** folgende Parameterwerte an:

```
CheckOnOpen=yes
CheckOnClose=no
```

KAPITEL 5. ARBEIT MIT KASPERSKY ANTI-VIRUS FOR SAMBA SERVERS

Der Antivirenschutz wird sowohl im Echtzeitmodus als auch auf Befehl durchgeführt. Betrachten wir diese Möglichkeiten genauer.

Der *Echtzeitschutz* wird von der Komponente *kavsamba* realisiert, die Aufrufe zum Öffnen von Dateien über den Samba-Server abfängt und im Hintergrundmodus das Schließen von Dateien überwacht. Dateien werden auf das Vorhandensein von Viren analysiert und den Einstellungen entsprechend bearbeitet. Der Zugriff auf gefährliche Dateien wird blockiert.

Beim *Scan auf Befehl*, der mit Hilfe der Komponente *kavscanner* erfolgt, kann die Untersuchung beliebiger Dateien (darunter auch Mail-Datenbanken, Archivdateien usw.) vorgenommen werden. In Abhängigkeit von den Untersuchungsergebnissen wird auf infizierte Dateien die Aktion angewandt, die in den Einstellungen der Konfigurationsdatei festgelegt ist.

Ein weiterer für die Antivirensicherheit wichtiger Bestandteil ist das *Update der Antiviren-Datenbanken* mit Hilfe der Komponente *keepup2date*. Diese Komponente führt das Update der Antiviren-Datenbanken und der Programm-Module entweder lokal oder im Remote-Modus durch.



Beachten Sie, dass bei allen im Folgenden für die Komponente *kavsamba* angeführten Beispielen nach Änderungen in der Konfigurationsdatei der Neustart von Kaspersky Anti-Virus erforderlich ist. Details zum Ausführen eines Neustarts .

5.1. Aktualisierung der Antiviren-Datenbanken

Ein obligatorischer Faktor des umfassenden Antivirenschutzes ist das Update der Antiviren-Datenbanken, das von der Komponente *keepup2date* der Anwendung ausgeführt wird. Als Updatequelle für die von Kaspersky Anti-Virus bei Suche und Desinfektion infizierter Objekte verwendeten Antiviren-Datenbanken dienen die Kaspersky-Lab-Updateserver. Zum Beispiel:

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

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

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

Eine Liste der Adressen, von denen Updates kopiert werden können, befindet sich in der Datei *updcfg.xml*, die zum Lieferumfang der Anwendung gehört.

Die Komponente *keepup2date* greift bei der Aktualisierung auf diese Liste zu, wählt eine Adresse und versucht, die Antiviren-Datenbanken vom Server zu kopieren. Wenn das Update von der gewählten Adresse fehlschlägt, greift die Komponente auf die nächste Adresse zu und versucht erneut, die Datenbanken zu aktualisieren.



Updates für die Antiviren-Datenbanken werden mehrmals stündlich auf den Kaspersky-Lab-Updateservern veröffentlicht.

Nach dem erfolgreichen Update wird der Befehl ausgeführt, der als Wert des Parameters **PostUpdateCmd** im Abschnitt **[updater.options]** der Konfigurationsdatei festgelegt ist. In der Grundeinstellung lädt dieser Befehl automatisch die Antiviren-Datenbanken neu. Wenn diesem Parameter ein falscher Wert zugeordnet wird, kann die Folge sein, dass die Anwendung entweder die aktualisierten Datenbanken nicht verwendet oder fehlerhaft funktioniert.



Alle Parameter der Komponente *keepup2date* sind in den Optionen **[updater.*]** der Konfigurationsdatei angeordnet.

Wenn die Struktur Ihres lokalen Netzwerks eine gewisse Komplexität aufweist, empfehlen wir Ihnen, jede Stunde die Updates der Antiviren-Datenbanken von den Updateservern herunterzuladen, sie in einem bestimmten Netzwerkordner abzulegen und für die lokalen Netzwerkcomputer das Kopieren der Datenbanken aus diesem Ordner festzulegen. Details zum Erstellen eines Netzwerkordners s. Pkt. 5.1.3 auf S. 36.

Das Update lässt sich mit Hilfe des Programms **cron** (s. Pkt. 5.1.1 auf S. 34) nach einem Zeitplan organisieren oder es kann durch manuellen Start aus der Befehlszeile auf Befehl des Administrators ausgeführt werden (s. Pkt. 5.1.2 auf S. 35).



Es wird ausdrücklich empfohlen, als Abstand zwischen den Updates der Antiviren-Datenbanken höchstens eine Stunde zu wählen!

Außerdem verfügt Version 5.5 von Kaspersky Anti-Virus über eine Option zur Auswahl des Typs der zu verwendenden Antiviren-Datenbanken. Dadurch lässt sich die optimale Sicherheitsstufe des Antivirenschutzes gewährleisten.

Standard-Datenbanken – Antiviren-Datenbanken, die eine ausführliche Beschreibung aller momentan vorhandenen Viren sowie Methoden für deren Identifikation und Desinfektion enthalten. Diese Antiviren-Datenbanken werden standardmäßig verwendet.

Erweiterte Datenbanken – Antiviren-Datenbanken, die neben Viren auch Informationen über Programme der Risikogruppe (RiskWare) und Werbeprogramme (AdWare) enthalten .

Programme der Risikogruppe enthalten Schwachstellen, die für Hackerangriffe, zum Eindringen unerlaubter Programme usw. benutzt werden können.

AdWare-Programme werden zusammen mit anderer Software installiert und zeigen danach Werbung an, die entweder in Zusatzfenstern erscheint oder den Benutzer dazu zwingt, entsprechende Webseiten zu besuchen. Neben der Belästigung durch aufdringliche Werbung führen solche Programme zu einer wesentlichen Belastung von Verbindungskanälen und erhöhen den Datenverkehr.

Für die gewöhnliche Arbeit ist es ausreichend, die standardmäßigen Antiviren-Datenbanken zu verwenden. Die erweiterten Datenbanken werden zur Gewährleistung eines erhöhten Sicherheitsniveaus für Informationen benutzt. Die Verwendung der erweiterten Antiviren-Datenbanken führt zu erhöhtem Ressourcenbedarf bei der Datenuntersuchung.

5.1.1. Automatisches Update der Antiviren-Datenbanken

Mit Hilfe des Programms cron können Sie das regelmäßige automatische Update der Antiviren-Datenbanken planen.



Aufgabe: Automatischer Start des Updates der Antiviren-Datenbanken alle 3 Stunden. Im Systembericht nur Fehler bei der Programmarbeit festhalten. In einem allgemeinen Bericht alle Aufgabenstarts festhalten. Keine Informationen an der Konsole anzeigen.



Lösung: Gehen Sie zur Lösung der Aufgabe folgendermaßen vor:

1. Geben Sie in der Konfigurationsdatei der Anwendung für die Parameter entsprechende Werte an, beispielsweise:

```
[updater.options]
KeepSilent=yes
[updater.report]
Append=yes
ReportLevel=4
```

2. Passen Sie die Datei an, in der die Regeln für die Arbeit des Prozesses cron festgelegt sind (**crontab -e**). Geben Sie dazu folgende Zeile an:

```
0 0-23/3 * * */opt/kaspersky/kav4samba/bin/kav4samba-keepup2date
```



Aufgabe: Download der Updates für die Antiviren-Datenbanken von den Kaspersky-Lab-Updateseiten. Adresse der Updateseite automatisch aus der Liste ermitteln, die zum Umfang der Komponente *keepup2date* gehört.



Lösung: Gehen Sie zur Lösung der Aufgabe folgendermaßen vor:

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



Aufgabe: Download der Updates für die Antiviren-Datenbanken von der Adresse, die der Administrator angibt. Wenn das Update von dieser Adresse fehlschlägt, wird der Updatevorgang abgebrochen.



Lösung: Gehen Sie zur Lösung der Aufgabe folgendermaßen vor:

Geben Sie für die Parameter **UseUpdateServerUrl** und **UseUpdateServerUrlOnly** im Abschnitt **[updater.options]** den Wert **Yes** an. Außerdem muss der Parameter **UpdateServerUrl** die Adresse des Updateservers enthalten.



Aufgabe: Download der Updates für die Antiviren-Datenbanken von der Adresse, die der Administrator angibt. Wenn das Update von dieser Adresse fehlschlägt, werden die Datenbanken von der Adresse aktualisiert, die in einer in Kaspersky Anti-Virus integrierten Updateliste festgelegt ist.



Lösung: Gehen Sie zur Lösung der Aufgabe folgendermaßen vor:

Geben Sie für den Parameter **UseUpdateServerUrl** im Abschnitt **[updater.options]** den Wert **Yes** und für den Parameter **UseUpdateServerUrlOnly** den Wert **No** an. Außerdem muss der Parameter **UpdateServerUrl** die Adresse des Updateservers enthalten.

5.1.2. Update der Antiviren-Datenbanken auf Befehl

Das Update der Antiviren-Datenbanken kann jederzeit aus der Befehlszeile gestartet werden.



Aufgabe: Das Update der Antiviren-Datenbanken starten. Arbeitsergebnisse in der Datei */tmp/updatesreport.log* speichern.



Lösung: Geben Sie zur Lösung dieser Aufgabe folgende Befehlszeile ein:

```
# kav4samba-keepup2date -l /tmp/updatesreport.log
```

Wenn es erforderlich ist, die Antiviren-Datenbanken auf mehreren Computern zu aktualisieren, bietet sich an, die Datenbanken ein Mal von den Updateservern herunterzuladen, sie in einem bestimmten Netzwerkordner abzulegen und die Netzwerkcomputer danach aus diesem Ordner zu aktualisieren. Dadurch wird der wiederholte Download aus dem Internet überflüssig.



Aufgabe: Das Update der Antiviren-Datenbanken soll aus dem Netzwerkordner **/home/bases** erfolgen. Wenn dieser Ordner leer ist, erfolgt das Update von den Kaspersky-Lab-Servern. Arbeitsergebnisse in der Berichtsdatei `report.txt` festhalten.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Geben Sie in der Konfigurationsdatei der Anwendung folgende Parameterwerte an:

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

2. Geben Sie in der Befehlszeile ein:

```
# kav4samba-keepup2date -l /tmp/report.txt
```

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

Damit die Aktualisierung der Antiviren-Datenbanken aus einem Netzwerkordner korrekt verläuft, ist es erforderlich, in diesem Ordner eine Dateistruktur anzulegen, die der Struktur auf den Kaspersky-Lab-Updateservern entspricht. Diese Aufgabe wird unten genau beschrieben.



Aufgabe: Erstellen eines Netzwerkordners, aus dem die Antiviren-Datenbanken auf lokale Netzwerkcomputer kopiert werden können.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Erstellen Sie einen lokalen Ordner.
2. Starten Sie die Komponente `keepup2date` folgendermaßen:

```
# kav4samba-keepup2date -u <dir>
```

wobei `<dir>` – vollständiger Pfad des erstellten Ordners.

3. Gewähren Sie den lokalen Computern den Netzwerkzugriff zum Lesen dieses Ordners.



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. Stellen Sie sicher, dass der Parameter **ProxyAddress** im Abschnitt **[updater.options]** der Konfigurationsdatei die Adresse des Proxyservers enthält. Die Adresse muss folgendes Format besitzen: **http://username:password@ip_address:port**. Dabei sind die Werte **ip_address** und **port** obligatorisch, während **username** und **password** nur dann anzugeben sind, wenn es für die Autorisierung auf dem Proxyserver notwendig ist.

oder:

1. Geben Sie im Abschnitt **[updater.options]** der Konfigurationsdatei für den Parameter **UseProxy** den Wert **Yes** an.
2. Verwenden Sie für die Umgebungsvariable **http_proxy** das Format **http://username:password@ip_address:port**. 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 Samba-Servers im Echtzeitmodus

Der Echtzeit-Antivirenschutz des Samba-Servers erfolgt mit Hilfe der Komponente *kavsamba*, die die Zugriffe auf Dateien über den Samba-Server überwacht. *kavsamba* wird beim Start der Betriebssystemsdienste gestartet. Nachdem die angefragte Datei mit Hilfe des in die Komponente integrierten Antivirenkerns analysiert wurde, trifft *kavsamba* eine Entscheidung über die weitere Arbeit mit der Datei (Zugriff erlauben/verbieten).

Der Desinfektionsmodus für infizierte Objekte ist standardmäßig deaktiviert. Beim Fund von infizierten, verdächtigen oder beschädigten Objekten wird der Zugriff darauf gesperrt und entsprechende Informationen werden protokolliert.



Alle Einstellungen der Komponente *kavsamba* sind in den Abschnitten **[samba.*]** der Konfigurationsdatei der Anwendung angeordnet. Sie können zusätzlich die Modi zur Desinfektion infizierter Objekte, zum Verschieben von infizierten Objekten in einen bestimmten Ordner usw. aktivieren. Nehmen Sie dazu die entsprechenden Einstellungen in der Konfigurationsdatei vor. Details dazu s. Pkt. 6.1.3 auf S. 45.

5.2.1. Konfiguration der Benutzerbenachrichtigung

Da *kavsamba* im Hintergrundmodus arbeitet, werden nur Start- und Hilfeinformationen auf der Konsole angezeigt. Zusätzliche Benachrichtigungsoptionen lassen sich beispielsweise durch E-Mails oder über das Standard-Tool **smbclient** realisieren. Betrachten wir diese Möglichkeiten genauer.

5.2.1.1. Monitoring mit Benachrichtigung durch smbclient

Das Standard-Tool **smbclient** dient der Übertragung von **winpopup**-Meldungen an den lokalen Computer. Im Betriebssystem Windows werden solche Meldungen (**winpopup**) auf dem Bildschirm angezeigt, wenn der Dienst Messenger (Nachrichtendienst) aktiviert ist. Dieses Tool wird in bestimmten Fällen automatisch installiert. Allerdings muss das Vorhandensein von **smbclient** vor dem Beginn der Arbeit überprüft werden.

Nützlich ist die Verwendung dieser Option zur Warnung von Benutzern, wenn versucht wird, über den Samba-Server auf eine infizierte Datei zuzugreifen.

Betrachten wird diese Benachrichtigungsmethode an einem Beispiel:



Aufgabe: Wenn versucht wird, über den Samba-Server auf eine infizierte Datei zuzugreifen, soll auf dem Benutzerbildschirm eine Meldung erscheinen.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Legen Sie eine Aktion (in diesem Fall die Bildschirmanzeige einer Meldung) für infizierte Dateien fest. Geben Sie dazu in der Konfigurationsdatei im Abschnitt **[samba.notify]** als Aktion folgende Zeile an:

```
OnInfected=exec echo "%USER%
%FULLPATH%/%FILENAME% is infected by %VIRUSNAME%"
| smbclient -M %USERHOST%
```

2. Starten Sie Kaspersky Anti-Virus neu.

5.2.1.2. Monitoring mit Benachrichtigung durch E-Mails

Wird das Monitoring mit Benachrichtigung per E-Mail organisiert, dann werden Warnungen über den versuchten Zugriff auf eine infizierte oder verdächtige Datei im Textteil einer E-Mail-Nachricht an eine festgelegte Adresse geschickt.



