

KASPERSKY LABS

**SECURE
YOUR
CYBERSPACE**

www.kaspersky.com



Kaspersky Anti-Virus® 5.0 for Samba Servers

HANDBUCH FÜR ADMINISTRATOREN

KASPERSKY ANTI-VIRUS® 5.0 FOR SAMBA SERVERS

Handbuch für Administratoren

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

Redaktion: Dezember 2003

Inhalt

KAPITEL 1. KASPERSKY ANTI-VIRUS® FOR SAMBA SERVERS.....	6
1.1. Hardware- und Softwarevoraussetzungen.....	7
1.2. Lieferumfang.....	8
1.3. Service für registrierte Benutzer.....	9
1.4. Textgestaltung.....	9
KAPITEL 2. INTERNE ARCHITEKTUR DER ANWENDUNG	11
2.1. Die Komponenten.....	11
2.2. Funktionsalgorithums	11
KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-VIRUS® FOR SAMBA SERVERS.....	13
3.1. Installation der Anwendung auf einem Server mit Linux.....	13
3.2. Installation des Programms auf einem Server mit FreeBSD oder OpenBSD ..	14
3.3. Installationsprozess	14
3.4. Konfiguration der Anwendung	15
3.5. Anordnungsschema der Dateien nach Verzeichnissen.....	16
3.6. Deinstallation von Kaspersky Anti-Virus® for Samba Servers	17
KAPITEL 4. KONFIGURATION NACH DER INSTALLATION	19
4.1. Standardeinstellungen des Produkts.....	19
4.2. Installation/Aktualisierung der Antiviren-Datenbanken	20
4.3. Konfiguration der Zusammenarbeit mit Webmin.....	20
4.4. Empfohlene Funktionsmodi	21
4.4.1. Optimaler Funktionsmodus	21
4.4.2. Modus für maximales Arbeitstempo	23
4.4.3. Modus für maximale Sicherheit.....	23
4.4.4. Modus zur Untersuchung von häufig aktualisierten Dateien	25
KAPITEL 5. ARBEIT MIT KASPERSKY ANTI-VIRUS® FOR SAMBA SERVERS	27
5.1. Aktualisierung der Antiviren-Datenbanken	27
5.2. Antivirenschutz von Samba-Servern im Echtzeitmodus.....	28
5.2.1. Konfiguration der Benutzerbenachrichtigung	28

5.2.1.1. Monitoring mit Benachrichtigung durch smbclient	29
5.2.1.2. Monitoring mit Benachrichtigung durch E-Mail-Nachrichten	29
5.3. Antivirenschutz von Dateisystemen	30
5.3.1. Dateiuntersuchung nach Aufforderung	31
5.3.2. Tägliche Untersuchung eines Verzeichnisses nach Taskplan (cron)	32
5.3.3. Zusätzliche Optionen: Verwendung von Skriptdateien	32
5.3.3.1. Desinfektion infizierter Archiv-Objekte	32
5.3.3.2. Senden einer Benachrichtigung an den Administrator	33
KAPITEL 6. ZUSÄTZLICHE EINSTELLUNGEN	35
6.1. Konfiguration des Echtzeit-Antivirenschutzes	35
6.1.1. Monitoringbereich	35
6.1.2. Modus zur Untersuchung und Desinfektion von Dateien	36
6.1.3. Aktionen für Dateien	37
6.1.4. Isolation infizierter Objekte	37
6.1.5. Konfiguration des Backup-Modus	38
6.2. Konfiguration des Antivirenschutzes für Dateisysteme	39
6.2.1. Untersuchungsbereich	39
6.2.2. Modus zur Untersuchung und Desinfektion von Dateien	41
6.2.3. Aktionen für Dateien	41
6.2.4. Konfiguration des Backup-Modus	42
6.3. Optimierung der Arbeit von Kaspersky Anti-Virus® for Samba Servers	43
6.3.1. Verwendung der Datenbank iChecker und Kopieren in einen Cache	43
6.3.2. Durchführen des Scannens im Hintergrund	44
6.4. Neustart von Kaspersky Anti-Virus® for Samba Servers	45
6.5. Lokalisierung des Formats für Datums- und Uhrzeitanzeige	46
6.6. Parameter für die Protokollerstellung von Kaspersky Anti-Virus®	47
6.6.1. Format von Meldungen über die Untersuchung	49
6.6.2. Format von Meldungen, die auf der Konsole angezeigt werden	51
KAPITEL 7. VERWENDUNG DER LIZENZEN	52
7.1. Lizenzierungspolitik	52
7.2. Verwaltung von Lizenzschlüsseln	52
7.2.1. Anzeige von Informationen über einen Lizenzschlüssel	53
7.2.2. Lizenzverlängerung	54
7.2.3. Entfernen eines Lizenzschlüssels	56

KAPITEL 8. HÄUFIGE FRAGEN ÜBER DIE ARBEIT MIT DEM PRODUKT.....	57
ANHANG A. INDEX.....	62
ANHANG B. SCHÄDLICHE PROGRAMME IN UNIX-UMGEBUNG.....	63
B.1. Viren.....	63
B.2. Trojanische Programme.....	65
B.3. Netzwürmer.....	66
KASPERSKY LABS LTD.....	68
B.4. Andere Produkte von Kaspersky Labs.....	69
B.5. Kontaktinformationen.....	73
ANHANG C. ENDBENUTZER-LIZENZVERTRAG FÜR KASPERSKY ANTI- VIRUS®.....	74

KAPITEL 1. KASPERSKY ANTI-VIRUS® FOR SAMBA SERVERS

Das Softwareprodukt **Kaspersky Anti-Virus® for Samba Servers** (im Folgenden auch **Kaspersky Anti-Virus®** genannt) gewährleistet die Antivirenuntersuchung auf Samba-Servern, die mit dem Betriebssystem Unix arbeiten.

Die Anwendung bietet die Untersuchung des Serverdateisystems auf zwei Ebenen: sowohl in Echtzeit, als auch nach Aufforderung. Beim Fund schädlicher Programme erlaubt Kaspersky Anti-Virus® die effektive Desinfektion oder das Blockieren infizierter Objekte zur Verhinderung einer weiteren Ausbreitung der Epidemie. Daneben ist die umgehende Benachrichtigung des Administrators über einen den Vorfall möglich.



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

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

- *Echtzeit-Schutz* des Samba-Dateiservers vor schädlichem Code (**On-Demand Scanner**).
- *Suche und Desinfektion* von schädlichem Code im Serverdateisystem *nach Aufforderung* (**On-Access Scanner**).
- *Benachrichtigung des Administrators* über das Vorhandensein infizierter oder verdächtiger Objekte.
- *Gewährleistung des aktuellen Zustands der Antiviren-Datenbanken* (**KeepUp2Date**).
- *Lokale und Remote-Administration* mit Hilfe des Moduls zur Web-Administration (**Webmin**).

Außerdem bietet Kaspersky Anti-Virus® seinen Benutzern folgende Zusatzfunktionen:

- Möglichkeit zum Ausführen von benutzerdefinierten Skripten 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 vor der Desinfektion (Backup) mit der Möglichkeit seiner Wiederherstellung im Fall des Eintritts unvorhergesehener 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 Echtzeit-Modus gleichzeitig zu scannenden Dateien, wobei überzählige zur Untersuchung aufgerufene Dateien in eine Warteschlange eingereiht werden.
- Möglichkeit zum automatischen Anhalten der Antivirenuntersuchung von Dateien im Hintergrund-Modus bei Überschreitung eines benutzerdefinierten Werts für die Belastungsgrenze auf dem Server, und zur Wiederaufnahme der Arbeit beim Sinken unter das zulässige Niveau.
- Möglichkeit der Definition einer beliebigen Kombination der Modi "Untersuchung beim Öffnen" und "Untersuchung beim Speichern" für jeden Ordner mit allgemeinem Zugriff.
- Möglichkeit zum Vornehmen individueller Einstellungen für den Antivirenschutz separat für jeden Ordner mit allgemeinem Zugriff.
- 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 ab dem Moment des Abbruchs wieder auf.
- Möglichkeit des Aufschiebens von Updates der Antiviren-Datenbanken und Updates der Anwendung.

1.1. Hardware- und Softwarevoraussetzungen

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

- Hardwarevoraussetzungen:
 - Prozessor der Pentium-Klasse oder höher.

- Mindestens 32 MB freier Arbeitsspeicher.
- Mindestens 100 MB verfügbarer Festplattenspeicher.
- Softwarevoraussetzungen:
 - Eines der folgenden Betriebssysteme:
 - Linux RedHat (Version 7.3, 8.0 und 9.0), Linux SuSE (Version 8.1 und 8.2) oder Linux Debian (Version 3.0);
 - FreeBSD Version 4.7 und 5.0;
 - OpenBSD Version 3.3;
 - Installierter Samba-Server Version 2.2.6 oder höher.
 - Installiertes Perl Version 5.0 oder höher.

1.2. Lieferumfang

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

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

- Versiegelter Umschlag mit Installations-CD, welche die Programmdateien enthält.
- Handbuch für Administratoren.
- Lizenzschlüssel, der auf der Installations-CD gespeichert ist.
- Registrierungskarte (mit Seriennummer des Produkts).
- Lizenzvertrag.



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

Beim Erwerb des Produkts in einem Online-Shop kopieren Sie das Produkt von der Internetseite von Kaspersky Labs. Die Distribution enthält neben dem eigentlichen Produkt auch das vorliegende Handbuch. Ein Lizenzschlüssel ist entweder Bestandteil der Distribution oder wird Ihnen nach Eingang der Bezahlung per E-Mail zugesandt.

Der Lizenzvertrag ist eine rechtsgültige Vereinbarung zwischen Ihnen und Kaspersky Labs 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 Kaspersky Anti-Virus® an den Händler zurückgeben, bei dem Sie diese erworben haben, und der Kaufbetrag des Abonnements wird an Sie zurückerstattet. Voraussetzung dafür ist, dass der versiegelte Umschlag mit der Installations-CD nicht geöffnet wurde.

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

1.3. Service für registrierte Benutzer

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

Durch den Erwerb eines Abonnements werden Sie zum registrierten Programm-benutzer und können während der Gültigkeitsdauer Ihres Abonnements 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 Labs und über das Auftauchen neuer Viren (Dieser Service gilt für Benutzer, die den Newsletter von Kaspersky Labs Ltd. abonniert haben).



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

1.4. 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.
 <i>Um diese Aktion durchzuführen,</i> <ol style="list-style-type: none"> 1. Schritt 1. 2. ... 	Beschreibung einer Folge von Schritten und möglichen Aktionen, die vom Benutzer durchgeführt werden.
 Aufgabe, Beispiel	Aufgabenstellung, Beispiel für die Realisierung der Optionen des Softwareprodukts
 Lösung	Lösung der vorhergehenden Aufgabe
[Parameter] – Funktion des Parameters.	Befehlszeilenparameter.
Text von Meldungen und Befehlszeilen	Text von Konfigurationsdateien, Informationsmeldungen des Programms und Befehlszeilen.

KAPITEL 2. INTERNE ARCHITEKTUR DER ANWENDUNG

Vor der Erklärung der funktionellen Möglichkeiten von Kaspersky Anti-Virus® for Samba Servers, werfen wir einen ausführlichen Blick auf seine interne Architektur. Dies führt zu einem besseren Verständnis des Funktionsalgorithmus von Anti-Virus.

2.1. Die Komponenten

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

- *kavsamba* (On-Access-Scanner);
- *kavscanner* (On-Demand-Scanner);
- *keepUp2Dater*.

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 diese 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.

2.2. Funktionsalgorithmus

In diesem Abschnitt betrachten wir die interne Architektur des Produkts im Kontext des Echtzeit-Antivirenschutzes. Der Untersuchungsprozess zur

Manuellen Suche (Suche nach Aufforderung durch den Benutzer) 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, aufgerufene Datei, 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 diese infiziert oder verdächtig ist (*warning*, *suspicion*, *infected*). In allen anderen Fällen (*clear*, *cured*) wird der Zugriff auf die Datei erlaubt.

KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-VIRUS® FOR SAMBA SERVERS

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

- Stellen Sie sicher, dass das System den Hardware- und Softwarevoraussetzungen für die Installation von Kaspersky Anti-Virus® entspricht (s. Pkt. 1.1 auf S. 7).
- Melden Sie sich als Benutzer **root** beim System an.

3.1. Installation der Anwendung auf einem Server mit Linux

Kaspersky Anti-Virus® for Samba Servers wird je nach Variante der Distribution in drei Installationsvarianten geliefert.



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

```
rpm -i <Dateiname_der_Distribution>
```



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

```
dpkg -i <Dateiname_der_Distribution>
```

Außerdem können Sie die Standard-Installationsvariante verwenden, die für alle Linux-Betriebssysteme einheitlich ist. Diese Variante kann dann verwendet werden, wenn die entsprechende Linux-Distribution rpm- oder deb-Formate nicht unterstützt (z.B. Slack Ware) oder wenn der Administrator keinen integrierten Paket-Manager benutzt.

Die Universaldistribution von Kaspersky Anti-Virus® for Samba Servers wird in Form eines Archivs geliefert. Das Archiv enthält einen Verzeichnisbaum der Distributionsdateien und das Installationsskript *install.sh*, das die Installation vornimmt.



Gehen Sie zum Start der Installation von Kaspersky Anti-Virus® auf dem Server folgendermaßen vor:

1. Kopieren Sie das Distributionsarchiv in ein Verzeichnis des Serverdateisystems und entpacken Sie es.
2. Starten Sie das Installationskript: *install.sh*.

3.2. Installation des Programms auf einem Server mit FreeBSD oder OpenBSD

Für Server, die mit den Betriebssystemen FreeBSD oder OpenBSD 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 der Installationsprozess mit einem Fehlercode abgeschlossen werden. Vergewissern Sie sich dann, dass Ihr Computer den Hardware- und Softwarevoraussetzungen entspricht (s. Pkt. 1.1 auf S. 7) und dass die erforderliche Vorbereitung des Systems vorgenommen wurde (s. Kapitel 3 auf S.13).

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, vor dem Beginn der Verwendung des Produkts die Antiviren-Datenbanken zu installieren. Die Prozedur zur Suche und Desinfektion von Viren basiert auf den Einträgen der Antiviren-Datenbanken, die eine Beschreibung aller im betreffenden Moment bekannten Viren und Methoden zur Desinfektion infizierter Objekte enthalten.

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

4. Installation des Lizenzschlüssels;

Wird kein Lizenzschlüssel installiert, dann wird der Konfigurationsprozess nicht ausgeführt und die Arbeit mit der Anwendung ist nicht möglich. Bei vorübergehendem Fehlen des Schlüssels (z.B. wenn das Produkt 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 vor dem Beginn der Produktverwendung zu installieren. Zu Details über diese Möglichkeit s. Pkt. 7.2 auf S.52.

5. Installation des Moduls Webmin.

Das Modul zur Remote-Administration zum Paket Webmin wird nur unter der Bedingung installiert, dass Webmin sich unter dem Standardpfad befindet. Nach der Installation des Moduls folgen entsprechende Empfehlungen für die Konfiguration der Zusammenarbeit mit der Anwendung.

3.4. Konfiguration der Anwendung

Unmittelbar nach dem Abschluss des Kopierens der Distributionsdateien auf den Server erfolgt die Konfiguration des Systems. Abhängig vom Paket-Manager wird diese 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 Programmvoraussetzungen.
- Suche und Änderung der Konfigurationsdatei des Samba-Servers.
- Überprüfung der Konfigurationsdatei des Samba-Servers auf das Vorhandensein von VFS-Objekten. Wenn in der Konfigurationsdatei des Samba-Servers bereits Zeilen mit den verwendeten VFS-Objekten vorhanden sind, wird auf dem Bildschirm eine Meldung darüber angezeigt und eine Anfrage auf deren Auskommentierung vorgenommen. Wird die Auskommentierung dieser Zeilen abgelehnt, dann beendet der Konfigurationsprozess seine Arbeit.

Wenn bei der Konfiguration des Systems die Anfrage auf bestimmte Zusatzangaben (z.B. Pfad der Konfigurationsdatei des Samba-Servers) erforderlich wird, dann werden auf der Server-Konsole 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 des Produkts 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 durchzuführen.

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:

ect/kav/5.0/kavsamba – Dieses Verzeichnis enthält die Konfigurationsdatei von Kaspersky Anti-Virus[®] und andere Konfigurationsdateien:

kav4sambaservers.co – Konfigurationsdatei;

/var/db/kav/5.0/kavsamba/bases und */var/db/kav/5.0/kavsamba/license* – Diese Verzeichnisse enthalten die Antiviren-Datenbanken und eine Liste der Updateserver für diese Datenbanken;

/var/db/kav/5.0/kavsamba/patches – Dieses Verzeichnis enthält heruntergeladene Patches der Anwendung.

Wenn Sie das Betriebssystem Linux installiert haben:

/opt/kav/5.0/kavsamba – Das Hauptverzeichnis von Anti-Virus, das folgende Elemente enthält:

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

kavscanner – ausführbare Datei der Komponente für den Antivirenschutz von Dateiservern Kaspersky Anti-Virus[®] On-Demand Scanner;

kavsamba – ausführbare Datei der Komponente für den Antivirenschutz im Echtzeit-Modus *kavsamba* (On-Access Scanner);

KeepUp2Date – ausführbare Datei der Komponente Kaspersky KeepUp2Date, die dem Update der Antiviren-Datenbanken dient;

/man/ – Verzeichnis der man-Dateien;

/setup/ - Verzeichnis zum Speichern von Dienstsripten und Webmin.

Wenn Sie das Betriebssystem FreeBSD oder OpenBSD installiert haben:

/usr/local/suare/kav/5.0/kavsamba – Das Hauptverzeichnis von Anti-Virus, das folgende Elemente enthält:

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

kavscanner – ausführbare Datei der Komponente für den Antivirenschutz von Dateiservern Kaspersky Anti-Virus® On-Demand Scanner;

kavsamba – ausführbare Datei der Komponente für den Antivirenschutz im Echtzeit-Modus kavsamba (On-Access Scanner);

KeepUp2Date – ausführbare Datei der Komponente Kaspersky KeepUp2Date, die dem Update der Antiviren-Datenbanken dient.

/man/ – Verzeichnis der man-Dateien.

/setup/ - Verzeichnis zum Speichern von Dienstsripten und Webmin.

3.6. Deinstallation von Kaspersky Anti-Virus® for Samba Servers

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 der Samba-Servers.



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

Außerdem muss der Administrator die Arbeit der Anwendung selbständig beenden. Dafür kann z.B. der folgende Befehl dienen:

```
kill -TERM `cat /var/run/kavsamba.pid`
```

Nachdem die oben genannten Aktionen vorgenommen wurden, kann direkt zur Deinstallationsprozedur übergegangen werden, die automatisch ausgeführt wird. Abhängig vom verwendeten Paket-Manager erfolgt der Start der Deinstallation auf unterschiedliche Weise. Betrachten wir die einzelnen Varianten genauer.