Damit Benachrichtigungen per E-Mail empfangen werden können, muss das Mailsystem entsprechend eingestellt sein!



Aufgabe: Der Administrator soll benachrichtigt werden, wenn ein Benutzer versucht, über den Samba-Server auf eine infizierte oder verdächtige Datei zuzugreifen.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Legen Sie eine Aktion für infizierte Dateien fest. Geben Sie dazu in der Konfigurationsdatei im Abschnitt **[samba.notify]** als Aktion folgende Zeile an:

```
OnInfected=exec echo "%USER%  
%FULLPATH%/FILENAME% from %USERHOST% is infected  
by %VIRUSNAME%" | mail -s 'Virus notification'  
spam-virus@localhost.ru
```

```
OnWarning=exec echo "%USER% %FULLPATH%/FILENAME%  
from %USERHOST% is probably infected by  
%VIRUSNAME%" | mail -s 'Virus notification' spam-  
virus@localhost.ru
```

```
OnSuspicion=exec echo "%USER%  
%FULLPATH%/FILENAME% from %USERHOST% is probably  
infected by %VIRUSNAME%" | mail -s 'Virus  
notification' spam-virus@localhost.ru
```



Vergessen Sie den Neustart von Kaspersky Anti-Virus nicht (s. Pkt. Error! Reference source not found. auf S. Error! Bookmark not defined.).

5.3. Antivirenschutz für Dateisysteme



Der Scan auf Befehl kann nur vom Benutzer **root** gestartet werden!

Der Antivirenschutz der Serverdateisysteme erfolgt mit Hilfe der Komponente *kavscanner*, die Serverdateien auf das Vorhandensein von Viren untersucht und den Einstellungen entsprechend die Bearbeitung infizierter und/oder verdächtiger Objekte durchführt. Die Bearbeitung der Objekte kann entweder rein informativen Charakter besitzen (Anzeige von Informationen im Bericht und auf der Serverkonsole, Benachrichtigung des Administrators) oder auch zur Veränderung des Objekts führen (Desinfektion, Verschieben in ein separates Verzeichnis, Löschen).



Alle Einstellungen der Komponente *kavscanner* befinden sich in den Abschnitten **[scanner.*]** der Konfigurationsdatei der Anwendung.



In der Grundeinstellung nimmt *kavscanner* (ebenso wie *kavsamba*) lediglich die Benachrichtigung des Benutzers/Administrators über den Fund infizierter Objekte vor. Zu Zusatzeinstellungen anderer Aktionen für eine Datei s. Pkt. 6.2.3 auf S. 50.

Die Untersuchung der Serverdateisysteme kann auf Befehl des Administrators aus der Befehlszeile oder mit Hilfe des Standard-Tools **cron** automatisch nach Zeitplan ausgeführt werden. Sie können entweder die Untersuchung aller Dateisysteme des Servers oder eines bestimmten Verzeichnisses festlegen. Es können auch Sektoren von Blockgeräten untersucht werden.

Im Folgenden finden Sie eine ausführliche Beschreibung der typischen Aufgaben für den Antivirenschutz von Serverdateisystemen.



Der Vorgang zur Virenuntersuchung des gesamten Computers ist eine Prozedur mit relativ hohem Ressourcenbedarf. Es ist zu beachten, dass dabei die Funktionsgeschwindigkeit des Servers verlangsamt wird. Deshalb wird empfohlen, für die Untersuchung einen Zeitraum zu wählen, in dem die Auslastung des Servers möglichst gering ist.

5.3.1. Dateiuntersuchung auf Befehl

Eine der Aufgaben, die mit Kaspersky Anti-Virus gelöst werden können, besteht in der Virenuntersuchung und Desinfektion von Dateien eines bestimmten Serververzeichnisses.



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

Die Arbeitsergebnisse der Komponente (Startdatum, Informationen über alle Dateien außer virusfreien Objekten, mit Detailinfos) sollen nur in der Berichtsdatei *kavscanner-aktuelles_Datum.log* erscheinen, die im gleichen Verzeichnis gespeichert wird.



Lösung: Geben Sie zur Lösung dieser Aufgabe folgende Befehlszeile ein:

```
# ./kav4samba-kavscanner -rlq  
-o kavscanner-`date +%F`.log -i3 -ePASBME -j3 -mCn  
/tmp
```

5.3.2. Untersuchung eines Ordners nach Zeitplan (cron)

Mit Hilfe des Tools **cron**, das dem zeitgesteuerten Start von Programmen dient, können Sie die automatische Ausführung einer beliebigen Aufgabe von Kaspersky Anti-Virus for Samba Servers festlegen. Dazu zählt auch die Untersuchung eines Ordners nach Zeitplan.



Aufgabe: Jeden Tag um 0 Uhr 00 Minuten soll die Virenuntersuchung des Verzeichnisses **/home** gestartet werden, wobei die Untersuchungsparameter aus der Konfigurationsdatei */etc/kav/kavscanner.cron* zu verwenden sind.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Legen Sie die Konfigurationsdatei */etc/kav/kavscanner.cron* an und bestimmen Sie die erforderlichen Untersuchungsparameter.
2. Ändern Sie die Datei, welche die Regeln für die Arbeit des Prozesses **crontab -e** festlegt: Geben Sie folgende Zeile an:

```
0 0 * * * /path/to/kav4samba-kavscanner -c  
/etc/kav/kavscanner.cron /home
```

5.3.3. Zusätzliche Optionen: Verwendung von Skriptdateien

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

5.3.3.1. Senden einer Benachrichtigung an den Administrator

Durch die Verwendung von Unix-Standardwerkzeugen können Sie Kaspersky Anti-Virus so einstellen, dass der Server-Administrator über den Fund infizierter, verdächtiger und beschädigter Dateien in den Dateisystemen benachrichtigt wird.



Aufgabe: Konfiguration der Benachrichtigung des Administrators über den Fund infizierter Dateien und Archive in den Dateisystemen des Servers bei jeder Untersuchung des Servers, die entsprechend den Parametern der Konfigurationsdatei der Anwendung ausgeführt wird.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

Geben Sie in der Konfigurationsdatei der Anwendung die Bearbeitungsregeln für gewöhnliche Objekte und Archiv-Objekte an:

```
[scanner.object]
```

```
OnInfected=exec echo %FULLPATH%/%FILENAME% is  
infected by %VIRUSNAME% | mail -s kav4samba-  
kavscanner admin@localhost.ru
```

```
[scanner.container]
```

```
OnInfected=exec echo archive %FULLPATH%/%FILENAME% is  
infected, viruses list is in the attached file %LIST%  
| mail -s kav4samba-kavscanner -a %LIST%  
admin@localhost.ru
```

KAPITEL 6. ZUSÄTZLICHE EINSTELLUNGEN

In diesem Kapitel behandeln wir ausführlich die zusätzlichen Funktionalitätseinstellungen von Kaspersky Anti-Virus. Im Unterschied zu den obligatorischen Einstellungen, die bei der Installation vorgenommen werden (s. Pkt. 3.3 auf S. 17) und ohne die die Anwendung nicht verwendet werden kann, erfolgen die Zusatzeinstellungen nach Ermessen des Administrators. Sie zielen auf die Erweiterung der Möglichkeiten der Anwendung und deren Anpassung an die Verwendungsbedingungen im Rahmen eines konkreten Unternehmens ab.

6.1. Konfiguration des Echtzeit- Antivirenschutzes

Wie oben erwähnt, erfolgt der Antivirenschutz des Samba-Servers im Echtzeitmodus durch die Komponente *kavsamba*.

Zur Konfiguration der Komponente können folgende Parameter angepasst werden:

- Untersuchungsbereich: Pfad und Objekte des Schutzes (s. Pkt. 6.1.1. auf S. 43).
- Modus zur Untersuchung und Desinfektion von Dateien (s. Pkt. 6.1.2 auf S. 44).
- Aktionen für Dateien (s. Pkt. 6.1.3. auf S. 45).
- Modus zum Erstellen von Sicherungskopien (s. Pkt. 6.1.5 auf S. 51).
- Erstellen von Bericht und Meldungen (s. Pkt. 6.5 auf S. 56).

6.1.1. Untersuchungsbereich

Der Untersuchungsbereich der Komponente *kavsamba* umfasst *Pfad* und *Objekte des Schutzes*.

Unter *Pfad* werden alle Dateisysteme verstanden, die für den Benutzer über den Samba-Server zugänglich sind. Eine Einschränkung des Pfads kann nur durch den Ausschluss bestimmter Verzeichnisse oder Dateien in der Konfigurationsdatei der Anwendung erfolgen (Abschnitt **[samba.options]**, Parameter **ExcludeMask** und **ExcludeDirs**).

Die *Schutzobjekte* (Dateitypen, die auf Viren untersucht werden) werden nur durch die Parameter der Konfigurationsdatei der Anwendung im Abschnitt **[samba.options]** festgelegt.



Beim Start der Komponente *kavsamba* kann der Schutzbereich nicht in der Befehlszeile festgelegt oder eingeschränkt werden. Diese Option steht nur für die Antivirenuntersuchung der Serverdateisysteme zur Verfügung (Komponente *kavscanner*).

6.1.2. Modus zur Untersuchung und Desinfektion von Dateien

kavsamba unterstützt für den Zugriff auf Dateien die Operationen Öffnen und Schließen. Standardmäßig werden beim Öffnen alle Dateien, die nicht leer sind, überprüft. Beim Schließen wird eine Datei überprüft, wenn sie verändert wurde.

In der Grundeinstellung ist der Desinfektionsmodus für gefundene infizierte Dateien nicht aktiviert. Es wird also lediglich der Benutzer (und/oder Administrator) benachrichtigt, wenn Viren oder verdächtige Objekte gefunden werden. Die Benachrichtigung erfolgt durch die Aufzeichnung einer Meldung in der Berichtsdatei (s. Pkt. 6.6 auf S. 56). Der Zugriff auf solche Objekte wird automatisch gesperrt.

Der Desinfektionsmodus für infizierte Objekte wird in der Konfigurationsdatei (Abschnitt **[samba.options]**, Parameter **Cure=yes**) aktiviert. Wenn eine Datei infiziert ist (d.h. den Status **Infected** besitzt) führt *kavsamba* nach der Dateiuntersuchung die Aktionen durch, die in den Einstellungen der Konfigurationsdatei festgelegt sind (s. Pkt. 6.1.3 auf S. 45).

Als Ergebnis der Untersuchung (und Desinfektion) erhält eine Datei einen der folgenden Status:

- **Clear** – Datei ist nicht infiziert.
- **Infected** – Datei ist infiziert.
- **Cured** – Infizierte Datei wurde erfolgreich desinfiziert.
- **CureFailed** – Desinfektion der Datei war erfolglos.
- **Warning** – Code der Datei besitzt Ähnlichkeit mit dem Code eines bekannten Virus.
- **Suspicion** – Datei ist verdächtig, von einem unbekanntem Virus infiziert zu sein.
- **Protected** – Datei kann nicht untersucht werden, weil sie verschlüsselt ist.

- **Corrupted** – Datei ist beschädigt.

Abhängig vom Status der Datei wird der Zugriff darauf entweder gesperrt (**Infected, CureFailed, Warning, Suspicion**) oder erlaubt (alle übrigen Status).



Auf Dateien mit dem Status **CureFailed** werden die Aktionen angewandt, die für infizierte Objekte festgelegt wurden!

Beachten Sie, dass *kavsamba* bei der Untersuchung von Container-Objekten (Archiven) zur Beschleunigung der Arbeit ein Archiv nicht weiter untersucht und dem gesamten Archiv den Status **Infected** zuweist, sobald ein Virus darin gefunden wurde. Das bedeutet, dass *kavsamba* nur einen Virus im Bericht vermerkt, auch wenn das Objekt von mehreren Viren infiziert ist.

6.1.3. Aktionen für Dateien

Für Dateien mit den Status **Infected, Suspicious, Warning, Cured, Protected, Corrupted** und **Error** kann eine Reihe von Aktionen festgelegt werden:

- *Verschieben in ein bestimmtes Verzeichnis* – Verschieben von Dateien mit einem bestimmten Status in einen festgelegten Ordner; *einfaches* und *rekursives Verschieben sind möglich*.
- *Löschen* der Datei aus dem Dateisystem.
- *Ausführen eines bestimmten Befehls* – Bearbeitung von Dateien mit Linux-Standardbefehlen, Skriptdateien usw.

Beachten Sie, dass die Komponente *kavsamba* bei den Aktionen nicht zwischen Dateien und Archiv-Objekten unterscheidet. Deshalb können im Bericht z.B. mehrere Virusnamen angegeben sein, durch die ein Objekt infiziert ist.

Die Bearbeitungsregeln für Objekte können folgendermaßen angepasst werden:

- Festlegen der Regeln in der Konfigurationsdatei der Anwendung, wenn sie als Standardaktionen verwendet werden sollen (Abschnitt **[samba.actions]**).
- Angabe der Bearbeitungsregeln in einer alternativen Konfigurationsdatei und Verwendung der Datei beim Start der Komponente.



Beachten Sie, dass der Netzwerkordner **/homes** virtuell ist und auf das Home-Verzeichnis aller Benutzer verweist. Für solche Ordner können keine individuellen Antivirenschutz-Parameter festgelegt werden.

Deshalb werden für die Definition der Schutzparameter von Home-Verzeichnissen die Einstellungen des Abschnitts **[samba.shares]** verwendet. Wenn die Antivirenuntersuchung im Abschnitt **[samba.shares]** deaktiviert ist, werden die Home-Verzeichnisse der Benutzer nicht geschützt.

6.1.4. Infizierte Objekte isolieren

Die Möglichkeit zum Verschieben infizierter Dateien in ein separates Verzeichnis wird zur Isolation eines infizierten Objekts verwendet (Abschnitt **[samba.actions]** Parameter **MovePath**). Das Verschieben findet dann statt, wenn die Desinfektion einer Datei erfolglos war (z.B. wenn nur zwei von drei Viren, durch die eine Datei infiziert ist, entfernt werden konnten).



Der Administrator kann festlegen, dass Objekte in Abhängigkeit vom Dateistatus in unterschiedliche Verzeichnisse verschoben werden.