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>
```



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

```
install.pl uninstall
```



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.

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 des Produkts wurden Standardwerte gewählt, welche die Arbeit mit Anti-Virus möglichst komfortabel gestalten (s. Pkt. 4.1 auf S. 19).



Es wird empfohlen, vor Beginn der Arbeit mit dem Produkt die Antiviren-Datenbanken zu installieren oder zu aktualisieren, falls dies nicht bereits während der Installation gemacht wurde, und die Serverdateisysteme auf das Vorhandensein von Viren zu scannen!

Vor Beginn der Arbeit mit dem Produkt ist es empfehlenswert, die Antiviren-Datenbanken zu aktualisieren und die gemeinsame Arbeit von Kaspersky Anti-Virus® mit dem Paket Webmin zu konfigurieren.

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

4.1. Standardeinstellungen des Produkts

Alle Funktionsparameter von Kaspersky Anti-Virus® für Linux sind in einer Datei der Anwendung gespeichert. Dies ist die Konfigurationsdatei, die standardmäßig verwendet wird.



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. 35).

Als Standard ist in den Einstellungen von Kaspersky Anti-Virus® festgelegt, dass die Komponente zum Antivirenschutz im Echtzeit-Modus (*kavsamba*) ihre Arbeit beim Start des Betriebssystems beginnt. Beim Start der Komponente zur Untersuchung nach Aufforderung (*kavscanner*) erfolgt ohne zusätzliche Befehlszeilenparameter die *Antivirenungersuchung* 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 Protokolldatei entsprechende Meldungen angezeigt.



Beachten Sie, dass in der Grundeinstellung die Desinfektion von gefundenen infizierten Dateien nicht durchgeführt wird!

4.2. Installation/Aktualisierung der Antiviren-Datenbanken

Wir empfehlen, unmittelbar nach der Installation des Produkts auf dem Server die Antiviren-Datenbanken zu installieren/aktualisieren.

Starten Sie dazu die Komponente *KeepUp2Dater*. Geben Sie in der Befehlszeile ein:

```
/Pfad/von/KeepUp2Dater
```

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



Wir empfehlen Ihnen, die Antiviren-Datenbanken **TÄGLICH** zu aktualisieren, weil jeden Tag neue Viren auftauchen. Dadurch wird der aktuelle Status des Produkts gewährleistet. Zu Details über die Varianten zur Organisation von Updates s. Pkt. 5.2.1-5.3.3.2 auf S. 28-33.

4.3. Konfiguration der Zusammenarbeit mit Webmin

Wird die Remote-Administration von Kaspersky Anti-Virus® beabsichtigt, dann ist die Konfiguration der Zusammenarbeit mit dem Paket Webmin 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 (Details über die Konfiguration des Programms Webmin s. Dokumentation des betreffenden Produkts).



Im Folgenden wird bei Beschreibungen von Webmin-Registerkarten, die Funktionsparameter von Kaspersky Anti-Virus® enthalten, der Pfad jeder Registerkarte genannt. Der Pfad wird in folgendem Format angegeben:

Other (Menüpunkt von Webmin) → KAV for Samba Servers → Name des Fensters oder der Registerkarte → usw.

In der Grundeinstellung werden alle Einstellungen, die mit Hilfe des Programms Webmin vorgenommen wurden, in der Standard-Konfigurationsdatei der Anwendung gespeichert.



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

1. Kopieren Sie die Daten aus der bestehenden Konfigurationsdatei in die neue Datei, die unter einem anderen Namen gespeichert werden muss. Führen Sie danach den Anforderungen entsprechend die Korrektur der neuen (alternativen) Konfigurationsdatei durch.
2. Geben Sie den Namen der alternativen Konfigurationsdatei auf der Registerkarte **Config edit** im Eingabefeld des Parameters **Full path to KAV config** an.
3. Geben Sie auf den entsprechenden Registerkarten die erforderlichen Parameter für den Antivirenschutz der Dateisysteme an.

Other → KAV for Samba Servers → Registerkarte Module configure

4.4. Empfohlene Funktionsmodi

Abhängig vom Volumen der Serverbelastung empfiehlt Kaspersky Labs verschiedene Varianten zur Konfiguration der optimalen Arbeit von Kaspersky Anti-Virus® for Samba Servers.



Zur detaillierten Beschreibung der Werte jedes Parameters s. entsprechende man.

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 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.

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

```
IcheckerDbFile=/var/db/kav/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  
Cluster=no  
HashType=md5
```

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

```
BackupPath=/tmp/samba-backup  
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
```



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

4.4.2. Modus für maximales Arbeitstempo

Dieser Modus ist auf die Gewährleistung der maximalen Arbeitsgeschwindigkeit der Anwendung hin orientiert. In diesem Fall wird die Sicherheit des Antivirenschutzes allerdings geringfügig vermindert.

Es wird empfohlen, die Untersuchung von Archiven zu deaktivieren und beim Schließen keine Untersuchung 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 (Zugriff zum Lesen 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
BgCheckFilesLimit=3
BgSheduleTime=5
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 **[path]** folgenden Parameterwert an:
`IcheckerDbFile=/var/db/kav/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=0`
`CheckFilesLimit=0`
`BgCheckFilesLimit=0`
`BgSheduleTime=0`
`Cluster=no`
`HashType=md5`
- Geben Sie im Abschnitt **[samba.path]** folgenden Parameterwert an:
`BackupPath=/tmp/samba-backup`
- 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 `Ichecker=yes`), sondern auch für `kavscanner` (Abschnitt `[scanner.options]` Parameter `Ichecker=yes`) aktiviert ist.

4.4.4. Modus zur Untersuchung von häufig aktualisierten Dateien

Dieser Modus wird für die Konfiguration des Antivirenschutzes von Ordnern mit allgemeinem Zugriff empfohlen, in denen häufig Aktualisierungen der Dateien erfolgen.

Der Modus zur Untersuchung von häufig aktualisierten Dateien unterscheidet sich von einem **empfohlenen Modus** dadurch, dass zur Beschleunigung der Arbeitsgeschwindigkeit für bestimmte Ordner mit allgemeinem Zugriff nach dem Schreiben keine Untersuchung erfolgt (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 Inhalt des Ordners wird dann entweder beim Zugriff durch einen Benutzer oder beim Scannen im Hintergrundmodus auf das Vorhandensein von Viren untersucht.

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

```
IcheckerDbFile=/var/db/kav/ichecker.db
```

```
Packed=yes  
Archives=yes  
SelfExtArchives=yes  
MailBases=yes  
MailPlain=yes  
Heuristic=yes  
Cure=yes  
Ichecker=yes  
FileCacheSize=20000  
CheckFilesLimit=20  
BgCheckFilesLimit=5  
BgSheduleTime=10  
Cluster=no
```

HashType=md5

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

BackupPath=/tmp/samba-backup

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 nach Aufforderung (manuell bzw. nach Zeitplan) 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 entsprechend der Einstellungen bearbeitet. Der Zugriff auf gefährliche Dateien wird blockiert.

Bei der manuellen Untersuchung, die mit Hilfe der Komponente *kavscanner* erfolgt, kann die Untersuchung beliebiger Dateien (darunter auch Mail-Datenbanken, Archivdateien u.a.) vorgenommen werden, die sich auf einem Computer befinden. Entsprechend der Untersuchungsergebnisse wird auf infizierte Dateien die Aktion angewandt, die in den Einstellungen der Konfigurationsdatei festgelegt wurde.

Außerdem besteht die Möglichkeit zur Aktualisierung der Antiviren-Datenbanken mit Hilfe der Komponente *KeepUp2Date*. Diese Komponente führt das Update der von Kaspersky Anti-Virus® für den Antivirenschutz verwendeten Antiviren-Datenbanken und der Programmmodule entweder lokal oder im Remote-Modus durch.



Beachten Sie, dass bei allen unten für den Prozess *kavsamba* angeführten Beispielen nach Änderungen in der Konfigurationsdatei der "Warmstart" von Kaspersky Anti-Virus® erforderlich ist. Details zum Ausführen eines Neustarts s. Pkt. 6.4 auf S.45.

5.1. Aktualisierung der Antiviren-Datenbanken

Als Updatequelle für die Antiviren-Datenbanken dienen die Updateserver von Kaspersky Labs. Zum Beispiel:

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

<http://downloads2.kaspersky-labs.com/updates/>
<ftp://downloads1.kaspersky-labs.com/updates/> und andere.

Eine Liste der Adressen, von denen Updates kopiert werden können, befindet sich in der Datei *servers.lst*, die zum Lieferumfang des Produkts gehört.

Im Folgenden betrachten wir die interessantesten Aufgaben zur Gewährleistung der Antivirensicherheit.

5.2. Antivirenschutz von Samba-Servern im Echtzeitmodus

Der Antivirenschutz von Samba-Servern im Echtzeitmodus wird von der Komponente *kavsamba* durchgeführt, die den Aufruf von Dateien über einen Samba-Server verfolgt. *kavsamba* wird beim Start der Betriebssystemdienste gestartet. Nach der Analyse der aufgerufenen Datei mit Hilfe des in die Komponente integrierten Antiviren-Kerns, entscheidet *kavsamba* über die weitere Behandlung der Datei (Zugriff erlauben/verbieten).

In der Grundeinstellung ist der Modus zur Desinfektion infizierter Objekte nicht aktiviert. Also wird beim Fund von infizierten, verdächtigen oder beschädigten Objekten der Zugriff auf diese gesperrt und es werden entsprechende Aufzeichnungen im Protokoll vorgenommen.



Alle Einstellungen der Komponente *kavsamba* befinden sich in den Abschnitten [samba.*] der Konfigurationsdatei der Anwendung.



Zusätzlich können die Modi zur Desinfektion infizierter Objekte, zum Verschieben solcher Objekte in ein separates Verzeichnis u.a. aktiviert werden. Nehmen Sie dazu entsprechende Einstellungsänderungen in der Konfigurationsdatei vor. Details s. Pkt. 6.1.3. auf S. 37.

5.2.1. Konfiguration der Benutzerbenachrichtigung

Da *kavsamba* im Hintergrundmodus arbeitet, werden mit Ausnahme von Start- und Dienstmeldungen keinerlei Informationen auf der Konsole angezeigt. Zusätzliche Optionen für Benachrichtigungen können beispielsweise durch E-Mail-Nachrichten oder über das Standarddienstprogramm **smbclient** realisiert werden. Betrachten wir diese Möglichkeiten genauer.

5.2.1.1. Monitoring mit Benachrichtigung durch smbclient

Bei der Installation eines Samba-Servers wird automatisch das Dienstprogramm **smbclient** installiert, mit dessen Hilfe **winpopup**-Meldungen an die Clientmaschine übergeben werden. Im Betriebssystem Windows werden solche Meldungen (**winpopup**) auf dem Benutzerbildschirm angezeigt, wenn der Dienst Messenger (Nachrichtendienst) aktiviert wurde.

Nützlich ist die Verwendung dieser Option zur Warnung von Benutzern (Administratoren) beim Versuch eines Zugriffs auf eine infizierte Datei über einen Samba-Server.

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 der Anwendung (oder in einer alternativen Datei) im Abschnitt **[samba.actions]** als Aktion folgende Zeile an:

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

2. Führen Sie durch folgenden Befehl den Neustart von *kavsamba* durch:

```
KILL -HUP <PID des Prozesses>
```



Denken Sie daran, einen "Warmstart" von Kaspersky Anti-Virus® vorzunehmen (s. Pkt. 6.4 auf S. 45).

5.2.1.2. Monitoring mit Benachrichtigung durch E-Mail-Nachrichten

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.



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 der Anwendung (oder in einer alternativen Datei) im Abschnitt **[samba.actions]** als Aktion folgende Zeile an:

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

2. Führen Sie durch folgenden Befehl den Neustart von *kavsamba* durch:

```
KILL -HUP <PID des Prozesses>
```

5.3. Antivirenschutz von Dateisystemen

Der Antivirenschutz der Dateisysteme eines Servers erfolgt mit Hilfe der Komponente *kavscanner*, die Serverdateien auf das Vorhandensein von Viren untersucht und entsprechend den Einstellungen die Bearbeitung infizierter und/oder verdächtiger Objekte durchführt. Die Bearbeitung der Objekte kann entweder rein informativen Charakter besitzen (Anzeige von Informationen im Protokoll 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.41

Die Untersuchung des Dateisystems Ihres Servers kann einmalig aus der Befehlszeile ausgeführt werden oder nach Taskplan mit Hilfe des Standarddienstprogramms **cron**. Sie können entweder die Untersuchung aller Dateisysteme des Servers oder eines bestimmten Verzeichnisses festlegen. Es können auch Sektoren von Blockgeräten untersucht werden.

Im Folgenden betrachten wir typische Aufgaben für den Antivirenschutz eines Serverdateisystems.



Der Prozess einer Virus-Untersuchung des gesamten Computers ist eine Prozedur mit hohem Ressourcenbedarf. Es ist zu beachten, dass dabei die Funktionsgeschwindigkeit des Servers verlangsamt wird. Deshalb wird empfohlen, für die Untersuchung eine Zeit zu wählen, während der die Auslastung des Servers möglichst gering ist.

5.3.1. Dateiuntersuchung nach Aufforderung

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



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 Protokolldatei *kavscanner-aktuelles_Datum.log* erscheinen, die im gleichen Verzeichnis gespeichert wird.



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

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

5.3.2. Tägliche Untersuchung eines Verzeichnisses nach Taskplan (cron)

Zum Lieferumfang aller Betriebssysteme der Unix-Familie gehört das Standarddienstprogramm zur Taskplanung **cron**, mit dessen Hilfe die automatische Ausführung eines beliebigen Tasks für Kaspersky Anti-Virus® for Samba Servers festgelegt werden kann, wozu auch die Untersuchung eines Verzeichnisses nach Taskplan zählt.



Aufgabe: Jeden Tag um 0 Uhr 00 Minuten soll die Virus-Untersuchung des Verzeichnisses **/home** gestartet werden. Dabei sollen die Scan-Parameter verwendet werden, die in der Konfigurationsdatei `/etc/kav/kavscanner.cron` festgelegt sind.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Legen Sie die Konfigurationsdatei `/etc/kav/kavscanner.cron` an und legen Sie die erforderlichen Scan-Parameter fest.
2. Ändern Sie die Datei, welche die Regeln für die Arbeit des Prozesses **cron** (**crontab -e**) festlegt: Geben Sie folgende Zeile an:

```
0 0 * * * /path/to/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 der Antiviren-Analyse unterzogen wurden. Hierzu werden unterschiedliche Unix-Standardbefehle sowie Skriptdateien verwendet. Mit Hilfe solcher Werkzeuge können erfahrene Administratoren die Aktionen für Objekte mit unterschiedlichem Status selbständig festlegen und so die Funktionalität von Kaspersky Anti-Virus® erweitern.

5.3.3.1. Desinfektion infizierter Archiv-Objekte

Kaspersky Anti-Virus® führt keine Desinfektion infizierter Dateien durch, die in Archive gepackt sind, findet aber in diesen enthaltene verdächtige und infizierte Objekte. Allerdings kann die Desinfektion durch eine zusätzliche Skriptdatei

realisiert werden. In der vorliegenden Dokumentation wird ein Beispiel für die Desinfektion von Archiven des Typs *tar* und *zip* mit Hilfe der Skriptdatei *vox.sh* besprochen. Dieses Skript gehört zum Lieferumfang von Kaspersky Anti-Virus®.



Aufgabe: Untersuchung aller auf dem Server vorhandenen Archive der Typen *tar* und *zip*, und Desinfektionsversuch aller in einem Archiv gefundenen infizierten Objekte mit Hilfe des Skripts *vox.sh*. Als Konfigurationsdatei soll */etc/kav/kavscanner.conf.in* verwendet werden, in der vorher die Verwendung der Skriptdatei für die Archivdesinfektion festgelegt wird.

Aufzeichnung einer Liste aller infizierten Objekte mit vollständigem Pfad in der Datei */tmp/infected_archive.lst*. Das Arbeitsprotokoll der Komponente soll nur in der Datei */tmp/logfile.log* erscheinen.



Lösung: Gehen Sie zur Lösung dieser Aufgabe folgendermaßen vor:

1. Legen Sie die alternative Datei *kavscanner.conf.in* an.
2. Legen Sie die Bearbeitungsregeln für infizierte Objekte fest. Geben Sie dazu im Abschnitt **[scanner.container]** dieser Datei folgende Zeile an:

```
OnInfected=exec /tmp/kavscanner/test/vox.sh
%FULLPATH%/ %FILENAME%
```

3. Geben Sie in der Befehlszeile ein:

```
# kavscanner -c kavscanner.conf.in -ePASE -qR
-o /tmp/logfile.log -j3
-pi /tmp/infected_archive.lst /
```

5.3.3.2. 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 Dateisystemen benachrichtigt wird.



Aufgabe: Konfiguration für die 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 kavscanner  
admin@localhost.ru
```

```
[scanner.container]
```

```
OnInfected=exec echo archive %FULLPATH%/FILENAME% is  
infected, viruses list is in the attached file %LIST%  
| mail -s 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 während des Installationsprozesses vorgenommen werden (s. Pkt. 3.3 auf S.14) und ohne die das Produkt nicht funktionsfähig ist, erfolgen die Zusatzeinstellungen nach Ermessen des Administrators. Sie zielen auf die Erweiterung der Möglichkeiten des Produkts und dessen Anpassung an die Verwendungsbedingungen im Rahmen eines konkreten Unternehmens ab.

6.1. Konfiguration des Echtzeit-Antivirenschutzes

Wie oben erwähnt, dient zum Antivirenschutz für Samba-Server im Echtzeitmodus die Komponente *kavsamba*.

Zur Konfiguration der Komponente können folgende Parameter angepasst werden:

- Monitoringbereich: Pfad und Objekte für das Monitoring (s. Pkt. 6.1.1. auf S. 35).
- Modus zur Untersuchung und Desinfektion von Dateien (s. Pkt. 6.1.2 auf S. 36).
- Aktionen für Dateien (s. Pkt. 6.1.3. auf S. 37).
- Modus zum Anfertigen von Sicherheitskopien (s. Pkt. 6.1.5 auf S. 42).
- Erstellen von Protokoll und Meldungen (s. Pkt.6.5 auf S.47).

6.1.1. Monitoringbereich

Der Monitoringbereich der Komponente *kavsamba* umfasst *Monitoringpfad* und *Monitoringobjekte*.

Unter *Monitoringpfad* werden alle Dateisysteme verstanden, die für Benutzer über den Samba-Server zugänglich sind. Eine Begrenzung des Pfads kann nur durch den Ausschluss bestimmter Verzeichnisse oder Dateien in der

Konfigurationsdatei der Anwendung (Abschnitt **[samba.options]**, Parameter **ExcludeMask** und **ExcludeDirs**) erfolgen.

Auch *Monitoringobjekte* (Dateitypen, die auf Viren untersucht werden) werden nur durch die Parameter der Konfigurationsdatei der Anwendung festgelegt.



Beim Start der Komponente *kavsamba* können Sie den Monitoringbereich nicht in der Befehlszeile festlegen oder einschränken. Diese Option steht nur für die Antivirenuntersuchung der Dateisysteme des Servers zur Verfügung (Komponente *kavscanner*).

6.1.2. Modus zur Untersuchung und Desinfektion von Dateien

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

In der Grundeinstellung ist der Modus zur Desinfektion gefundener infizierter 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 Protokolldatei (s. Pkt. 6.6 auf S. 47). Der Zugriff auf derartige Objekte wird automatisch blockiert.