Wenn ein solches Verzeichnis erhalten bleiben soll, empfiehlt es sich, es mit Hilfe des Parameters **ExcludeDir** (Abschnitt **[samba.options]**) der Konfigurationsdatei aus dem Untersuchungsbereich auszuschließen.



Aufgabe: Virenuntersuchung aller Dateien, die über den Samba-Server aufgerufen werden, und Desinfektion, wenn ein Objekt infiziert ist. Infizierte Objekte, deren Desinfektion erfolglos ist, werden mit vollständiger Pfadangabe in das Verzeichnis **/tmp/infected** verschoben.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Aktivieren Sie in der Konfigurationsdatei der Anwendung den Modus zur Desinfektion infizierter Objekte (**Cure=yes** im Abschnitt **[samba.options]**).
2. Erstellen Sie eine Regel zur Isolierung von infizierten Objekten. Geben Sie dazu im Abschnitt **[samba.actions]** der Konfigurationsdatei folgende Zeile an:

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

3. Starten Sie Kaspersky Anti-Virus neu (s. Pkt. Error! Reference source not found. auf S. Error! Bookmark not defined.).

6.1.5. Modus zum Erstellen von Sicherungskopien von Objekten

Wenn Dateien infiziert sind und als Aktion für infizierte Objekte das Löschen aus dem Dateisystem festgelegt ist, besteht die Gefahr des Verlusts wichtiger Daten. Um dem vorzubeugen, bietet Kaspersky Anti-Virus die Möglichkeit zum Kopieren der Dateien in ein Backup-Verzeichnis.

Bevor eine Datei desinfiziert oder gelöscht wird, legt die Anwendung im Backup-Verzeichnis (Abschnitt **[samba.path]**, Parameter **BackupPath**) eine Kopie davon an. Da eine Sicherungskopie gespeichert wird, kann die ursprüngliche Datei bei Bedarf wiederhergestellt werden, falls die Datei während der Desinfektion beschädigt wurde. Die Datei wird mit vollständigem Pfad im Backup gespeichert. Bei wiederholter Speicherung im Backup-Verzeichnis wird die ältere Kopie der Datei jeweils automatisch durch die aktuelle ersetzt.

Beachten Sie, dass in der Grundeinstellung der Modus zum Anfertigen einer Sicherungskopie im Backup nicht aktiviert ist und dementsprechend der Pfad des Verzeichnisses, das zum Speichern von Sicherungskopien dienen soll, nicht festgelegt ist. Um diese Option zu verwenden, müssen Sie den Pfad selbst festlegen.



Wird ein Objekt aus dem Dateisystem gelöscht, dann wird seine Kopie solange im Backup aufbewahrt, bis der Administrator sie löscht.

6.2. Konfiguration des Antivirenschutzes für Dateisysteme

Der Antivirenschutz der Serverdateisysteme erfolgt mit Hilfe der Komponente *kavscanner*. Die standardmäßig verwendeten Funktionsparameter der Komponente *kavscanner* sind in der Konfigurationsdatei der Anwendung enthalten. Diese Parameter bieten die maximale Untersuchung der Dateisysteme, die für Workstation, auf der das Produkt installiert ist, verfügbar sind. Alle verfügbaren Dateien werden auf das Vorhandensein von Viren untersucht, darunter:

- gepackte Dateien
- Archive
- selbstextrahierende Archive
- Mail-Datenbanken

- E-Mail-Nachrichten

Die Gesamtauswahl der Parameter für den Antivirenschutz der Serverdateisysteme lassen sich nach ihren Funktionen in folgende Gruppen unterteilen:

- Untersuchungsbereich (s. Pkt. 6.2.1 auf S. 48) (Dieser Parameter entspricht dem Untersuchungsbereich bei der Verwendung des Echtzeitschutzes).
- Modus zur Untersuchung und Desinfektion von Dateien (s. Pkt. 6.2.2 auf S. 49).
- Aktionen für Dateien (s. Pkt. 6.2.3 auf S. 50).

Betrachten wir die Einstellungen jeder einzelnen Gruppe genauer.

6.2.1. Untersuchungsbereich

Der Untersuchungsbereich lässt sich bedingt in zwei Teile gliedern:

- *Untersuchungspfad* – Liste der Verzeichnisse und Dateien, in denen die Virensuche durchgeführt wird.
- *Untersuchungsobjekte* – Typen der Dateien, die auf das Vorhandensein von Viren gescannt werden (Archive, E-Mails usw.).

In der Grundeinstellung werden alle Objekte der verfügbaren Dateisysteme untersucht, wobei mit dem aktuellen Verzeichnis begonnen wird.



Zur Untersuchung aller Dateisysteme des Servers ist es erforderlich, in das Stammverzeichnis zu wechseln oder in der Befehlszeile den gewünschten Untersuchungsbereich anzugeben.

Der Untersuchungspfad kann durch folgendermaßen geändert werden:

- Durch Leerzeichen getrennte Angabe der Verzeichnisse und Dateien mit absoluten oder relativen (im Bezug auf das aktuelle Verzeichnis) Pfaden direkt in der Befehlszeile beim Start der Komponente.
- Angabe der Untersuchungspfade in einer Textdatei. Dabei wird in der Befehlszeile durch den Parameter `-@ <Dateiname>` festgelegt, dass diese Datei verwendet werden soll. Jedes Objekt in dieser Datei wird in einer extra Zeile und mit absoluter Pfadangabe angegeben.



Werden in der Befehlszeile sowohl ein Untersuchungspfad als auch eine Textdatei mit einer Liste von Untersuchungsobjekten angegeben, so werden zuerst die in der Befehlszeile angegebenen und danach die in der Datei festgelegten Objekte untersucht.

- Einschränkung der Pfade, die standardmäßig festgelegt sind (alle, beginnend mit dem aktuellen Verzeichnis) oder in der Befehlszeile aufgezählt werden, indem in der Konfigurationsdatei der Anwendung Masken für Dateien und Verzeichnisse angegeben werden, die aus dem Untersuchungsbereich ausgeschlossen werden sollen (Abschnitt **[scanner.options]**, Parameter **ExcludeMask** und **ExcludeDirs**).
- Deaktivieren der *rekursiven Untersuchung von Verzeichnissen* (Abschnitt **[scanner.options]**, Parameter **Recursion** oder Befehlszeilenparameter **-r**).
- Anlegen einer alternativen Konfigurationsdatei. Dabei wird beim Start der Komponente durch den Parameter **-c <Dateiname>** festgelegt, dass diese Datei verwendet werden soll.

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

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

6.2.2. Modus zur Untersuchung und Desinfektion von Dateien

Der Modus zur Untersuchung und Desinfektion von Dateien für die Komponente *kavscanner* entspricht vollständig jenem der Komponente *kavsamba*. Die einzige Ausnahme besteht darin, dass *kavscanner* auch für Dateien mit dem Status **Corrupted** unterschiedliche Aktionen durchführt (Details zu den Aktionen s. Pkt. 6.1.3 auf S. 45).

Beachten Sie, dass die Desinfektionsoption in der Grundeinstellung nicht aktiviert ist. Standardmäßig erfolgt lediglich die Virenuntersuchung der Dateien und es wird über den Fund infizierter, verdächtiger oder beschädigter Objekte durch Meldungen auf der Konsole und im Bericht informiert.

Als Ergebnis der Virenuntersuchung erhält jede Datei einen bestimmten Status (**Clear**, **Infected**, **Warning** usw.), auf dessen Grundlage die in der Konfigurationsdatei festgelegten Aktionen mit dem Objekt vorgenommen werden.

Beachten Sie, dass bei aktiviertem Desinfektionsmodus (Abschnitt **[scanner.options]**, Parameter **Cure=yes**) für Dateien mit dem Status **Infected** ein Desinfektionsversuch erfolgt.

6.2.3. Aktionen für Dateien

Abhängig vom Status einer Datei können auf diese bestimmte Aktionen angewandt werden. In der Grundeinstellung wird nur die Benachrichtigung über den Fund von Dateien mit einem bestimmten Status durchgeführt, indem auf der Konsole und im Bericht Meldungen erscheinen.

Für Dateien mit den Status **Infected**, **Suspicious**, **Warning**, **Cured**, **Protected**, **Corrupted** und **Error** kann aber analog zu der Komponente *kavsamba* eine Reihe von Aktionen festgelegt werden:

- *Verschieben in ein bestimmtes Verzeichnis* – Verschieben von Dateien mit einem bestimmten Status in ein bestimmtes Verzeichnis; *einfaches* und *rekursives Verschieben sind möglich*.
- *Löschen* der Datei aus dem Dateisystem
- *Ausführen eines bestimmten Befehls* – Bearbeitung von Dateien mit Unix/Linux-Standardbefehlen, Skriptdateien usw.

Bei der Untersuchung von Serverdateisystemen unterscheidet Kaspersky Anti-Virus zwischen einem *gewöhnlichen Objekt* (Datei) und einem *Container-Objekt* (das aus mehreren Objekten besteht – Archiv). Auch die Aktionen, die mit solchen Objekten durchgeführt werden, unterscheiden sich. Sie werden in der Konfigurationsdatei in unterschiedlichen Abschnitten festgelegt. Für gewöhnliche Objekte im Abschnitt **[scanner.object]**, für zusammengesetzte Objekte im Abschnitt **[scanner.container]**.

Aktionen für selbstextrahierende Archive sind nicht eindeutig: Ist das Archiv selbst infiziert, dann wird es als gewöhnliches Objekt betrachtet, ist aber ein Objekt innerhalb des Archivs infiziert, dann gilt das Archiv als Container-Objekt. Dementsprechend werden in solchen Fällen auch die Aktionen für Archive durch die Parameter unterschiedlicher Abschnitte der Konfigurationsdatei bestimmt.

Die Aktionen für bestimmte Dateien werden folgendermaßen festgelegt:

- Angabe der Aktionen in der Konfigurationsdatei der Anwendung, wenn sie als Standardaktionen verwendet werden sollen (Abschnitte **[scanner.object]** und **[scanner.container]**).
- Angabe der Aktionen in einer alternativen Konfigurationsdatei und Verwendung der Datei beim Start der Komponente.
- Angabe der Aktionen für die laufende Session durch Befehlszeilenparameter beim Start der Komponente *kavscanner*.

6.2.4. Modus zum Erstellen von Sicherungskopien

Die Einstellungsmöglichkeiten für das Anfertigen von Sicherungskopien bei der Durchführung des Antivirenschutzes von Dateisystemen entsprechen vollständig den in Pkt. 6.1.5 auf S. 47 für den Antivirenschutz im Echtzeitmodus beschriebenen Optionen. Deshalb werden die Einstellungen für diesen Modus hier nicht näher beschrieben.



Aufgabe: Virenuntersuchung und Desinfektion aller Objekte in den Verzeichnissen und Dateien, die in der Datei `/tmp/download.lst` angegeben sind. Infizierte Dateien, deren Desinfektion fehlschlägt, sollen je nach Status mit vollständigem Pfad in folgende Verzeichnisse verschoben werden: infizierte Dateien nach `/tmp/infected`, verdächtige nach `/tmp/suspicious` und beschädigte nach `/tmp/warning`.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Legen Sie die alternative Konfigurationsdatei `scan_sample.conf` an.
2. Vergewissern Sie sich, dass der Modus zur Desinfektion infizierter Objekte aktiviert ist (**Cure=yes** im Abschnitt **[scanner.options]**).
3. Legen Sie die Bearbeitungsregeln für infizierte Objekte fest. Geben Sie dazu in den Abschnitten **[scanner.object]** und **[scanner.container]** der Konfigurationsdatei `scan_sample.conf` folgende Zeilen an:

```
OnInfected=MovePath /tmp/infected
OnSuspicion=MovePath /tmp/suspicious
OnWarning=MovePath /tmp/warning
```

4. Geben Sie in der Befehlszeile ein:

```
# kav4samba-kavscanner - -@/tmp/downloads.lst -c
sample_scan.conf
```

6.3. Optimierung der Arbeit von Kaspersky Anti-Virus for Samba Servers

Zur Verringerung der Serverbelastung bietet Kaspersky Anti-Virus for Samba Servers einige effektive Methoden zur Optimierung seiner Arbeit. Betrachten wir diese näher.



Verwendung der Datenbank iChecker und des Cache für untersuchte Dateien.

Die Anwendung benutzt verschiedene Technologien, die es überflüssig machen, jedes Mal eine Antivirenuntersuchung vorzunehmen, wenn ein Benutzerzugriff auf eine Datei erfolgt. Für solche Dateien ist eine Vergleichsoperation mit bereits darüber existierenden Daten ausreichend. Der Algorithmus zur Virenuntersuchung eines Objekts (einer Datei) lässt sich folgendermaßen beschreiben:

Bei der ersten Untersuchung einer beliebigen Datei werden Informationen über sie (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 *kavsamba* und *kavscanner* untersucht wurden.
- Cache der untersuchten Dateien – Eine Datenbank, die Informationen über alle von der Komponente *kavsamba* untersuchten Dateien enthält. Diese Datenbank befindet sich im Arbeitsspeicher und wird beim Abschluss der Arbeit der Komponente *kavsamba* nicht gespeichert.

Wenn bei der Untersuchung die Informationen über eine Datei nicht in der Datenbank iChecker aufgenommen werden (d.h. die Datei ist nicht virusfrei oder ihr Format wird nicht unterstützt), dann werden in der anderen Datenbank Informationen darüber fixiert.

Bei jedem folgenden Zugriff eines Benutzers auf die Datei wird zuerst in der Datenbank iChecker und danach (wenn das Objekt in der ersten Datenbank nicht gefunden wurde) im Cache nach passenden Informationen gesucht. Als Suchkriterium dient der Dateiname. Wird eine solche Datei in einer der Datenbanken gefunden, dann werden die Informationen über die Datei mit den 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 aufgerufene Datei gefunden werden, wird eine vollständige Antivirenuntersuchung der Datei durchgeführt.



Wenn Sie bei der Arbeit mit der Anwendung den Typ der zu verwendenden Antiviren-Datenbanken geändert haben, müssen die Informationen manuell aus der iChecker-Datenbank entfernt werden (Der vollständige Pfad der Datenbank wird durch den Parameter **icheckerDbFile** im Abschnitt **[path]** der Konfigurationsdatei der Anwendung festgelegt).

Diese Notwendigkeit ergibt sich daraus, dass die Datenbank infizierte Objekte enthalten kann, deren Identifikation mit Hilfe der standardmäßigen Antiviren-Datenbanken nicht möglich ist, die aber mit Hilfe der erweiterten Signaturen erkannt werden können. Da Dateien, die in der iChecker-Datenbank verzeichnet sind, nicht erneut untersucht werden, könnte es andernfalls zu einer Infektion des Computers kommen.