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 Untersuchung der Datei die Aktionen durch, die in den Einstellungen der Konfigurationsdatei festgelegt wurden (s. Pkt. 6.1.3 auf S. 37).

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

- **Clear** – Datei ist nicht infiziert.
- **Infected** – Datei ist infiziert.
- **Cured** – Datei wurde erfolgreich desinfiziert.
- **CureFailed** – Desinfektionsversuch der Datei war erfolglos.
- **Warning** – Code der Datei besitzt Ähnlichkeit mit dem Code eines bekannten Virus.
- **Suspicion** – Datei ist verdächtig auf Virusinfektion.

- **Protected** – Datei kann nicht untersucht werden, weil sie verschlüsselt ist.
- **Corrupted** – Datei ist beschädigt.

Abhängig vom Status der Datei wird der Zugriff darauf entweder erlaubt oder blockiert.



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

6.1.3. Aktionen für Dateien

Für Dateien mit den Status **Infected**, **Suspicious**, **Warning** kann eine Reihe von Aktionen festgelegt werden:

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

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

Die Bearbeitungsregeln für Objekte können mit folgenden Methoden 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.

6.1.4. Isolation infizierter Objekte

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 nicht möglich ist (z.B. wenn nur zwei von drei Viren, durch die eine Datei infiziert ist, entfernt werden konnten).



Der Administrator festlegen, dass Objekte in Abhängigkeit von ihrem Dateistatus in unterschiedliche Verzeichnisse verschoben werden.

Wenn ein solches Verzeichnis gespeichert werden soll, wird empfohlen, es mit Hilfe des Parameters **ExcludeDir** (Abschnitt **[samba.options]**) der Konfigurationsdatei aus dem Untersuchungsbereich auszuschließen.



Aufgabe: Virus-Untersuchung aller Dateien, die über den Samba-Server aufgerufen werden, und Desinfektion, wenn ein Objekt infiziert ist. Wenn der Desinfektionsversuch erfolglos ist, sollen infizierte Objekte mit vollständiger Pfadangabe in das Verzeichnis /tmp/infected verschoben werden.



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. Legen Sie die Bearbeitungsregeln für infizierte Objekte fest. Geben Sie dazu im Abschnitt **[samba.actions]** der Konfigurationsdatei folgende Zeile an:

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

6.1.5. Konfiguration des Backup-Modus

Wurden Dateien von einem absolut neuartigen Virustyp infiziert, über den noch kein Eintrag in den Antiviren-Datenbanken existiert, und als Aktion für infizierte Objekte wurde das Löschen aus dem Dateisystem festgelegt, dann besteht die Gefahr des Verlusts wichtiger Daten. Um dies zu vermeiden, bietet Kaspersky Anti-Virus® die Option zum Kopieren der Dateien in ein Backup-Verzeichnis.

Vor der Desinfektion oder dem Löschen einer Datei wird in einem Backup-Verzeichnis (Abschnitt **[samba.path]**, Parameter **BackupPath**) eine Kopie von ihr angelegt. Dies erlaubt die Speicherung einer Sicherheitskopie für den Fall, dass die Datei während des Desinfektionsprozesses beschädigt wird. Die Datei wird mit vollständigem Pfad in Backup gespeichert. Bei wiederholter Speicherung im Backup-Verzeichnis wird eine alte Kopie der Datei jeweils automatisch durch die aktuellste ersetzt.

Beachten Sie, dass in der Grundeinstellung der Modus zum Anfertigen einer Sicherheitskopie in Backup nicht aktiviert ist und dementsprechend der Pfad des Verzeichnisses, das zum Speichern von Sicherheitskopien dienen soll, nicht festgelegt ist. Zur Verwendung dieser Option müssen Sie diesen Pfad selbstständig festlegen.



Beim Löschen eines Objekts aus dem Dateisystem wird dessen Kopie solange in Backup aufbewahrt, bis sie vom Administrator gelöscht wird.

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 und auf die maximale Untersuchung der Dateisysteme eingestellt, die von der Workstation aus verfügbar sind, auf der das Produkt installiert ist. Alle verfügbaren Dateien werden auf das Vorhandensein von Viren gescannt, 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. 6.2.1 auf S.39) (Dieser Parameter entspricht dem Monitoringbereich bei der Verwendung des Echtzeitschutzes).
- Modus zur Untersuchung und Desinfektion von Dateien (s. 6.2.2 auf S.41).
- Aktionen für Dateien (s. 6.2.3 auf S.41).

Betrachten wir nun die Einstellungen jeder einzelnen Gruppe.

6.2.1. Untersuchungsbereich

Der Scanbereich lässt sich bedingt in zwei Teile gliedern:

- *Untersuchungspfad* – Liste der Verzeichnisse und Dateien, in denen die Virussuche durchgeführt wird.
- *Untersuchungsobjekte* – Typen der Dateien, die auf das Vorhandensein von Viren gescannt werden (Archive, Mail-Nachrichten 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 Untersuchungsbereich anzugeben.

Der Untersuchungspfad kann durch folgende Methoden 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 des Scanpfads in einer Textdatei und Festlegen der Verwendung dieser Datei in der Befehlszeile durch den Parameter **-@ <Dateiname>**. Jedes Objekt in dieser Datei wird in einer neuen Zeile und mit absoluter Pfadangabe angegeben.



Werden in der Befehlszeile sowohl der Untersuchungspfad als auch eine Textdatei mit einer Liste von Untersuchungsobjekten angegeben, dann 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 und Festlegen der Verwendung dieser Datei durch den Befehlszeilenparameter **-c <Dateiname>** beim Start der Komponente.

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.

Beachten Sie, dass die Option zur Desinfektion in der Grundeinstellung nicht aktiviert ist. Es wird lediglich die Virus-Untersuchung der Dateien durchgeführt und durch Anzeige von Meldungen auf der Konsole und im Protokoll über den Fund infizierter, verdächtiger oder beschädigter Objekte informiert.

Als Ergebnis der Virus-Untersuchung erhält jede Datei einen bestimmten Status (**Clear**, **Infected**, **Warning** usw.), und der Zugriff zu untersuchten Dateien wird gewährt oder blockiert.

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

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 Protokoll Meldungen erscheinen.

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

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

Bei der Durchführung einer Untersuchung von Serverdateisystemen unterscheidet Kaspersky Anti-Virus® zwischen einem gewöhnlichen Objekt (Datei) und einem zusammengesetzten (das aus mehreren Objekten besteht – Archiv). Auch die Aktionen, die mit solchen Objekten durchgeführt werden, unterscheiden sich; in der Konfigurationsdatei werden sie 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, wird es als gewöhnliches Objekt betrachtet, ist aber ein Objekt innerhalb des Archivs infiziert, als zusammengesetztes. Dementsprechend werden in solchen Fällen auch die Aktionen für Archive durch die Parameter unterschiedlicher Abschnitte der Konfigurationsdatei bestimmt.

Zur Auswahl der Aktion für bestimmte Dateien dienen folgende Methoden:

- 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. Konfiguration des Backup-Modus

Die Einstellungsmöglichkeiten zum Anfertigen von Sicherheitskopien bei der Durchführung des Antivirenschutzes von Dateisystemen entsprechen vollständig den in Pkt. 6.1.5 auf S. 38 für den Antivirenschutz im Echtzeitmodus beschriebenen. Deshalb werden die Einstellungen für diesen Modus hier nicht näher beschrieben.



Aufgabe: Virus-Untersuchung aller Objekte in den Verzeichnissen und Dateien, die in der Datei `/tmp/download.lst` angegeben sind, und deren Desinfektion. Im Fall des erfolglosen Desinfektionsversuchs sollen gefundene infizierte Dateien mit vollständigem Pfad in das Verzeichnis `/tmp/infected`, verdächtige nach `/tmp/suspicious`, und beschädigte nach `/tmp/warning` verschoben werden.



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:

```
# 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.

6.3.1. Verwendung der Datenbank iChecker und Kopieren in einen Cache

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

Bei der ersten Untersuchung einer beliebigen Datei werden Informationen 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 der Komponente *kavsamba* und mit der Komponente *kavscanner* untersucht wurden.
- Cache der untersuchten Dateien – Eine Datenbank, die Informationen über alle untersuchten Dateien enthält. Diese Datenbank enthält nur Informationen über Objekte, die mit der Komponente *kavsamba* untersucht wurden. Sie 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 (die Datei ist nicht virusfrei oder ihr

Format wird nicht unterstützt), dann werden diese in der anderen Datenbank fixiert.

Bei jedem folgenden Zugriff eines Benutzers auf die Datei wird zuerst eine Suche in der Datenbank iChecker und danach (wenn das Objekt in der ersten Datenbank nicht gefunden wurde) im Cache vorgenommen. 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 Zustands des Objekts und seiner Beschreibung in der Datenbank wird die Datei als unverändert betrachtet und nicht auf das Vorhandensein von Viren untersucht.

Wenn weder in den "sauberen Dateien" noch im Cache Informationen über die angeforderte Datei gefunden werden, wird eine vollständige Antivirenuntersuchung der Datei durchgeführt.

6.3.2. Durchführen des Scannens im Hintergrund

Da die Suche nach Daten über aufgerufene Objekte in den oben genannten Datenbanken sehr schnell erfolgt, kann die Serverbelastung wesentlich verringert werden und es besteht die Möglichkeit zu erhöhter Effektivität bei der Ressourcenverwendung des Servers, was insbesondere bei der *Durchführung des Dateiscannens im Hintergrund* gilt.

Während der Arbeit ermittelt Anti-Virus seine Auslastung. Wenn diese nicht über dem Sollwert liegt, untersucht er im Hintergrundmodus Dateien aus Ordnern, die allgemein zugänglich sind und sich auf dem Samba-Server befinden, sowie jene Dateien, die während des Arbeitsprozesses geändert wurden.

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 **QueueBgSizeLimit**). 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 wird der Benutzer, der die Untersuchung veranlasste, etwas länger auf eine Antwort warten, als erwartet. Beim Abschluss der Untersuchung wird die Datei aus der Warteschlange genommen. Darüber erfolgt keine zusätzlich Meldung.

Dadurch wird die maximal zulässige Serverbelastung eingehalten.

6.4. Neustart von Kaspersky Anti-Virus[®] for Samba Servers

Es bestehen mehrere Varianten für den Neustart von Kaspersky Anti-Virus[®] for Samba Servers:

- Es wird empfohlen, nach der Aktualisierung der Antiviren-Datenbanken einen "Warmstart" durchzuführen.

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

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

```
/etc/init.d/kavsamba reload avebases
```

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

```
/usr/local/share/kav/5.0/kavsamba/setup/kavsamba.sh/  
reload avebases
```

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

```
/usr/local/etc/rc.d/kavsamba.sh/ reload avebases
```

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

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

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

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

```
/etc/init.d/kavsamba reload
```

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

```
/usr/local/share/kav/5.0/kavsamba/setup/kavsamba.sh/  
reload
```

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

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

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

- Ist das zwangsläufige Beenden der Arbeit des Prozesses *kavsamba* erforderlich, dann verwenden Sie im Linux-Distributionen den Befehl:

```
/etc/init.d/kavsamba stop
```

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

```
/usr/local/share/kav/5.0/kavsamba/setup/kavsamba.sh/  
stop
```

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

```
/usr/local/etc/rc.d/kavsamba.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 Anti-Virus for Samba Servers seine Arbeit korrekt abschließt.



Es wird nachdrücklich empfohlen, den Befehl **kill -9** nicht zum Beenden der Arbeit mit dem Prozess *kavsamba* zu verwenden. Durch das Ausführen dieses Befehls wird zwar die Arbeit des Prozesses beendet, jedoch bleibt im System eine Reihe von temporären und Arbeitsdateien erhalten, die nur manuell gelöscht werden können. Beim Vorhandensein solcher Dateien halten bestimmte Anwendungen den Prozess für gestartet.

6.5. Lokalisierung des Formats für Datums- und Uhrzeitanzeige

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

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 verfügt über die Möglichkeit zum Ändern des Formats für Datum und Uhrzeit. Die Lokalisierung der Formate wird im Abschnitt **[locale]** der Konfigurationsdatei der Anwendung vorgenommen. Sie können folgende Formate festlegen:

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

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

6.6. Parameter für die Protokollerstellung von Kaspersky Anti-Virus®

Die Arbeitsergebnisse aller Komponenten von Kaspersky Anti-Virus® werden in einem Protokoll aufgezeichnet, das 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 Report aufgezeichnet und auf dem Bildschirm angezeigt werden, identisch. Wenn Sie wollen, dass auf der Konsole andere Informationen angezeigt werden als in der Reportdatei, ist eine Reihe von Zusatzeinstellungen erforderlich.

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

Die **Protokollgenauigkeit** 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.

In der folgenden Tabelle werden alle möglichen Niveaus der Protokollgenauigkeit aufgezählt.

Niveau	Bezeichnung des Niveaus	Bedeutung
	Fatale Fehler	Nur Informationen über kritische Fehler (Fehler, die zum Beenden der Arbeit des Programms führen, weil bestimmte Aktionen nicht ausgeführt werden können). Zum Beispiel: Eine Komponente ist infiziert oder bei der Untersuchung, beim Laden von Datenbanken und Lizenzschlüsseln kam es zu einem Fehler.
1	Errors	Informationen über sonstige Fehler, einschließlich Fehlern, die nicht zum Beenden der Arbeit von Komponenten führten; z.B.: Informationen über Fehler bei der Untersuchung einer Datei.
2	Info	Wichtige Meldungen mit informativem Charakter; z.B.: Informationen darüber, ob eine Komponente gestartet wurde, Pfad der Konfigurationsdatei, Untersuchungsbereich, Informationen über die Antiviren-Datenbanken, über Lizenzschlüssel, Ergebnisstatistik.
3	Activity	Meldungen über die Untersuchung von Dateien entsprechend dem Niveau des Untersuchungsprotokolls.
10	Debug	Alle Meldungen die das Erkennen, Lokalisieren und Korrigieren von Programmfehlern (Debuggen) betreffen; z.B.: Inhalt der Konfigurationsdatei.

Informationen über fatale Fehler bei der Arbeit einer Komponente werden unabhängig vom gewählten Genauigkeitsniveau angezeigt. Das optimale Niveau für die Arbeit der Komponente ist Niveau **3**, das auch als Standard gilt.

Das generelle Format für die Anzeige von Informationen für ein beliebiges der genannten Genauigkeitsniveaus besitzt folgendes Aussehen:

```
[Datum Uhrzeit Protokollierungsniveau] STRING
```

wobei:

[Datum Uhrzeit Protokollierungsniveau]- Parameter, der vom System erstellt wird und Datum und Uhrzeit (im Format, das der Administrator gewählt hat) sowie das Niveau der Protokollgenauigkeit (den ersten Buchstaben, der dem Namen des Genauigkeitsniveaus entspricht) enthält.



Das Format für die Anzeige von Datum und Uhrzeit kann im Abschnitt **[locale]** der Konfigurationsdatei der Anwendung geändert werden (s. Pkt.6.5 auf S. 46).

`String` – Protokollzeile; besitzt abhängig von der Art der Meldung unterschiedliches Format. Folgende Arten von Meldungen sind vorgesehen:

- Meldungen über das Scannen.
- Sonstige Meldungen (über den Start einer Komponente, über das Laden der Antiviren-Datenbanken, Rückgabewerte usw.)
- Meldungen, die auf der Konsole angezeigt werden.

Betrachten wir die Arten von Meldungen und das ihnen entsprechende Format ausführlicher.

6.6.1. Format von Meldungen über die Untersuchung



Meldungen über die Untersuchung werden nur für die Komponenten *kavscanner* und *kavsamba* generiert.

Das Format des Protokolls über das Scannen jeder Datei, das von der Komponente *kavscanner* erstellt wird, ist davon abhängig, zu welchem Objekttyp (gewöhnliches oder Archiv-Objekt) die Datei zählt.

Für ein **gewöhnliches Objekt** besitzen die Meldungen über das Scannen folgendes Format:

- Erweitertes Meldungsformat (**ShowObjectResultOnly=no**):

```
"Dateiname" Ergebnis [Virusname]
```

- Kurzes Meldungsformat (**ShowObjectResultOnly=yes**):

```
"Dateiname" Ergebnis
```

wobei:

`Virusname` – Name des Virus für die Ereignisse CURED, INFECTED, CUREFAILED, WARNING, SUSPICION. Für andere Ereignisse bleibt dieses Feld leer.

`Ergebnis` – Status, den die Datei als Ergebnis der Untersuchung und Desinfektion erhält. Die vollständige Liste der möglichen Ergebnisse befindet sich in der unten folgenden Tabelle.

Auch für Meldungen über **zusammengesetzte Objekte** (Archive) stehen ein erweitertes und ein kurzes Format für Meldungen über das Scannen zur Verfügung:

- Erweitertes Meldungsformat (**ShowContainerResultOnly=no**):

"Archivname"

"Dateiname" Ergebnis [Virusname]

"Dateiname" Ergebnis [Virusname]

- Kurzes Meldungsformat (**ShowContainerResultOnly=yes**):

"Dateiname" Ergebnis

Ereignis/Ergebnis	Bedeutung
OK	Datei ist virusfrei.
CURED (nur bei aktiviertem Desinfektionsmodus)	Datei war infiziert und wurde erfolgreich desinfiziert.
INFECTED	Datei ist von einem oder mehreren Viren infiziert; Anfrage auf Desinfektion wurde nicht festgelegt.
CUREFAILED (nur bei aktiviertem Desinfektionsmodus)	Datei ist von einem oder mehreren Viren infiziert; Anfrage auf Desinfektion wurde festgelegt, aber Desinfektion der Datei ist nicht möglich.
WARNING	Code der Datei besitzt Ähnlichkeit mit dem Code eines bekannten Virus.
SUSPICION	Datei ist verdächtig auf Infektion durch einen unbekanntes Virus.
ERROR	Datei kann nicht untersucht werden, weil ein Fehler aufgetreten ist (z.B. als Ergebnis der Bearbeitung eines beschädigten Archivs).
PROTECTED	Datei kann nicht untersucht werden, weil sie verschlüsselt ist.
CORRUPTED	Datei ist beschädigt.

Für die Komponente *kavsamba* besitzen die Hinweise über das Scannen das Format, das dem erweiterten Format für Meldungen der Komponente *kavscanner* entspricht.

"Dateiname" Ergebnis [Virusname]

wobei:

Virusname – Name des Virus (oder mehrerer Viren, mit denen das Objekt infiziert ist, durch Komma getrennt aufgezählt) für die Ereignisse CURED, INFECTED, CUREFAILED, WARNING, SUSPICION. Für andere Ereignisse bleibt dieses Feld leer.

Ergebnis – Status, den die Datei als Ergebnis der Untersuchung und Desinfektion erhält. Die vollständige Liste der möglichen Ergebnisse befindet sich in der obigen Tabelle.

6.6.2. Format von Meldungen, die auf der Konsole angezeigt werden



Die Anzeige von Meldungen auf der Konsole betrifft die Komponente *kavscanner*.