Durchführen einer Untersuchung im Hintergrund.

Da die Suche nach Daten über aufgerufene Objekte in den oben genannten Datenbanken sehr schnell verläuft, lässt sich die Serverbelastung wesentlich verringern und die Effektivität bei der Ressourcenverwendung des Servers kann gesteigert werden, was insbesondere die *Durchführung des Dateiuersuchung im Hintergrund* betrifft.

Während der Arbeit ermittelt Anti-Virus seine Auslastung. Wenn diese nicht über dem vorgegebenen Maximalwert liegt, untersucht er im Hintergrundmodus Dateien aus gemeinsamen Ordnern sowie jene Dateien, die während der Arbeit verändert werden.

Die Auslastung wird durch die maximale Anzahl von Dateien festgelegt, die gleichzeitig untersucht werden können (Abschnitt **[scanner.option]** Parameter **CheckFilesLimit**). Außerdem wird die Anzahl der Dateien festgelegt, die gleichzeitig im Hintergrundmodus untersucht werden können (Abschnitt **[scanner.option]** Parameter **BgCheckFilesLimit**). Ein weiterer Parameter ist der Zeitraum, nach dessen Verstreichen eine neue Datei zur Antivirenuntersuchung angefordert wird (Abschnitt **[samba.options]** Parameter **BgSheduleTime**).

Überschreitet die Anzahl der zur Untersuchung aufgerufenen Dateien den maximal zulässigen Wert, dann werden neu hinzukommende Dateien in eine Warteschlange gestellt und erst beim Sinken der Belastung unter den Maximalwert untersucht.

In diesem Fall müssen Benutzer, die die Untersuchung veranlasst haben, etwas länger auf eine Antwort warten, als erwartet. Beim Abschluss der Untersuchung wird die Datei aus der Warteschlange genommen. Darüber erfolgt keine zusätzliche Meldung.



Wenn das Anfrageintervall nicht festgelegt wurde ((**BgScheduleTime=0**), findet keine Untersuchung im Hintergrundmodus statt.

Dadurch wird die maximal zulässige Serverbelastung eingehalten.

6.4. Neustart von Kaspersky Anti-Virus



Während Kaspersky Anti-Virus neu gestartet wird, ist der Zugriff auf [**samba.shares**], der von Kaspersky Anti-Virus geschützt wird, gesperrt.

Es gibt mehrere Varianten für den Neustart von Kaspersky Anti-Virus:

- Der "Warmstart" wird nach der Aktualisierung der Antiviren-Datenbanken empfohlen.

Dabei werden die Antiviren-Datenbanken neu geladen, während alle Verbindungen bestehen bleiben. In diesem Modus findet kein Neustart der Komponente *kavsamba* statt, weshalb der Dateicache usw. erhalten bleibt.

Der "Warmstart" erfolgt durch Eingabe des folgenden Befehls in der Befehlszeile:
Für Linux-Distributionen:

```
/etc/init.d/kav4samba reload_avbase
```

Für FreeBSD -Distributionen:

```
/usr/local/etc/rc.d/kav4samba.sh reload_avbase
```

In diesem Fall erhält der Prozess *kavsamba* das Signal **SIGUSR1**.

- Das Ausführen des "Kaltstarts" wird empfohlen, wenn Änderungen in der Konfigurationsdatei oder in den Einstellungen erfolgten, oder ein neuer Lizenzschlüssel installiert wurde.

Dabei werden Konfigurationsdatei und Datenbanken neu eingelesen und alle Verbindungen mit einem Benutzer getrennt, da das eigentliche Programm zuerst seine Arbeit einstellt und danach neu gestartet wird.

Der "Kaltstart" erfolgt dies durch Eingabe des folgenden Befehls in der Befehlszeile:

Für Linux-Distributionen:

```
/etc/init.d/kav4samba reload
```

Für FreeBSD-Distributionen:

```
/usr/local/etc/rc.d/kav4samba.sh reload
```

In diesem Fall erhält der Prozess *kavsamba* das Signal **SIGHUP**.

- Durch die Eingabe des folgenden Befehls in der Befehlszeile kann die Arbeit von Kaspersky Anti-Virus zwangsläufig beendet werden:

Für Linux-Distributionen:

```
/etc/init.d/kav4samba stop
```

Für FreeBSD-Distributionen erfolgt dies durch Eingabe des folgenden Befehls in der Befehlszeile:

```
/usr/local/etc/rc.d/kav4samba.sh stop
```

Der Befehl sendet das Signal **SIGTERM** an den Prozess *kavsamba*, durch den die Arbeit von *kavsamba* beendet wird, alle von ihm erzeugten Kopien geschlossen werden und Kaspersky Anti-Virus seine Arbeit korrekt abschließt.



Es wird ausdrücklich empfohlen, den Befehl **kill -9** nicht zu verwenden, um die Arbeit mit dem Prozess *kavsamba* zu beenden. Zwar wird die Arbeit des Prozesses durch das Ausführen dieses Befehls beendet, aber es bleiben eine Reihe temporärer Dateien und Arbeitsdateien im System gespeichert, die nur manuell gelöscht werden können. Bestimmte Anwendungen halten den Prozess als aktiv, wenn solche Dateien im System vorhanden sind.

6.5. Lokalisierung des Formats für Datums- und Uhrzeitanzeige

Während der Arbeit mit Kaspersky Anti-Virus wird für jede Komponente ein Bericht erstellt. Außerdem werden unterschiedliche Meldungen für Benutzer und Administrator generiert. Solche Informationen enthalten jeweils die Angabe von Datum und Uhrzeit.

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

%H:%M:%S – angezeigtes Format des Uhrzeit (hh.mm.ss);

%d/%m/%y – angezeigtes Format der Datums (dd.mm.yy).

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

%I:%M:%S %P – zur Anzeige der Uhrzeit im Zwölfstunden-Format (Parameter **TimeFormat**).

%y/%m/%d oder **%m/%d/%y** – zur Anzeige des Datums (Parameter **DateFormat**) (yy.mm.dd bzw. mm.dd.yy).

6.6. Parameter für die Berichtsführung von Kaspersky Anti-Virus

Die Arbeitsergebnisse aller Komponenten von Kaspersky Anti-Virus werden in einem Bericht aufgezeichnet, der in einer Datei gespeichert wird.



Die Ergebnisse der Antivirenbearbeitung der Serverdateisysteme werden außerdem auf der Konsole angezeigt. In der Grundeinstellung sind die Informationen, die im Bericht aufgezeichnet und auf dem Bildschirm angezeigt werden, identisch. Wenn Sie möchten, dass auf der Konsole andere Informationen angezeigt werden als in der Berichtsdatei, ist eine Reihe von Zusatzeinstellungen erforderlich.

Der Umfang der angezeigten Informationen kann durch Änderung der *Berichtsgenauigkeit* beeinflusst werden.

Die **Berichtsgenauigkeit** wird durch eine Ziffer angegeben, welche die Genauigkeit der Informationen über die Arbeit der Komponenten im Protokoll festlegt. Jedes Folgeniveau umfasst die Informationen des vorhergehenden und bestimmte Zusatzinformationen.

Die folgende Tabelle enthält die möglichen Niveaus der Protokollgenauigkeit.

Niveau	Bezeichnung des Niveaus	Bedeutung
0	Kritische Fehler	Nur Informationen über kritische Fehler (Fehler, die zum Beenden der Arbeit der Anwendung führen, weil bestimmte Aktionen nicht ausgeführt werden können). Beispiele: Eine Komponente ist infiziert oder Fehler bei der Untersuchung oder beim Laden von Datenbanken und Lizenzschlüsseln.
1	Errors	Informationen über sonstige Fehler, einschließlich Fehlern, die nicht zum Beenden der Arbeit von Komponenten führten. Beispiel: Informationen über einen Fehler bei der Untersuchung einer Datei.

Niveau	Bezeichnung des Niveaus	Bedeutung
2	Warning	Informationen über Fehler, die zum Beenden der Arbeit des Produkts führen können. Beispiel: Informationen über zu wenig freien Platz auf einem Laufwerk.
3	Info, Notice	Wichtige Meldungen mit informativem Charakter. Beispiele: Informationen darüber, ob eine Komponente gestartet wurde, Pfad der Konfigurationsdatei, Untersuchungsbereich, Informationen über die Antiviren-Datenbanken bzw. Lizenzschlüssel, Ergebnisstatistik.
4	Activity	Meldungen über die Untersuchung von Dateien entsprechend dem Niveau des Untersuchungsberichts.
10	Debug	Alle Meldungen die das Erkennen, Lokalisieren und Korrigieren von Programmfehlern (Debuggen) betreffen. Beispiel: Inhalt der Konfigurationsdatei.

Informationen über kritische Fehler bei der Arbeit einer Komponente werden unabhängig vom gewählten Genauigkeitsniveau angezeigt. Das optimale Niveau ist Niveau **4**, das auch als Standard gilt.

KAPITEL 7. VERWALTUNG VON LIZENZSCHLÜSSELN

In Kaspersky Anti-Virus for Samba Servers ist eine Begrenzung des Nutzungszeitraums für die Anwendung vorgesehen (in der Regel beträgt dieser Zeitraum ein Jahr ab dem Erwerb). Bei Ablauf der Gültigkeitsdauer der Lizenz zur Benutzung von Kaspersky Anti-Virus wird die Anwendung weiterhin funktionieren, allerdings wird die Aktualisierung der Antiviren-Datenbanken nicht mehr möglich sein. Kaspersky Anti-Virus wird weiterhin die Desinfektion infizierter Objekte durchführen, dabei aber die alten Antiviren-Datenbanken verwenden.

Der Lizenzschlüssel verleiht Ihnen das Recht zur Benutzung der Anwendung und enthält alle erforderlichen Informationen, die mit der von Ihnen erworbenen Lizenz verbunden sind. Dazu zählen: Lizenztyp, Ende der Gültigkeitsdauer, Händlerinformationen u.a.

Neben dem Recht zur Verwendung der Anwendung während der Gültigkeitsdauer der Lizenz erhalten Sie folgende Möglichkeiten:

- Technische Unterstützung (rund um die Uhr)
- stündliches Update der Antiviren-Datenbanken
- Aktualisierung der Anwendung (Patch)
- Neue Versionen der Anwendung (Upgrade)
- frühzeitige Informationen über neue Viren

Wenn die Gültigkeitsdauer der Lizenz abläuft, verlieren Sie automatisch das Recht auf die oben genannten Möglichkeiten. Kaspersky Anti-Virus wird weiterhin die Antivirenbearbeitung der Serverdateisysteme durchführen, dabei aber nur die Antiviren-Datenbanken verwenden, die am Datum des Ablaufs der Lizenzgültigkeit aktuell waren. Die automatische Updatefunktion für die Antiviren-Datenbanken wird nicht mehr zur Verfügung stehen. Wird versucht, die Antiviren-Datenbanken manuell zu aktualisieren, dann verliert die Anwendung ihre Funktionsfähigkeit.

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

7.1.1. Informationen zum Lizenzschlüssel anzeigen

Die Informationen über installierte Lizenzschlüssel können in den Berichten über die Arbeit der Komponenten *kavscanner* und *kavsamba* kontrolliert werden, da beim Start jeder Komponente Informationen über die Schlüssel geladen werden.

Daneben verfügt Kaspersky Anti-Virus über eine spezielle Komponente mit dem Namen *licensemanager*, die es ermöglicht, nicht nur ausführlichere Informationen über die Schlüssel, sondern auch bestimmte Zusatzinformationen zu erhalten.

Alle Informationen können auf der Serverkonsole angezeigt werden oder mit Hilfe von Webmin von jedem Remote-Computer Ihres Netzwerks angeschaut werden.



Um Informationen über alle installierten Lizenzschlüssel anzuzeigen,

geben Sie in der Befehlszeile ein:

```
#./kav4samba-licensemanager -s
```

Auf der Serverkonsole werden folgende Informationen angezeigt:

```
Kaspersky license manager Version 5.5  
Copyright (C) Kaspersky Lab. 1997-2006.  
Portions Copyright (C) Lan Crypto  
License file 0003D3EA.key, serial 0038-000419-  
0003D3EA, "Kaspersky Anti-Virus for Unix", expires  
04-07-2003 in 28 days
```



Um Informationen über einen Lizenzschlüssel anzuzeigen,

geben Sie in der Befehlszeile beispielsweise folgende Zeile ein:

```
#./kav4samba-licensemanager -k 00053E3D.key
```

Auf der Serverkonsole werden folgende Informationen angezeigt:

```
Kaspersky license manager Version 5.5  
Copyright (C) Kaspersky Lab. 1997-2006.  
Portions Copyright (C) Lan Crypto  
Serial 0038-000419-0003D3EA, "Kaspersky Anti-Virus  
for Linux", expires 04-07-2003 in 28 days
```

7.1.2. Lizenz verlängern

Die Verlängerung der Lizenz für die Benutzung von Kaspersky Anti-Virus verleiht Ihnen das Recht auf die Wiederherstellung der vollen Funktionalität der Anwendung. Außerdem werden die in Kapitel 7 auf S. 58 genannten Zusatzleistungen erneuert.

Die Gültigkeitsdauer der Lizenz hängt vom Typ der Lizenzierung ab, den Sie beim Erwerb des Produkts gewählt haben.



Um die Lizenz für die Benutzung 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, indem Sie an die Verkaufsabteilung (sales@kaspersky.com) schreiben oder auf unserer Internetseite (www.kaspersky.com/de) im Abschnitt **ONLINE-SHOP → LIZENZVERLÄNGERUNG** das entsprechende Formular **ausfüllen**. Nach Eingang der Bezahlung wird Ihnen der Lizenzschlüssel per E-Mail an die Adresse zugeschickt, die im Bestellformular angegeben wurde.

Der gekaufte Lizenzschlüssel wird mit Hilfe des Tools *licensmanager* installiert (Parameter **LicensePath** in der Konfigurationsdatei der Anwendung).



Um einen neuen Schlüssel zu installieren:

geben Sie in der Befehlszeile beispielsweise folgende Zeile ein:

```
#!/kav4samba-licensmanager -a 00053E3D.key
```

Auf der Serverkonsole werden folgende Informationen angezeigt:

```
Kaspersky license manager. Version 5.5.0/RELEASE  
Copyright (C) Kaspersky Lab. 1998-2006.  
Key file 00053E3D.key is successfully registered
```

Es wird empfohlen, anschließend die Antiviren-Datenbanken zu aktualisieren.