Die Anzeige von Informationen der Komponente *kavscanner* auf der Konsole wird durch das Vorhandensein oder Fehlen des Befehlszeilenparameters **-q** beim Start der Komponente reguliert. Wenn der Parameter angegeben wird, werden keine Informationen auf der Konsole angezeigt.

In der Grundeinstellung entsprechen Format und Umfang der auf dem Bildschirm angezeigten Informationen vollständig den in der Reportdatei aufgezeichneten Daten.

Für die Komponente *kavscanner* kann die Auswahl von auf der Konsole angezeigten Informationen geändert werden. Dazu sind im Abschnitt **[scanner.display]** der Konfigurationsdatei der Anwendung entsprechende Änderungen erforderlich.

Hier kann die Bildschirmanzeige von Informationen über das Scannen von Objekten innerhalb eines Archivs (**ShowArchiveContent**, **ShowContainerResultOnly**), über virusfreie Dateien (**ShowOK**) und über den aktuellen Status der Arbeit der Komponente (**ShowProgress**) reguliert werden.

Die Genauigkeit des Untersuchungsprotokolls wird bei Vorhandensein des Abschnitts **[display]** aus der Befehlszeile durch den Parameter **-x<option>** reguliert.

KAPITEL 7. VERWENDUNG DER LIZENZEN

7.1. Lizenzierungspolitik

Für die vorliegende Anwendung wurde eine Begrenzung des Nutzungszeitraums für das Produkt vorgesehen (in der Regel beträgt dieser Zeitraum ein Jahr ab dem Erwerb des Produkts). Bei Ablauf der Gültigkeitsdauer der Lizenz zur Benutzung von Kaspersky Anti-Virus® wird das Produkt seine Arbeit fortsetzen, allerdings ist die Aktualisierung der Antiviren-Datenbanken nicht mehr möglich. Anti-Virus wird weiterhin die Desinfektion infizierter Objekte durchführen, dabei aber die alten Antiviren-Datenbanken verwenden.

Zur Verlängerung der Lizenz können Sie sich mit der Firma in Verbindung setzen, bei der Sie das Produkt gekauft haben, und dort einen neuen Lizenzschlüssel erwerben. Außerdem können Sie die Lizenz direkt bei Kaspersky Labs verlängern. Schreiben Sie dazu an die Verkaufsabteilung (sales@kaspersky.com) oder füllen Sie auf unserer Internetseite (www.kaspersky.com/de) im Abschnitt **BUY ON-LINE → FÜR LINUX-SYSTEME** das entsprechende Formular aus. Nach Eingang der Bezahlung wird Ihnen der Lizenzschlüssel per E-Mail an die Adresse zugeschickt, die im Bestellformular angegeben wurde.

7.2. Verwaltung von Lizenzschlüsseln

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

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

- Technische Unterstützung (rund um die Uhr);
- tägliches Update der Antiviren-Datenbanken;
- Produktaktualisierung (Patch);

- Neue Produktversionen (Upgrade);
- frühzeitige Benachrichtigung über neue Viren.

Bei Ablauf der Gültigkeitsdauer der Lizenz 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 steht nicht mehr zur Verfügung. 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 zu verfolgen.

7.2.1. Anzeige von Informationen über einen Lizenzschlüssel

Sie können Informationen über die installierten Lizenzschlüssel in den Protokollen über die Arbeit der Komponenten *kavscanner* und *kavsamba* kontrollieren, da beim Start jeder der beiden Komponenten Informationen über die Schlüssel geladen werden.

Daneben ist in Kaspersky Anti-Virus® eine spezielle Komponente *licensemanager* vorgesehen, die es ermöglicht, nicht nur ausführlichere Informationen über die Schlüssel, sondern auch bestimmte analytische Daten 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:

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

Auf der Serverkonsole werden folgende Informationen angezeigt:

```
Kaspersky license manager. Version 5.0.0.0/RELEASE  
Copyright (C) Kaspersky Labs. 1998-2003.  
Active key info:
```

```
Product name: Kaspersky Anti-Virus 5 Business Optimal 1
month (Samba Servers)
Key file 00053BC3.key
Type: Commercial
Expiration date: 17-11-2003, expires in 60 days
Serial: 02B1-000454-00053BC
Additional key info:
Product name: Kaspersky Anti-Virus 5 Business Optimal 1
month (Samba Servers)
Key file 00053E3D.key
Type: Commercial
Expiration date: expired
Serial: 02B1-000454-00053E3
```



Um Informationen über eine Lizenzdatei anzuzeigen,

geben Sie in der Befehlszeile z.B. folgende Zeile ein:

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

Auf der Serverkonsole werden folgende Informationen angezeigt:

```
Kaspersky license manager. Version 5.0.0.0/RELEASE
Copyright (C) Kaspersky Labs. 1998-2003.
Product name: Kaspersky Anti-Virus 5 Business Optimal 1
month (Samba Servers)
Creation date: 23-07-2003
Expiration date: 21-11-2003
Serial 02B1-000454-00053E3
Type: Commercial
Lifespan: 30
```

7.2.2. Lizenzverlängerung

Die Verlängerung der Lizenz für die Benutzung von Kaspersky Anti-Virus® verleiht Ihnen das Recht auf die Wiederherstellung der vollen Funktionalität des Produkts. Außerdem werden die Zusatzleistungen, die in Pkt. 7.2 auf S. 52 genannt sind, erneuert.

Die Gültigkeitsdauer der Lizenz hängt vom Typ der Lizenzierung ab, den Sie beim Erwerb des Produkts gewählt haben (für Kaspersky Anti-Virus® for Samba Servers beträgt die Dauer in der Regel ein Jahr).



Um die Lizenz für die Benutzung von Kaspersky Anti-Virus® for Samba Servers zu verlängern:

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

oder:

Verlängern Sie die Lizenz direkt bei Kaspersky Labs, indem Sie an die Verkaufsabteilung (sales@kaspersky.com) schreiben oder auf unserer Internetseite (www.kaspersky.com/de) im Abschnitt **BUY ON-LINE → FÜR LINUX-SYSTEME** das entsprechende Formular ausfüllen. Nach Eingang der Bezahlung wird Ihnen der Lizenzschlüssel per E-Mail an die Adresse zugeschickt, die im Bestellformular angegeben wurde.

Nach dem Erwerb eines Lizenzschlüssels ist dessen Installation mit Hilfe des Dienstprogramms *licensemanager* erforderlich (Parameter **LicensePath** in der Konfigurationsdatei der Anwendung).



Um einen neuen Schlüssel zu installieren:

geben Sie in der Befehlszeile z.B. folgende Zeile ein:

```
#./licensemanager -a 00053E3D.key
```

Auf der Serverkonsole werden folgende Informationen angezeigt:

```
Kaspersky license manager. Version 5.0.0.0/RELEASE  
Copyright (C) Kaspersky Labs. 1998-2003.  
Key file 00053E3D.key is successfully registered
```

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

Wenn Sie vor Ablauf der Gültigkeitsdauer des aktuellen 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 gezählt.

Die Methode zur Installation eines Reserveschlüssels entspricht jener zur Installation des Hauptschlüssels. Danach werden bei einer Anfrage nach Informationen über den Lizenzschlüssel auf der Konsole sowohl Informationen über den aktuellen Schlüssel wie auch über den Reserveschlüssel angezeigt.

7.2.3. Entfernen eines Lizenzschlüssels



Um einen aktuellen Lizenzschlüssel zu entfernen,

geben Sie in der Befehlszeile z.B. folgende Zeile ein:

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

Auf der Serverkonsole werden folgende Informationen angezeigt:

```
Kaspersky license manager. Version 5.0.0.0/RELEASE  
Copyright (C) Kaspersky Labs. 1998-2003.  
Active key was successfully removed
```



Um einen Reserveschlüssel zu entfernen,

geben Sie in der Befehlszeile z.B. folgende Zeile ein:

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

Auf der Serverkonsole werden folgende Informationen angezeigt:

```
Kaspersky license manager. Version 5.0.0.0/RELEASE  
Copyright (C) Kaspersky Labs. 1998-2003.  
Additional key was successfully removed
```

KAPITEL 8. HÄUFIGE FRAGEN ÜBER DIE ARBEIT MIT DEM PRODUKT



Warum ruft Kaspersky Anti-Virus® eine gewisse Senkung der Serverleistungsfähigkeit hervor und führt zu bemerkbarer Prozessorbelastung?

Das Erkennen von Viren ist eine rein 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 Virus, der den Antiviren-Datenbanken hinzugefügt wird, die Gesamtzeit der Untersuchung. Das ist ein notwendiger Preis für die Zuverlässigkeit und Sicherheit Ihrer Daten.

Andere Antivirenprogrammen verkürzen die Untersuchungszeit, indem schwieriger zu erkennende oder (am Ort, an dem sich die Herstellerfirma geographisch befindet) seltene Viren, sowie kompliziert zu analysierende Dateiformate (z.B. pdf) aus den Antiviren-Datenbanken ausgeschlossen werden. Im Unterschied dazu ist sich Kaspersky Labs sicher, dass die Aufgabe eines Antivirenprogramms darin besteht, die reale Antivirensicherheit zu garantieren, nicht eine Scheinsicherheit, da es keinen halben Schutz geben kann. Denn ein "teilweiser Schutz" ist schlechter als überhaupt kein Schutz (weil der Benutzer im letzten Fall selbständig Vorsichtsmaßnahmen ergreifen wird).

Kaspersky Anti-Virus® erlaubt es dem Benutzer, sich maximal geschützt zu fühlen. Erfahrenen Benutzern ermöglicht Kaspersky Anti-Virus® außerdem die Beschleunigung der Antivirenuntersuchung, indem auf Kosten der allgemeinen Sicherheit bestimmte Dateitypen von der Antivirenuntersuchung ausgeschlossen werden. Wir empfehlen diese Vorgehensweise allerdings nicht, wenn der Benutzer das Gefühl des maximalen Schutzes bevorzugt.