Wenn Sie vor Ablauf der Gültigkeitsdauer des aktiven Lizenzschlüssels einen neuen Schlüssel installieren möchten, können Sie diesen als Reserveschlüssel verwenden. Der Reserveschlüssel beginnt seine Arbeit nach Ablauf der Abonnementsdauer des vorhergehenden. Die Gültigkeitsdauer eines Reserveschlüssels wird ab dem Moment seiner Aktivierung gerechnet.

Der Reserveschlüssel auf die gleiche Weise installiert wie der Hauptschlüssel. Danach werden bei einer Anfrage nach Informationen über den Lizenzschlüssel auf der Konsole sowohl Informationen über den aktiven Schlüssel wie auch über den Reserveschlüssel angezeigt.

7.1.3. Lizenzschlüssel löschen



Um alle installierten Lizenzschlüssel zu löschen,

geben Sie in der Befehlszeile beispielsweise folgende Zeile ein:

```
#./kav4samba-licensemanager -da
```

Auf der Serverkonsole werden folgende Informationen angezeigt:

```
Kaspersky license manager. Version 5.5.0.0/RELEASE  
Copyright (C) Kaspersky Lab. 1998-2006.  
Active key was successfully removed
```



Um einen Reserveschlüssel zu löschen,

geben Sie in der Befehlszeile beispielsweise folgende Zeile ein:


```
#./kav4samba-licensemanager -dr
```

Auf der Serverkonsole werden folgende Informationen angezeigt:

```
Kaspersky license manager. Version 5.5.0.0/RELEASE  
Copyright (C) Kaspersky Lab. 1998-2006.  
Additional key was successfully removed
```

KAPITEL 8. TESTEN DER KORREKTEN FUNKTION VON KASPERSKY ANTI-VIRUS

Wir empfehlen Ihnen, nach der Installation und Konfiguration von Kaspersky Anti-Virus mittels eines "Testvirus" und seinen Modifikationen zu überprüfen, ob die Anwendung richtig eingestellt ist und funktioniert.

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

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



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

Sie können den "Testvirus" von der offiziellen Webseite der Organisation **EICAR** unter http://www.eicar.org/anti_virus_test_file.htm herunterladen. Falls keine Internetverbindung vorhanden ist, können Sie selbst einen "Testvirus" herstellen. Geben Sie dazu in einen beliebigen Texteditor folgende Zeichenkette ein und speichern Sie die Datei unter dem Namen **eicar.com**:

```
X5O!P%@AP[4PZX54(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 des standardmäßigen "Testvirus". 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 "Testvirus", indem Sie eines der Präfixe aus der unten folgenden Tabelle hinzufügen (s. Tabelle 1).



Mit Hilfe des EICAR-"Testvirus" können Sie die korrekte Arbeit von Kaspersky Anti-Virus nur dann testen, wenn Antiviren-Datenbanken vorhanden sind, die nicht vor dem 24.10.2003 datiert sind (kumulatives Update – Oktober 2003).

Tabelle 1. Modifikationen des "Testvirus"

Präfix	Objekttyp
Kein Präfix, standardmäßiger "Testvirus"	Infiziert. Objekt kann nicht desinfiziert werden.
CORR–	Corrupted. Objekt ist beschädigt.
SUSP–	Suspicious (unbekannter Viruscode)
WARN–	Warning (veränderter Code eines bekannten Virus)
ERRO–	Error. Bei der Untersuchung des Objekts ist ein Fehler aufgetreten.
CURE–	Cured. Objekt wird desinfiziert, wobei der Text des "Viruskörpers" in CURED geändert wird.
DELE–	Objekt wird automatisch gelöscht.

In der ersten Spalte der Tabelle sind die Präfixe aufgeführt, die am Anfang der Zeichenkette des standardmäßigen "Testvirus" 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 vorzunehmenden Einstellungen des Antivirenprogramms festgelegt.

KAPITEL 9. MÖGLICHE FRAGEN BEI DER ARBEIT MIT DER ANWENDUNG

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

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

Das wird durch die Verwendung der neuen Technologie iChecker™ ermöglicht. Dabei wird eine Datenbank 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 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 echte und nicht nur scheinbare Antivirensicherheit zu garantieren. Denn ein "teilweiser Schutz" ist schlechter als überhaupt kein Schutz, da der Benutzer im letzten Fall eigene Vorsichtsmaßnahmen treffen wird.

Kaspersky Anti-Virus erlaubt es dem Benutzer, sich in höchstem Maße sicher zu fühlen. Außerdem bietet Kaspersky Anti-Virus erfahrenen Benutzern die Möglichkeit, die Antivirenuntersuchung zu beschleunigen, indem bestimmte Dateitypen von der Antivirenuntersuchung ausgeschlossen werden, wobei aber die Sicherheit in gewisser Hinsicht eingeschränkt wird. Wir raten von dieser Möglichkeit ab, wenn der Benutzer ein Höchstmaß an Sicherheit bevorzugt.

Für den maximalen Schutz der Benutzer erkennt Kaspersky Anti-Virus über 40 Archive und Installationsprogramme und kann Viren in über 350 unterschiedlichen Dateiformaten identifizieren. 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 mit Kaspersky Anti-Virus erkennbaren Viren täglich erhöht (ungefähr 30 neue Viren pro Tag) und die Anzahl der unterstützten Formate ständig steigt. Das wird durch die Verwendung neuer unikalischer Technologien wie iChecker™ erreicht, die von Kaspersky Lab entwickelt wurden. Dabei wird eine Datei nur einmal, und zwar bei der ersten Untersuchung auf Viren untersucht. Bei allen folgenden Untersuchungen wird die Datei nicht mehr untersucht, wenn die Bedingung erfüllt wird, dass sie nicht verändert wurde. Dadurch lässt sich die Leistungsfähigkeit von Kaspersky Anti-Virus nach der ersten Untersuchung einer Datei extrem steigern.



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 Testschlüssel (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. Anti-Virus wird weiterhin die Desinfektion infizierter Objekte durchführen, dabei jedoch die alten Antiviren-Datenbanken benutzen.

Der Download von Antiviren-Datenbanken von der Kaspersky-Lab-Seite wird mit Hilfe von Kaspersky Anti-Virus nicht mehr möglich sein. Selbst wenn versucht wird, die Antiviren-Datenbanken manuell zu kopieren, wird Kaspersky Anti-Virus sie nicht verwenden.

Aus diesem Grund können wir Ihnen für diesen Fall keinen Schutz vor einer Infektion durch neue Viren garantieren.



Frage: Der Lizenzschlüssel für Kaspersky Anti-Virus ist auf einer Diskette gespeichert. Was soll ich tun, wenn mein Computer nicht über ein Diskettenlaufwerk verfügt?

Es bestehen zwei Möglichkeiten zur Lösung dieses Problems

Sie können einen Brief mit einer Problembeschreibung an die Adresse der Verkaufsabteilung von Kaspersky Lab (sales@kaspersky.com) schicken. Geben Sie in diesem Schreiben unbedingt das Datum und den Ort an, an dem Sie Kaspersky Anti-Virus erworben haben. Nennen Sie außerdem die vollständige Registrierungsnummer. Die Mitarbeiter der Verkaufsabteilung werden Ihre Schlüsseldatei an die von Ihnen angegebene E-Mail-Adresse senden.

Außerdem können Sie den Inhalt der Diskette auf einem anderen Computer, der über ein entsprechendes Laufwerk verfügt, lesen und auf einem Datenträger speichern, den Sie auf Ihrem Computer lesen können. Geben Sie bei der Installation von Kaspersky Anti-Virus diesen Datenträger als Quelle des Lizenzschlüssels an.

Eine weitere Möglichkeit besteht darin, den Inhalt der Diskette auf einem anderen Computer, der über ein entsprechendes Laufwerk verfügt, zu speichern und die Schlüsseldatei per E-Mail an Ihre Adresse zu schicken. Nachdem Sie die E-Mail auf Ihrem Computer empfangen haben, speichern Sie die Schlüsseldatei in einer Datei auf Ihrer Festplatte. Bei der Installation von Kaspersky Anti-Virus geben Sie diese Datei als Quelle für den Lizenzschlüssel an.



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

Überprüfen Sie zuerst, ob in der vorliegenden Dokumentation, insbesondere im vorliegenden Kapitel, oder auf unserer Internetseite (**Dienste → Wissensdatenbank/FAQ → Kaspersky Anti-Virus 5.5 for Samba Servers**) eine Lösungsmethode für Ihr Problem enthalten ist.

Außerdem empfehlen wir Ihnen, sich an die Firma zu wenden, bei der Sie Kaspersky Anti-Virus erworben haben, oder einen Brief an den Technischen Supportservice zu schreiben (Das entsprechende Formular finden Sie auf: <http://www.kaspersky.com/de/helpdesk.html>).



Frage: *Kann ein Angreifer die Antiviren-Datenbanken verändern?*

Ein Angreifer kann Antiviren-Datenbanken von der Kaspersky-Lab-Seite herunterladen und sie in den Ordner kopieren, in dem die Antiviren-Datenbanken gespeichert sind. Trotzdem wird Kaspersky Anti-Virus diese Datenbanken nicht bei der Arbeit verwenden.

Alle Antiviren-Datenbanken besitzen eine unikale 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: *Werden folgende Prozessoren mit folgender Architektur unterstützt: PowerPC, SPARC, Alpha, PA-RISC u.a.?*

Diese Prozessorarten werden in der aktuellen Version der Anwendung nicht unterstützt.



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

Kaspersky Anti-Virus Version 5.5 wurde auf Distributionen von RedHat, Debian SuSE und Mandriva getestet und die Distributionen von Kaspersky Anti-Virus wurden speziell für diese erstellt.

Auf Distributionen, die nicht in der Liste der von Kaspersky Lab unterstützten stehen, kann es zu fehlerhafter Arbeit der Anwendung kommen. Dies hängt vor allem mit Besonderheiten des Betriebssystems zusammen. Die Distribution Ihres Systems kann beispielsweise eine andere Bibliotheksversion verwenden oder besitzt einen nicht standardmäßigen Ort für die Skripts zur Systeminitialisierung. In diesem

Fall kann Ihnen der technische Kundendienst von Kaspersky Lab nicht helfen.



Frage: *Wie wird ein Archiv des Typs .tgz oder .tar.gz entpackt?*

Archive des Typs .tgz oder .tar.gz werden durch folgenden Befehl entpackt:

```
tar zxvf <Archivname>
```



Frage: *Kann Kaspersky Anti-Virus durch Network Control Centre for Windows kontrolliert werden?*

Die Verwendung von Network Control Centre for Windows ist bei der Arbeit mit Kaspersky Anti-Virus for Unix nicht möglich. In dieser Version der Anwendung ist die Möglichkeit der Remote-Konfiguration mit Hilfe eines speziellen Moduls des Webmin-Pakets vorgesehen.



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

Eine Lösungsmöglichkeit für dieses Problem sieht folgendermaßen aus: Geben Sie in der Befehlszeile ein:

```
$ 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:

```
$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 A.

ZUSÄTZLICHE ANGABEN ZU DER ANWENDUNG

Dieser Anhang bietet eine Beschreibung der Verzeichnisstruktur der Distribution von Kaspersky Anti-Virus nach der Installation, der Konfigurationsdatei und der Befehlszeilenparameter und ihrer Rückgabewerte. Als Beispiel dient eine Skriptdatei zur Desinfektion von Archiven.

A.1. Konfigurationsdatei von Kaspersky Anti-Virus

Zum Lieferumfang von Kaspersky Anti-Virus gehört die Konfigurationsdatei *kav4sambaservers.conf*, in der die Funktionsparameter der Anwendung enthalten sind. Bei der Beschreibung der Parameter dieser Datei werden die Standardwerte genannt, sofern solche vorgesehen sind.

Der Abschnitt **[path]** enthält Parameter, die den Pfad der wichtigsten Dateien bestimmen, ohne die die Anwendung nicht funktionsfähig ist:

BasesPath – vollständiger Pfad der Antiviren-Datenbanken.

LicensePath – vollständiger Pfad des Ordners für Lizenzschlüssel.

lcheckerDbFile – vollständiger Pfad des Ordners zum Speichern von Datenbanken, die mit Hilfe der iChecker-Technologie untersucht worden sind.

Der Abschnitt **[locale]** enthält Parameter, die das Datums- und Uhrzeitformat bestimmen:

TimeFormat=%H:%M:%S – Anzeigeformat für die Uhrzeit entsprechend strftime.



Sie können als Anzeigeformat für die Uhrzeit den Zwölfstundenthrhythmus (am, pm) wählen: **%I:%M:%S %P**

DateFormat=%d/%m/%y – Anzeigeformat für das Datum entsprechend strftime.



Sie können das Anzeigeformat für das Datum anpassen. Beispielsweise: `%y/%m/%d` oder `%m/%d/%y`.

Der Abschnitt **[samba.options]** enthält Untersuchungsparameter für den Antivirenschutz im Echtzeitmodus:

ExcludeDirs=Maske1:Maske2:....:Maske(n) – Masken der Ordner, die von der Untersuchung ausgeschlossen werden; standardmäßig werden alle Ordner untersucht.

ExcludeMask=Maske1:Maske2:....:Maske(n) – Masken der Dateien, die von der Untersuchung ausgeschlossen werden; standardmäßig werden alle Dateien untersucht.

Packed=yes – Untersuchungsmodus für gepackte Dateien. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

Archives=yes – Untersuchungsmodus für Archive. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

SelfExtArchives=yes – Untersuchungsmodus für selbstextrahierende Archive. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren. Wenn der Untersuchungsmodus für Archive aktiviert ist (**Archives=yes**), werden selbstextrahierende Archive auch dann untersucht, wenn der Parameter **SelfExtArchives** den Wert **no** besitzt.

MailBases=yes – Untersuchungsmodus für Mail-Datenbanken. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

MailPlain=yes – Untersuchungsmodus für E-Mails im Nur-Text-Format. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

Heuristic=yes – Modus zur Verwendung der Heuristischen Code-Analyse während der Untersuchung. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

Cure=no – Modus zur Desinfektion infizierter Objekte. Wählen Sie den Parameterwert **yes**, um den Modus zu aktivieren.

Ichecker=yes – Modus zur Verwendung der Technologie iChecker bei der Antivirenuntersuchung. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

FileCacheSize – Anzahl der Einträge über virusfreie Objekte, die sich im Datei-Cache befinden.

BgCheckFilesLimit – maximale Anzahl von im Hintergrundmodus gleichzeitig zu untersuchenden Objekten. Wenn der Parameter **0** besitzt wird keine Untersuchung im Hintergrundmodus vorgenommen.

BgScheduleTime – Zeitraum, nach dessen Ablauf im Hintergrundmodus die Antivirenuntersuchung einer neuen Datei aus den gemeinsamen Ordnern gestartet wird (in Sek.).

HashType=md5|crc32 – Typ des zu verwendenden Hash. Als Standard gilt der Typ **md5**.

UseAVbasesSet=standard|extended – Typ der Antiviren-Datenbanken, die von der Anwendung verwendet werden. Der Typ **extended** umfasst neben den Einträgen, die im Typ **standard** enthalten sind, auch die Signaturen potentiell gefährlicher Programme wie beispielsweise AdWare, Programme zur Remote-Administration u.a.

Der Abschnitt **[samba.path]** enthält Parameter, die die Pfade der wichtigsten Dateien bestimmen, ohne die die Komponente kavsamba nicht funktioniert:

BackupPath= Pfad – vollständiger Pfad des Ordners zum Speichern von Sicherungskopien der untersuchten Objekte.

SambaConfigFile=Pfad – vollständiger Pfad der Konfigurationsdatei des Samba-Servers.

PidFile=Pfad – vollständiger Pfad der pid-Datei der Komponente kavsamba.

Der Abschnitt **[samba.shares]** enthält Parameter, die die Untersuchungsoptionen für die Dateien in gemeinsamen Ordnern festlegen:

CheckOnOpen – Antivirenuntersuchung einer Datei bei einer Anfrage zum Öffnen.

CheckOnClose – Antivirenuntersuchung einer Datei beim Speichern.

Abschnitte der Form **[samba.shares:SHARENAME]** können in der Konfigurationsdatei erstellt werden und enthalten die Parameter, die die Optionen für den Antivirenschutz eines bestimmten gemeinsamen Ordners bestimmen (beispielsweise des Ordners **SHARENAME**):

CheckOnOpen – Antivirenuntersuchung einer Datei bei einer Anfrage zum Öffnen.

CheckOnClose – Antivirenuntersuchung einer Datei beim Speichern.



Wenn Sie individuelle Schutzparameter für einen gemeinsamen Ordner festgelegt haben und Kaspersky Anti-Virus wurde nicht gestartet, dann wird der Zugriff auf diesen Ordner gesperrt.

Der Abschnitt **[samba.actions]** enthält Parameter, die die Aktionen für Objekte der einzelnen Typen festlegen:

OnInfected=Aktion – Aktionen im Fall des Funds einer infizierten Datei. Wenn der Desinfektionsmodus für infizierte Dateien aktiviert ist, wird diese Aktion auf Objekte angewandt, deren Desinfektion fehlgeschlagen ist.

OnSuspicion=Aktion – Aktionen im Fall des Funds einer verdächtigen Datei, deren Code dem Code eines Virus ähnelt, der bisher nicht bei Kaspersky Lab bekannt ist.

OnWarning=Aktion – Aktionen im Fall des Funds einer Datei, deren Code dem Code eines bekannten Virus ähnelt.

OnCured=Aktion – Aktionen im Fall des Funds und der erfolgreichen Desinfektion eines infizierten Objekts.

OnProtected=Aktion – Aktionen im Fall des Funds eines Objekts, das durch Kennwort verschlüsselt ist. Solche Objekte können nicht untersucht werden.

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

OnError=Aktion – Aktionen für den Fall des Auftretens eines Systemfehlers während der Untersuchung eines Objekts.

Die Syntax des Parameters **Aktion** besteht aus zwei Teilen: die eigentliche Aktion und ihr Zusatzparameter, die durch Leerzeichen getrennt werden. Der Wert des Zusatzparameters steht in Klammern. Beispiel: **OnInfected=move /tmp/infected**

Die Aktion kann einen der folgenden Werte besitzen:

- *move* <Ordner> – Datei in den <Ordner> verschieben.
- *movePath* <Ordner> – Datei rekursiv (mit absolutem Pfad) in den <Ordner> verschieben.
- *remove* – Datei löschen.
- *exec* <Parameter> – Die durch den Wert <Parameter> festgelegte Aktion mit dem Objekt ausführen.

Als Makros für den Zusatzparameter einer Aktion stehen zur Verfügung:

- %VIRUSNAME% – Name des gefundenen Virus.
- %FULLPATH% – vollständiger Pfad eines Ordners.
- %FILENAME% – Dateiname ohne Pfad.

Der Abschnitt **[samba.notify]** enthält Parameter, für den Fall eines bestimmten Objekttyps das Senden von Benachrichtigungen festlegen:

OnInfected=Aktion – Benachrichtigung beim Fund einer infizierten Datei.

OnSuspicion=Aktion – Benachrichtigung beim Fund einer verdächtigen Datei, deren Code dem Code eines Virus ähnelt, der bisher nicht bei Kaspersky Lab bekannt ist.

OnWarning=Aktion – Benachrichtigung beim Fund einer Datei, deren Code dem Code eines bekannten Virus ähnelt.

OnCured=Aktion – Benachrichtigung beim Fund und Desinfektion eines infizierten Objekts.

OnProtected=Aktion – Benachrichtigung beim Fund eines Objekts, das durch Kennwort verschlüsselt ist. Solche Objekte können nicht untersucht werden.

OnCorrupted=Aktion – Benachrichtigung beim Fund einer beschädigten Datei.

OnError=Aktion – Benachrichtigung für den Fall des Auftretens eines Systemfehlers während der Untersuchung eines Objekts.

Die Aktion kann einen der folgenden Werte besitzen:

- *move* <Ordner> – Datei in den <Ordner> verschieben.
- *movePath* <Ordner> – Datei rekursiv (mit absolutem Pfad) in den <Ordner> verschieben.
- *remove* – Datei löschen.
- *exec* <Parameter> – Die durch den Wert <Parameter> festgelegte Aktion mit dem Objekt ausführen.

Als Makros für den Zusatzparameter einer Aktion stehen zur Verfügung:

- %USER% – Name des Benutzers, der die Datei angefordert hat.
- %USERIP% – IP des Benutzers, der die Datei angefordert hat.
- %USERHOST% – Host des Benutzers, von dem die Datei angefordert wurde.
- %VIRUSNAME% – Name des gefundenen Virus.
- %FULLPATH% – vollständiger Pfad eines Ordners.
- %FILENAME% – Dateiname ohne Pfad.

Der Abschnitt [**samba.report**] enthält Parameter für die Berichtsführung über die Arbeitsergebnisse der Komponente kavsamba:

ReportFileName – Name der Berichtsdatei, in der die Arbeitsergebnisse der Komponente gespeichert werden.

ReportMaxSize – Größe der Berichtsdatei (in Byte).

ReportLevel – Ausführlichkeitsstufe des Berichts.

Append=yes – Modus zum Hinzufügen neuer Meldungen in die Berichtsdatei. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

ShowOK=yes – Modus zur Anzeige von Meldungen über virusfreie Dateien im Bericht. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

Der Abschnitt **[scanner.options]** enthält Parameter für die Untersuchung der Serverdateisysteme:

ExcludeDirs=Maske1:Maske2:...:Maske(n) – Masken der Ordner, die von der Untersuchung ausgeschlossen werden; standardmäßig werden alle Ordner untersucht.

ExcludeMask=Maske1:Maske2:...:Maske(n) – Masken der Dateien, die von der Untersuchung ausgeschlossen werden; standardmäßig werden alle Dateien untersucht.

Packed=yes – Untersuchungsmodus für gepackte Dateien. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

Archives=yes – Untersuchungsmodus für Archive. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

SelfExtArchives=yes – Untersuchungsmodus für selbstextrahierende Archive. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren. Wenn der Untersuchungsmodus für Archive aktiviert ist (**Archives=yes**), werden selbstextrahierende Archive auch dann untersucht, wenn der Parameter **SelfExtArchives** den Wert **no** besitzt.

MailBases=yes – Untersuchungsmodus für Mail-Datenbanken. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

MailPlain=yes – Untersuchungsmodus für E-Mails im Nur-Text-Format. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

Heuristic=yes – Modus zur Verwendung der Heuristischen Code-Analyse während der Untersuchung. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

Recursion=yes – Modus zur rekursiven Behandlung von Ordnern bei der Virenuntersuchung. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

Ichecker=yes – Modus zur Verwendung der Technologie iChecker bei der Antivirenuntersuchung. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

Cure=no – Modus zur Desinfektion infizierter Objekte. Wählen Sie den Parameterwert **yes**, um den Modus zu aktivieren.

UseAVbasesSet=standard|extended – Typ der Antiviren-Datenbanken, die von der Anwendung verwendet werden. Der Typ **extended** umfasst neben den Einträgen, die im Typ **standard** enthalten sind, auch die Signaturen potentiell gefährlicher Programme wie beispielsweise AdWare, Programme zur Remote-Administration u.a.

FollowSymlinks – Modus für die Arbeit mit symbolischen Links. Wenn der Parameter den Wert **yes** besitzt, werden alle symbolischen Links verfolgt. Wenn der Parameter den Wert **no** besitzt, werden symbolische Links zu Verzeichnissen nicht verfolgt.

MaxLoadAvg – Parameter, der als Zahlenwert die Stufe der Serverauslastung angibt. Wenn die Auslastung den festgelegten Wert überschreitet, wird die Antivirenuntersuchung vorübergehend angehalten. Die Untersuchung wird wieder fortgesetzt, wenn die Serverauslastung auf den festgelegten Wert sinkt.

Der Abschnitt **[scanner.path]** enthält einen Parameter, der wichtigsten Dateien bestimmen, ohne die die Komponente kavscanner nicht funktioniert:

BackupPath= Pfad – vollständiger Pfad des Ordners zum Speichern von Sicherungskopien der untersuchten Objekte.

Der Abschnitt **[scanner.object]** enthält Parameter, die die Aktionen festlegen, die bei der Antivirenuntersuchung der Dateisysteme für gewöhnliche Objekte der einzelnen Typen gelten:

OnInfected=Aktion – Aktionen im Fall des Funds einer infizierten Datei. Wenn der Desinfektionsmodus für infizierte Dateien aktiviert ist, wird diese Aktion auf Objekte angewandt, deren Desinfektion fehlgeschlagen ist.

OnSuspicion=Aktion – Aktionen im Fall des Funds einer verdächtigen Datei, deren Code dem Code eines Virus ähnelt, der bisher nicht bei Kaspersky Lab bekannt ist.

OnWarning=Aktion – Aktionen im Fall des Funds einer Datei, deren Code dem Code eines bekannten Virus ähnelt.

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

OnCured=Aktion – Aktionen im Fall des Funds und der erfolgreichen Desinfektion eines infizierten Objekts.

OnProtected=Aktion – Aktionen im Fall des Funds eines Objekts, das durch Kennwort verschlüsselt ist. Solche Objekte können nicht untersucht werden.

OnError=Aktion – Aktionen für den Fall des Auftretens eines Systemfehlers während der Untersuchung eines Objekts.

Die Syntax des Parameters **Aktion** besteht aus zwei Teilen: die eigentliche Aktion und ihr Zusatzparameter, die durch Leerzeichen getrennt werden. Der Wert des Zusatzparameters steht in Klammern. Beispiel: **OnInfected=move /tmp/infected**

Die Aktion kann einen der folgenden Werte besitzen:

- *move* <Ordner> – Datei in den <Ordner> verschieben.
- *movePath* <Ordner> – Datei rekursiv (mit absolutem Pfad) in den <Ordner> verschieben.
- *remove* – Datei löschen.
- *exec* <Parameter> – Die durch den Wert <Parameter> festgelegte Aktion mit dem Objekt ausführen.

Als Makros für den Zusatzparameter der Aktion **exec** stehen für Container zur Verfügung:

- %LIST% – Name der Datei oder der Liste mit infizierten, verdächtigen und beschädigten Dateien, die in einem Container gefunden wurden. Die Datei besitzt folgendes Format: **<Virusname>|t<Dateiname>**.
- %FULLPATH% – vollständiger Pfad des Containers.
- %FILENAME% – Dateiname ohne Pfad.
- %CONTAINERTYPE% – Typ des Containers in Zeilenform.

Der Abschnitt **[scanner.container]** enthält Parameter, die die Aktionen für festlegen, die bei der Antivirenuntersuchung der Dateisysteme für Archive gelten:

OnCorrupted=Aktion – Aktionen im Fall des Funds einer beschädigten Containers.

OnInfected=Aktion – Aktionen im Fall des Funds eines infizierten Objekts in einem Container. Wenn der Desinfektionsmodus für infizierte Dateien aktiviert ist, wird diese Aktion auf Container angewandt, deren Desinfektion fehlgeschlagen ist, und wird ausgeführt, nachdem alle Aktionen mit den Container-Objekten ausgeführt wurden.

OnSuspicion=Aktion – Aktionen im Fall des Funds eines verdächtigen Objekts in einem Container.

OnWarning=Aktion – Aktionen im Fall des Funds eines verdächtigen Objekts (deren Code dem Code eines bekannten Virus ähnelt) in einem Container.

OnCured=Aktion – Aktionen im Fall des Funds und der erfolgreichen Desinfektion eines infizierten Objekts in einem Container.

OnProtected=Aktion – Aktionen im Fall des Funds eines Objekts, das durch Kennwort verschlüsselt ist, in einem Container. Solche Objekte können nicht untersucht werden.

OnError=Aktion – Aktionen für den Fall des Auftretens eines Systemfehlers während der Untersuchung eines Containers.

Die Syntax der Aktionen für alle genannten Objekttypen entspricht der Beschreibung, die oben im Abschnitt **[scanner.object]** gegeben wird.

Der Abschnitt **[scanner.report]** enthält Parameter für die Berichtsführung über die Arbeitsergebnisse der Komponente kavscanner:

ReportFileName – Name der Berichtsdatei, in der die Arbeitsergebnisse der Komponente gespeichert werden.

ReportLevel=4 – Ausführlichkeitsstufe des Berichts.

Append=yes – Modus zum Hinzufügen neuer Meldungen in die Berichtsdatei. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

ShowOK=yes – Modus zur Anzeige von Meldungen über virusfreie Dateien im Bericht. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

ShowContainerResultOnly=no – Modus zur Berichtsanzeige der Untersuchungsergebnisse für Archive in Kurzform. Wählen Sie den Parameterwert **yes**, damit die Kurzform für den Bericht verwendet wird.

ShowObjectResultOnly=no – Modus zur Berichtsanzeige der Untersuchungsergebnisse für gewöhnliche Objekte in Kurzform. Wählen Sie den Parameterwert **yes**, damit die Kurzform verwendet wird.

Der Abschnitt **[updater.path]** enthält Parameter, die die Pfade bestimmen, die für die Arbeit der Komponente zum Update der Antiviren-Datenbanken erforderlich sind:

AVBasesTestPath – vollständiger Pfad des Ordners zum Speichern der Antiviren-Datenbanken.

BackUpPath – vollständiger Pfad des Ordners zum Speichern der Sicherungskopien der Antiviren-Datenbanken.

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

UseUpdateServerUrl=no – Modus zur Verwendung der Adresse, die durch den Parameter **UpdateServerUrl** bestimmt wird, beim Update.

UseUpdateServerUrlOnly=no – Modus, in dem zum Update der Antiviren-Datenbanken nur die Adresse verwendet wird, die im Parameter **UpdateServerUrl** angegeben ist. Wenn diese Option den Wert **no** besitzt, dann wird bei erfolglosem Updateversuch der Datenbanken von der Adresse **UpdateServerUrl** eine andere Adresse aus der Liste der Updateserver benutzt.

PostUpdateCmd – Befehl, der sofort nach dem erfolgreichen Abschluss des Updates der Antiviren-Datenbanken ausgeführt werden soll. Der in der Konfigurationsdatei, die im Lieferumfang der Anwendung enthalten ist, festgelegt ist, startet automatisch das erneute Einlesen der von der

Anwendung aktualisierten Antiviren-Datenbanken. Es wird davor gewarnt, diesen Parameter zu ändern.

RegionSettings=ru – Ländereinstellungen des Benutzers (die zwei ersten Buchstaben der Landesbezeichnung). Dieser Wert wird zur Optimierung des Downloads der Antiviren-Datenbanken von einem Kaspersky-Lab-Updateserver verwendet.

ConnectTimeout=30 – Zeitlimit für das Update der Datenbanken (in Sekunden). Wenn während des Downloads von Datenbanken innerhalb des angegebenen Zeitlimits keine Daten vom Server eingehen, wird ein anderer Server aus der Liste der Kaspersky-Lab-Updateserver ausgewählt.

UseProxy – Modus zur Verwendung eines Proxyserver bei der Verbindung mit dem Kaspersky-Lab-Updateserver. Wenn der Parameter den Wert **no** besitzt, wird kein Proxyserver verwendet. Wenn der Parameter den Wert **yes** besitzt, wird die Proxyserveradresse verwendet, die vom Parameter **ProxyAddress** bestimmt wird. Wenn für den Parameter **ProxyAddress** kein Wert vorhanden ist, wird der Wert der Umgebungsvariablen **http_proxy** verwendet. Wenn für die Umgebungsvariable kein Wert festgelegt wurde, wird kein Proxyserver verwendet.

ProxyAddress – Adresse des für die Verbindung zu verwendenden Proxyserver. Der Parameter wird in der Form **http://username:password@url:port** angegeben. Die Elemente **username** und/oder **password** sind in der Proxyserveradresse optional. Wenn keine Adresse angegeben wird, wird der Wert aus der Umgebungsvariablen **http_proxy** verwendet.

Der Abschnitt **[updater.report]** enthält Parameter für die Berichtsführung über die Arbeitsergebnisse der Komponente keepup2date:

Append=yes – Modus zum Hinzufügen neuer Meldungen in die Berichtsdatei. Wählen Sie den Parameterwert **no**, um den Modus zu deaktivieren.

ReportFileName – Name der Berichtsdatei, in der die Arbeitsergebnisse der Komponente gespeichert werden.

ReportLevel=4 – Ausführlichkeitsstufe des Berichts.

A.2. Befehlszeilenschlüssel der Komponente kavsamba

Die Parameter der Konfigurationsdatei können beim Start des Programms mit Hilfe von Befehlszeilenschlüsseln aus der Befehlszeile geändert werden.

Optionen für die Hilfe:	
-h	Hilfe-Informationen über die Komponente kavsamba auf der Konsole anzeigen.
-v	Programmversion anzeigen.
Konfigurationsoptionen:	
-c (-y) <Pfad_der_Datei>	Die alternative Konfigurationsdatei <Pfad_der_Datei> verwenden.

A.3. Rückgabewerte der Komponente kavsamba

Bei der Arbeit kann die Komponente kavsamba folgende Werte zurückgeben:

0	Die Komponente wurde gestartet.
64	Lizenzinformationen fehlen oder unter dem in der Konfigurationsdatei angegebenen Pfad wurde keine Lizenzdatei gefunden.
65	Das Laden der Konfigurationsdatei ist fehlgeschlagen.
70	Die Komponente kavsamba ist beschädigt.

A.4. Befehlszeilenschlüssel der Komponente kavscanner

Die Parameter der Konfigurationsdatei können beim Start des Programms mit Hilfe von Befehlszeilenschlüsseln aus der Befehlszeile geändert werden.

Optionen für die Hilfe:	
-h	Hilfe-Informationen über die Komponente kavscanner auf der Konsole anzeigen.
-v	Programmversion anzeigen.
Konfigurationsoptionen:	
-c (-C) <Pfad_der_Datei>	Die alternative Konfigurationsdatei <Pfad_der_Datei> verwenden.
-g<Pfad_der_Datei>	Eine Liste aller bekannten Viren, die in den Antiviren-Datenbanken eingetragen sind, in der Datei <Pfad_der_Datei> speichern.
-f	Die beschädigte Signatur der Komponente kavscanner ignorieren und versuchen, die Komponente zu reparieren.
Untersuchungsoptionen:	
-e <Option>	Die standardmäßig verwendete Untersuchungsoption ändern. Als <Option> können folgende Modi verwendet werden:
P/p	Die Untersuchung gepackter Dateien aktivieren/deaktivieren.
A/a	Die Untersuchung von Archiven aktivieren/deaktivieren.
S/s	Die Untersuchung selbstextrahierender Archive aktivieren/deaktivieren (Um den Modus zur Untersuchung selbstextrahierender Archive auszuschalten, muss auch die Untersuchung von Archiven deaktiviert sein).

B/b	Die Untersuchung von Mail-Datenbanken aktivieren/deaktivieren.
M/m	Die Untersuchung von E-Mails im Nur-Text-Format aktivieren/deaktivieren.
E/e	Die Heuristische Code-Analyse aktivieren/deaktivieren.
-R/r	Die rekursive Untersuchung aktivieren/deaktivieren.
-S/s	Den Modus zum Öffnen symbolischer Links aktivieren/deaktivieren.
-l	Nur lokale Dateisysteme untersuchen.
Optionen für die Berichtsführung:	
-q	Keine Meldungen an der Konsole anzeigen.
-o <Name>	Angabe des Namens der Datei, in der der Bericht über die Arbeit der Komponente gespeichert werden soll. Wenn kein Dateiname angegeben wird, wird kein Bericht erstellt.
-j<Zahl>	Angabe der Ausführlichkeitsstufe für den Bericht. Der Wert bezieht sich auf die im Bericht enthaltenen Informationen. Als <Zahl> kann eine der folgenden Ausführlichkeitsstufen dienen:
1	Meldungen über sonstige Fehler anzeigen bzw. nicht anzeigen.
2	Infomeldungen anzeigen bzw. nicht anzeigen.
3	Meldungen über die Untersuchung anzeigen bzw. nicht anzeigen.
10	Meldungen mit Debug-Infos anzeigen bzw. nicht anzeigen.
-x<Option>	Angabe der Ausführlichkeitsstufe für den Untersuchungsbericht, der an der Konsole angezeigt werden soll. Als <Option> kann eine der folgenden Ausführlichkeitsstufen dienen:
O/o	Kurzes/erweitertes Format der Meldungen über die

	Untersuchung eines gewöhnlichen Objekts.
C/c	Kurzes/erweitertes Format der Meldungen über die Untersuchung eines Archivs.
N/n	Die Bildschirmanzeige von Meldungen über virusfreie Dateien aktivieren/deaktivieren.
P/p	Die Anzeige von Informationen über die laufende Arbeit der Komponente auf der Konsole aktivieren/deaktivieren.
-m<Option>	Angabe der Ausführlichkeitsstufe für den Untersuchungsbericht, der in der Berichtsdatei gespeichert werden soll. Als <Option> kann eine der folgenden Ausführlichkeitsstufen dienen:
O/o	Kurzes/erweitertes Format der Meldungen über die Untersuchung eines gewöhnlichen Objekts.
C/c	Kurzes/erweitertes Format der Meldungen über die Untersuchung eines Archivs.
N/n	Das Speichern von Meldungen über virusfreie Dateien in der Berichtsdatei aktivieren/deaktivieren.
Optionen für Dateien:	
-p<Option> <Dateiname>	Eine Liste der Objekte in der angegebenen Datei speichern. Jedes Objekt mit vollständigem Pfad in einer extra Zeile speichern. Als <Option> können dienen:
i	Liste der infizierten Objekte in der Datei <Dateiname> speichern.
s	Liste der verdächtigen Objekte in der Datei <Dateiname> speichern.
c	Liste der beschädigten Objekte in der Datei <Dateiname> speichern.
w	Liste der Objekte, deren Code dem Code bekannter Viren ähnelt, in der Datei <Dateiname> speichern.
-@ <filelist.lst>	Die Objekte untersuchen, deren Pfad in der Datei

	<filelist.lst> genannt ist.
Optionen für die Bearbeitung von Dateien (Wenn diese Parameter in der Befehlszeile bestimmt werden, werden dadurch die in der Konfigurationsdatei angegebenen Werte ersetzt):	
-i0	Nur auf das Vorhandensein von Viren untersuchen.
-i1	Infizierte Objekte desinfizieren. Irreparable Objekte werden übersprungen.
-i2	Infizierte Objekte desinfizieren. Gewöhnliche irreparable Objekte werden gelöscht. Wenn sich das irreparable Objekt in einem Container befindet, es aus dem Container gelöscht.
-i3	Infizierte Objekte desinfizieren. Gewöhnliche irreparable Objekte werden gelöscht. Wenn sich das irreparable Objekt in einem Container befindet, wird der ganze Container gelöscht.
-i4	Infizierte Objekte und Container löschen.

A.5. Rückgabewerte der Komponente kavscanner

Bei der Arbeit kann die Komponente kavscanner folgende Werte zurückgeben:

0	Es wurden keine Viren gefunden.
5	Alle infizierten Objekte wurden desinfiziert.
10	Es wurden kennwortgeschützte Archive gefunden.
15	Es wurden beschädigte Dateien gefunden.
20	Es wurden verdächtige Dateien gefunden.
21	Es wurden Dateien gefunden, deren Code dem Code bekannter Viren ähnelt.
25	Es wurden infizierte Dateien gefunden.

30	Bei der Untersuchung von Dateien ist ein Systemfehler aufgetreten.
50	Das Laden der Antiviren-Datenbanken ist fehlgeschlagen (Der in der Konfigurationsdatei angegebene Pfad wurde nicht gefunden).
55	Die Antiviren-Datenbanken sind beschädigt.
60	Das Datum der Antiviren-Datenbanken liegt außerhalb der Gültigkeitsdauer des Lizenzschlüssels.
64	Lizenzinformationen fehlen oder unter dem in der Konfigurationsdatei angegebenen Pfad wurde keine Lizenzdatei gefunden.
65	Das Laden der Konfigurationsdatei ist fehlgeschlagen.
66	Ungültige Option der Konfigurationsdatei.
70	Die Komponente kavscanner ist beschädigt.
75	Die Komponente kavscanner ist beschädigt und kann nicht desinfiziert werden.

A.6. Befehlszeilenschlüssel der Komponente *licensmanager*

Optionen für die Hilfe:	
-h	Hilfe-Informationen über die Komponente <i>licensmanager</i> auf der Konsole anzeigen.
-v	Programmversion anzeigen.
Optionen für die Arbeit mit Lizenzschlüsseln:	
-s	Informationen über alle installierten Lizenzschlüssel auf der Konsole anzeigen.
-c (-C)	Die alternative Konfigurationsdatei

<Pfad_der_Datei>	<Pfad_der_Schlüsseldatei> verwenden.
-k <Pfad_der_Datei>	Informationen über den Schlüssel <Pfad_der_Schlüsseldatei> auf der Konsole anzeigen.
-a <Pfad_der_Datei>	Den Lizenzschlüssel <Pfad_der_Schlüsseldatei> installieren.
-d <a r>	Alle Lizenzschlüssel löschen/ den Reserve-Lizenzschlüssel löschen.

A.7. Rückgabewerte der Komponente licensemanager

Bei der Arbeit kann die Komponente licensemanager folgende Werte zurückgeben:

0	Die Komponente hat erfolgreich Informationen über einen Lizenzschlüssel geladen und seine Arbeit abgeschlossen.
30	Bei der der Komponente ist ein Systemfehler aufgetreten.
64	Lizenzinformationen fehlen oder unter dem in der Konfigurationsdatei angegebenen Pfad wurde keine Lizenzdatei gefunden.
65	Das Laden der Konfigurationsdatei ist fehlgeschlagen.
66	Ungültige Option der Konfigurationsdatei.

A.8. Befehlszeilenschlüssel der Komponente keepup2date

Optionen für die Hilfe:	
-v	Anwendungsversion auf der Konsole anzeigen und die Arbeit der Komponente beenden.

-h	Hilfe-Informationen über von der Komponente unterstützte Befehlszeilenparameter auf der Konsole anzeigen und die Arbeit der Komponente beenden.
-s	Eine vollständige Liste der Updateserver mit dem Ländercode auf der Konsole anzeigen.
Funktionsoptionen:	
-r	Rückkehr vom letzten Update zu der vorhergehenden Version.
-k	Den Befehl PostUpdateCmd nach dem erfolgreichen Abschluss des Updates der Antiviren-Datenbanken nicht ausführen.
-q	Modus für die Arbeit der Komponente, in dem auf der Konsole keine Systemmeldungen angezeigt werden.
-e	Modus für die Arbeit der Komponente, in dem auf der Konsole nur Meldungen über kritische Systemfehler angezeigt werden.
-b <Pfad>	Beim Update im Ordner <Pfad> eine Kopie der vorhandenen Antiviren-Datenbanken anlegen.
-x <Pfad_der_Datei>	Alle Updates der Antiviren-Datenbanken in den lokalen Ordner <Pfad_der_Datei> kopieren.
-t <Pfad>	Den Ordner <Pfad> zum Speichern von temporären Dateien verwenden.
-u <Pfad_der_Datei>	Das letzte Update der Antiviren-Datenbanken in den lokalen Ordner <Pfad_der_Datei> kopieren.
-c <Pfad_der_Datei>	Die alternative Konfigurationsdatei <Pfad_der_Datei> verwenden. Dieser Schlüssel funktioniert, wenn auf dem Server nur eine Kaspersky-Lab-Anwendung installiert ist oder wenn die zu aktualisierende Anwendung durch den Schlüssel -p festgelegt wird (Andernfalls wird eine Systemmeldung über mehrere installierte Anwendungen angezeigt).

-g <URL>	Adresse für das Update der Antiviren-Datenbanken. Bei Angabe dieses Schlüssels wird das Update von der festgelegten Adresse vorgenommen.
-d <Pfad_der_Datei>	Verwendung der pid-Datei der Anwendung, die sich im lokalen Ordner <Pfad_der_Datei> befindet.
Optionen die Berichtsführung:	
-l <Pfad_der_Datei>	Die Arbeitsergebnisse der Komponente in der Datei <Pfad_der_Datei> speichern.

A.9. Rückgabewerte der Komponente `keepup2date`

Bei der Arbeit kann die Komponente `keepup2date` folgende Werte zurückgeben:

0	Das Update der Antiviren-Datenbanken ist nicht erforderlich.
1	Das Update der Antiviren-Datenbanken wurde erfolgreich ausgeführt.
10	Ein kritischer Fehler ist aufgetreten. Der Updatevorgang wird abgebrochen.
12	Bei der Rückkehr zur letzten Version des Updates der Antiviren-Datenbanken ist ein Fehler aufgetreten.
30	Der Befehl PostUpdateCmd konnte nach dem Update der Datenbanken nicht gestartet werden.
60	Lizenzinformationen fehlen oder unter dem in der Konfigurationsdatei angegebenen Pfad wurde keine Lizenzdatei gefunden.
75	Das Laden der Konfigurationsdatei ist fehlgeschlagen oder es ist ein Fehler in den Parametern der Konfigurationsdatei aufgetreten.

ANHANG B. KASPERSKY LAB

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

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

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

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

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

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

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

B.1. Andere Produkte von Kaspersky Lab

Kaspersky Anti-Virus® Personal

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

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

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

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

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

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

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

Kaspersky Anti-Virus® Personal Pro

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

Kaspersky Anti-Virus® Personal Pro bietet:

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

Kaspersky® Anti-Hacker

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

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

entsprechende Anwendung, so dass die auf dem Computer gespeicherten Daten geschützt bleiben.

Durch Verwendung der SmartStealth™-Technologie wird das Aufspüren des Computers von außerhalb erheblich erschwert: da der Computer unsichtbar bleibt, ist er vor Hackerangriffen geschützt, ohne dass jedoch Ihre eigene Kommunikations- und Arbeitsfähigkeit über das Internet beeinträchtigt wird. Das Programm gewährleistet angemessenen Schutz aber auch den standardmäßigen Zugriff auf die Daten des Computers.

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

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

Kaspersky® Personal Security Suite

Kaspersky® Personal Security Suite ist ein Programmkomplex, welcher der Organisation des umfassenden Schutzes eines PCs unter dem Betriebssystem Microsoft Windows dient. Der Komplex verhindert das Eindringen von schädlichen und potentiell gefährlichen Programmen über alle möglichen Quellen, gewährleistet den Schutz vor Versuchen zum unerlaubten Zugriff auf Daten des Computers und schützt vor Spam.

Kaspersky® Personal Security Suite verfügt über folgende Funktionen:

- Antivirenschutz der Daten, die auf dem Computer gespeichert sind.
- Schutz der Benutzer der Mail-Clients Microsoft Office Outlook und Microsoft Outlook Express vor unerwünschten E-Mails (Spam).
- Schutz des Computers vor unerlaubtem Datenzugriff sowie Schutz vor Netzwerkangriffen aus dem lokalen Netzwerk oder Internet.

Kaspersky Lab News Agent

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

News Agent verfügt außerdem über folgende Funktionen:

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

News Agent funktioniert unter dem Betriebssystem Microsoft Windows. Er kann als separates 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. 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 den Formaten txt und html in Berichten speichern.

Kaspersky® OnLine Scanner Pro

Dieses Programm stellt einen Abonnementsdienst dar, der den Besuchern der Hersteller-Webseite zur Verfügung steht und die effektive Antivirenuntersuchung des Computers und die Desinfektion infizierter Dateien im Online-Modus erlaubt. Kaspersky OnLine Scanner Pro wird direkt im Webbrowser ausgeführt. 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 den Formaten txt und html in Berichten speichern.

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

Der Proaktive Schutz umfasst:

- **Kontrolle über Veränderungen im Dateisystem.** Das Programm erlaubt es, eine Liste der Anwendungen anzulegen, deren Komponentenbestand kontrolliert werden soll. Dadurch lässt sich die Verletzung der Integrität von Anwendungen durch Schadprogramme verhindern.
- **Überwachung von Prozessen im Arbeitsspeicher.** Kaspersky Anti-Virus 6.0 warnt den Benutzer rechtzeitig, wenn gefährliche, verdächtige oder versteckte Prozesse auftreten oder wenn normale Prozesse auf unerlaubte Weise verändert werden.
- **Überwachung von Veränderungen in der Registrierung des Betriebssystems** 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® Internet Security 6.0

Kaspersky® Internet Security 6.0 ist eine komplexe Lösung für den Schutz eines Personalcomputers vor den wichtigsten Bedrohungen (Viren, Hackerangriffe, Spam und Spyware), denen Informationen unterliegen. Alle Komponenten lassen sich über eine einheitliche Benutzeroberfläche einstellen und steuern.

Die Funktion des Antivirenschutzes 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. Für die populären Mailprogramme Microsoft Office Outlook, Microsoft Outlook Express und The Bat! sind Plugins und die Desinfektion von Mail-Datenbanken vorgesehen.
- **Antivirenuntersuchung des Internet-Datenstroms**, der mit HTTP-Protokoll eintrifft, im Echtzeitschutz-Modus.
- **Schutz des Dateisystems:** Der Antivirenuntersuchung können beliebige einzelne Dateien, Ordner und Laufwerke unterzogen werden. Außerdem sind vordefinierte Untersuchungsaufgaben für die Virenanalyse von kritischen Bereichen des Betriebssystems und von Objekten, die beim Start des Betriebssystems Microsoft Windows gestartet werden, vorhanden.
- **Proaktiver Schutz:** Das Programm führt die ununterbrochene Überwachung der Aktivität von Anwendungen und Prozessen durch, die im Arbeitsspeicher des Computers gestartet werden, verhindert gefährliche Veränderungen des Dateisystems und der Registrierung, und stellt das System nach schädlicher Einwirkung wieder her.

Der **Schutz vor Internetbetrug** beruht auf dem Erkennen von Phishing-Angriffen. Dadurch lässt sich der Diebstahl Ihrer vertraulichen Informationen verhindern (in erster Linie Kennwörter, Konto- und Kreditkartennummern, sowie Sperren der Ausführung gefährlicher Skripts auf Webseiten, Sperren von Pop-up-Fenstern und Werbeflächern). Die Funktion zum **Sperren der Einwahl auf kostenpflichtige Telefonnummern** ermöglicht es, Programme zu identifizieren, die versuchen Ihr Modem für versteckte Verbindungen mit kostenpflichtigen Telefondiensten zu missbrauchen, indem diese Programme gesperrt werden.

Kaspersky® Internet Security 6.0 **erkennt Versuche zum Scannen der Ports Ihres Computers**, die häufig Netzwerkangriffe ankündigen. Auf der **Basis von vordefinierten Regeln** führt das Programm die Kontrolle aller Netzwerkaktionen durch und überwacht alle **eingehenden und ausgehenden Datenpakete**. Der **Stealth-Modus** (SmartStealth™-Technologie) **macht den Computer für die externe Umgebung praktisch unsichtbar**. In diesem Modus wird jede

Netzwerkaktivität verboten, wenn sie nicht durch Ausnahmeregeln erlaubt wird, die vom Benutzer festgelegt wurden.

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

- Untersuchung nach Blacklists (gesperrte Mailinhalte) und Whitelists (freigegrabene Mailinhalte)
- Phrasenuntersuchung im Mail-Text
- Analyse des Mail-Texts mit Hilfe eines lernfähigen Algorithmus
- Erkennung von Spam in Bilddateien

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 Erweiterungsspeichern, 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 des Zugriffs auf das Gerät selbst wie auch auf die im Speicher des PDA und auf Speicherkarten enthaltenen Daten.

Kaspersky Anti-Virus Mobile

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

- **Scan auf Befehl** des Arbeitsspeichers eines mobilen Geräts, der Speicherkarten, einzelner Ordner oder einer konkreten Datei. Beim Fund eines infizierten Objekts wird es in die Quarantäne verschoben oder gelöscht.

- **Echtzeituntersuchung:** Alle eingehenden und veränderten Objekte, sowie Dateien, auf die versucht wird zuzugreifen, werden automatisch untersucht.
- **Untersuchung nach Zeitplan:** Die Informationen, die im Arbeitsspeicher eines mobilen Geräts gespeichert sind, können untersucht werden.
- **Schutz vor sms- und mms-Spam.**

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 Linux; *Dateispeicher* unter Samba.
- *Mailsysteme* vom Typ Microsoft Exchange 2000/2003, Lotus Notes/Domino, postfix, exim, sendmail und qmail.
- *Internet-Firewalls:* CheckPoint Firewall –1; Microsoft ISA Server 2000 Standard Edition, Microsoft ISA Server 2004 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 Steuerungssystem miteinander verbunden und werden über eine gemeinsame Benutzeroberfläche bedient. Mit diesem System erhalten Sie einen Virenschutz, der sich vollständig an die Systemanforderungen Ihres internen Netzes anpassen lässt.

¹ Je nach Lieferumfang

Kaspersky® Corporate Suite bietet Rundumschutz² vor Viren für:

- *Computerarbeitsplätze* unter Microsoft Windows 98/Me, Microsoft Windows 2000/NT/XP Workstation und Linux.
- *Dateiserver* unter Microsoft Windows NT 4.0 Server, Microsoft Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, Linux; *Dateispeicher* unter Samba.
- *Mailsysteme* vom Typ Microsoft Exchange Server 2000/2003, Lotus Notes/Domino, postfix, exim, sendmail und qmail.
- *Internet-Firewalls*: CheckPoint Firewall –1; Microsoft ISA Server 2000 Enterprise Edition; Microsoft ISA Server 2004 Enterprise Edition.
- Handheld-PCs, die unter Symbian OS, 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 Mitteilungen auf Spam überprüft. Das Programm ist kompatibel mit jedem beliebigen Mailing-System und kann sowohl auf bereits funktionierenden als auch auf separaten Mailservern installiert werden.

Die tägliche Aktualisierung der Filterdatenbank mit Mustertexten aus unserem Sprachlabor garantiert eine hohe Effizienz dieses Produkts. Die Datenbank-Updates erscheinen alle 20 Minuten.

Kaspersky® SMTP Gateway

² Je nach Lieferumfang

Kaspersky[®] SMTP-Gateway for Linux / Unix dient der Antivirenbearbeitung von E-Mails, die mit 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 Technologien der Firma Microsoft verwendet werden. Die Anwendung untersucht alle mit dem SMTP-Protokoll auf dem Exchange-Server eingehenden Nachrichten auf das Vorhandensein von Viren, wobei Antivirentechnologien von Kaspersky Lab verwendet werden, und auf Spam-Merkmale, wozu die Filterung nach formalen Kennzeichen (E-Mail-Adresse, IP-Adresse, Größe der Mail, Kopfzeile) dient. Außerdem analysiert er den Inhalt des Briefs und seiner Anhänge mit Hilfe von intelligenten Technologien, die einzigartige Grafiksignaturen zum Erkennen von Spam in grafischer Form enthalten. 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 das Vorhandensein von Viren und anderen schädlichen Programmen (Spyware, Adware usw.) durch. Außerdem erfolgt die zentralisierte Filterung des E-Mail-Nachrichtenstroms auf Spam-Merkmale. Die Anwendung enthält ferner eine Reihe zusätzlicher Optionen, mit denen der E-Mail-Datenstrom nach Name oder MIME-Typen der angehängten Dateien gefiltert werden kann. Daneben stehen Mittel zur Verringerung der Belastung des Mailsystems und zur Abwehr von Hackerangriffen zur Verfügung.

Kaspersky Anti-Virus[®] for Proxy Server

Kaspersky Anti-Virus[®] for Proxy Server ist eine Antivirenlösung zum Schutz des Web-Datenstroms, der nach http-Protokoll über einen Proxyserver erfolgt. Die Anwendung nimmt im Echtzeitmodus die Antivirenuntersuchung des Internetverkehrs vor, hindert Schadprogramme daran, beim Internetservern in den Computer einzudringen, und scannt Dateien, die aus dem Internet heruntergeladen werden.

Kaspersky Anti-Virus® for MIMESweeper for SMTP

Kaspersky Anti-Virus® for MIMESweeper for SMTP bietet die Hochgeschwindigkeits-Antivirenuntersuchung des SMTP-Datenverkehrs auf Servern, die Clearswift MIMESweeper verwenden.

Das Programm besitzt die Form eines Plugins für die Anwendung MIMESweeper for SMTP der Firma Clearswift und führt im Echtzeitmodus die Antivirenuntersuchung und die Bearbeitung der eingehenden und ausgehenden E-Mail-Nachrichten durch.

B.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 Informationen	WWW: http://www.kaspersky.de http://www.viruslist.de/
Feedback zu unseren Benutzerhandbüchern	docfeedback@kaspersky.com (Diese Adresse ist für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.)

ANHANG C. 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 sind eine Rückgabe der Software ausgeschlossen.

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

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

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

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

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

2. EINSCHRÄNKUNGEN

- Einschränkungen im Hinblick auf Zurückentwicklung (Reverse Engineering), Dekompilierung und Disassemblierung. Sie sind nicht berechtigt, die SOFTWARE zurückzuentwickeln (Reverse Engineering), zu dekompileieren oder zu disassemblieren, es sei denn und nur insoweit, wie das anwendbare Recht, ungeachtet dieser Einschränkung, dies ausdrücklich gestattet. Sie sind nicht berechtigt, diese Software in automatischen, halbautomatischen oder manuellen Tools zu verwenden, welche dazu dienen, Virensignaturen, Virenerkennungsroutinen, sowie beliebige andere Daten oder Codes zum Erkennen von schädlichem Code oder Daten zu erstellen.
- Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.
- Supportleistungen. Nach Kauf und Aktivierung der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die Lizenzdauer. Supportleistungen verstehen sich wie folgt:
 - – stündliche Updates der Antiviren-Datenbank
 - – kostenloses Updates der Software
 - – kostenlose technische Unterstützung sowohl per e-Mail als auch per Telefon mit KASPERSKY LAB

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

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

5. GEWÄHRLEISTUNG. KASPERSKY LAB gewährleistet, dass:

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

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

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

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

7. ANWENDBARES RECHT. Dieser Vertrag unterliegt der Gesetzgebung des Landes, indem das Produkt erworben wurde.