Zur Garantie des maximalen Schutzes der Benutzer erkennt Kaspersky Anti-Virus® mehr als 40 Archive und Installationsprogramme und kann Viren in mehr als 350 unterschiedlichen Dateiformaten identifizieren. Für die Antivirensicherheit ist das sehr bedeutsam, weil jedes der erkennbaren Formate einen ausführbaren schädlichen Code enthalten kann. Erwähnenswert ist auch, dass jede Version des Produkts im Vergleich zur vorhergehenden schneller arbeitet, obwohl sich die Gesamtzahl der von Kaspersky Anti-Virus® erkennbaren Viren täglich erhöht (ungefähr 30 neue Viren pro Tag) und die Anzahl erkennbarer Formate ständig gesteigert wird. Das wird durch die Verwendung neuer unikatler Technologien

erreicht, die von Kaspersky Labs entwickelt werden. Als Beispiel kann i-Checker dienen. Dort wird eine Datei nur einmal auf Viren untersucht – bei der ersten Untersuchung. Unter der Bedingung, dass die Datei nicht verändert wurde, wird sie bei allen folgenden Untersuchungen keiner Virusanalyse unterzogen. Dadurch steigt die Leistungsfähigkeit von Anti-Virus nach der ersten Untersuchung einer Datei wesentlich.

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



Frage: *Werden Prozessoren mit folgender Architektur unterstützt: PowerPC, SPARC, Alpha, PA-RISC u.a.?*

Diese Prozessor-Arten werden in der aktuellen Produktversion nicht unterstützt.



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

Kaspersky Anti-Virus® for Samba Servers wurde auf Distributionen von RedHat, Debian und SuSE getestet und die Distributionen von Kaspersky Anti-Virus® wurden speziell für diese erstellt.



Wenn Ihre Distribution mit einer unterstützten Distribution kompatibel ist (z.B. ASPLinux ist kompatibel mit Red Hat Linux), dann ist das Auftreten von Problemen mit kritischem Charakter sehr unwahrscheinlich.

Auf Distributionen, die nicht in der Liste der von Kaspersky Labs unterstützten Distributionen enthalten sind, ist die fehlerhafte Arbeit des Produkts möglich. Dies steht vor allem mit Besonderheiten des Betriebssystems in Verbindung. Die Distribution Ihres Systems kann zum Beispiel eine andere Version einer Bibliothek verwenden oder der Pfad der Skripte zur Systeminitialisierung ist nicht standardmäßig. In diesem Fall kann Ihnen der Technische Supportservice von Kaspersky Labs keine Hilfe anbieten.



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

Archive des Typs .tgz oder .tar.gz werden durch folgenden Befehl extrahiert: `tar zxvf <Archivname>`



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 vorübergehenden Schlüssel (Evaluierungsschlüssel) anbieten, der für zwei Wochen oder einen Monat gültig ist. Nach Ablauf der Gültigkeitsdauer wird der Schlüssel blockiert.



Frage: *Was passiert, wenn die Lizenz zur Produktbenutzung 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 der Antiviren-Datenbanken von der Kaspersky-Lab-Seite mit Hilfe der Komponente *KeepUp2Date* wird nicht mehr möglich sein. Wenn Sie Antiviren-Datenbanken ohne die Verwendung von *KeepUp2Date* herunterladen, wird Kaspersky Anti-Virus® nicht funktionieren.

Demzufolge können wir Ihnen in diesem Fall den Schutz vor einer Infektion durch neue Viren nicht garantieren.

Der Grund liegt in den individuell verwendeten Einstellungen des Dienstprogramms *crond*.



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

Die Verwendung von Network Control Centre für Windows bei der Arbeit mit Kaspersky Anti-Virus® für Unix ist nicht möglich. In der aktuellen Produktversion wurde die Möglichkeit zur Remote-Konfiguration mit Hilfe eines Spezialmoduls zu dem Paket *Webmin* vorgesehen.



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

(Services → Für unsere Kunden → Technischer Support → Online-Support) 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 (support@kaspersky.com) zu schreiben.

Um sicherzustellen, dass Ihre Frage möglichst schnell bearbeitet wird:

1. Geben Sie in der Betreffzeile Ihrer Nachricht das Betriebssystem Ihres Servers, den Namen der Komponente, dessen Anpassung nicht möglich ist, und das Problem an. Zum Beispiel:
Linux, Webmin, kein Zugriff auf die Einstellungen für die Liste der Lizenzbenutzer.
2. Schreiben Sie Ihre Nachricht im Nur-Text-Format (plain text). Nachrichten im HTML-Format können Schwierigkeiten beim Lesen bereiten.
3. Geben Sie am Beginn der Nachricht die genaue Version des Betriebssystems, der Distribution von Kaspersky Anti-Virus® und den Namen Ihrer Schlüsseldatei an.
4. Beschreiben Sie das Problem möglichst kurz und verständlich. Bedenken Sie, dass der Supportservice vor der Lektüre Ihres Briefs noch nichts von Ihrem Problem weiß und Ihnen nur helfen kann, nachdem das Problem vollständig verstanden und nachvollzogen wurde.
5. Senden Sie folgende Daten an den Technischen Supportservice, nachdem Sie diese in ein Archiv gepackt haben:
 - die Dateien des Verzeichnisses `/etc/kav/`;
 - die Protokolldatei der Anti-Virus-Komponente, z.B.: `/var/log/kavscanner.rpt`;
 - die Informationen, die nach dem Befehl `ps -ax` auf der Konsole angezeigt werden;
 - den Lizenzschlüssel.
6. Machen Sie im Brief unbedingt Angaben über das Vorhandensein folgender Elemente:
 - SCSI-Controller;
 - sehr alter oder sehr neuer Prozessor, mehrere Prozessoren;
 - Arbeitsspeicher geringer als 64 MB oder größer als 2 GB.



Frage: Wie können die vom Programm auf der Konsole angezeigten Informationen in einer Datei gespeichert werden?

Eine Lösungsmöglichkeit dieser Aufgabe besteht in der Eingabe der folgenden Befehlszeile:

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

wobei:

`some_app` – die Anwendung, deren auf der Standardausgabe angezeigte Zeilen und angezeigte Meldungen über Funktionsfehler Sie in einer Datei speichern wollen;

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

Beispiel:

```
$KeepUp2Dater > ./updater.log 2>&1
```

In diesem Fall werden in der Datei `updater.log` des aktuellen Verzeichnisses die standardmäßig angezeigten Zeilen und Fehlermeldungen der Komponente `kavupdater` aufgezeichnet.



Frage: Kann ein Angreifer die Antiviren-Datenbanken verändern?

Ein Angreifer kann Antiviren-Datenbanken von der Kaspersky-Lab-Seite herunterladen und diese im Verzeichnis der Antiviren-Datenbanken speichern. Allerdings wird Kaspersky Anti-Virus® diese Datenbanken nicht für seine 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 Labs 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.

ANHANG A. INDEX

Aktualisierung der Antiviren-

Datenbanken, 52, 59

Installations-CD, 8

Lieferumfang

Buy off-line, 8

Buy on-line, 8

Lizenzschlüssel, 59

Lizenzvertrag, 8

, 2

Technischer Support, 73

Technischer Support, 9

, 2

ANHANG B. SCHÄDLICHE PROGRAMME IN UNIX- UMGEBUNG

In der Umgebung von Unix-Systemen sind Viren in wesentlich geringerem Umfang verbreitet als beispielsweise in der Umgebung von Windows. Die Gründe dafür liegen in Besonderheiten der jeweiligen Plattform. Die größte Verbreitung besitzen Trojaner und Netzwürmer.

Die Ausbreitung schädlicher Programme vollzieht sich über Netzwerke, wobei auch "Löcher" in der Software ausgenutzt werden. Betrachten wir die Arten schädlicher Programms für Unix und die Infektionsmethoden näher.

B.1. Viren

Ein Virus ist ein Programm (eine bestimmte Auswahl eines ausführbaren Codes und/oder Befehlen), das fähig ist, Kopien von sich selbst anzufertigen (die nicht unbedingt vollständig mit dem Original übereinstimmen) und diese ohne Wissen des Benutzers in unterschiedliche Objekte und/oder Ressourcen von Computersystemen, Netzwerken usw. einzufügen. Dabei behalten die Kopien die Fähigkeit zur weiteren Ausbreitung.

Bei der Untersuchung der Fundorte von Viren ergibt sich, dass Viren in Unix-Systemen in der Regel Dateiviren sind, die ihren Code in ausführbare Dateien schreiben oder Zwillingdateien erstellen.

Nach Unterschieden hinsichtlich der Funktionsalgorithmen lassen sich unterscheiden:

- *residenter Virus* – Ein Virus, der bei der Infektion seinen residenten Teil im Arbeitsspeicher hinterlässt. Der residente Teil fängt danach Aufrufe des Betriebssystems an infizierbare Objekte ab und dringt in diese ein. Residente Viren befinden sich im Arbeitsspeicher und gelten bis zum Ausschalten des Computers oder zum Neustart des Betriebssystems als aktiv.
- *nicht residenter Virus* – Ein Virus, der den Arbeitsspeicher des Computers nicht infiziert und eine zeitlich begrenzte Aktivität besitzt. Bestimmte Viren hinterlassen im Arbeitsspeicher residente Programme von geringem Umfang, die keine Viren verbreiten.

Viren, die Unix-Systeme infizieren können, sind in der Regel ungefährlich, da sich ihre Wirkung auf die Verringerung des freien Festplattenspeichers, Graphik-,

Laut- und andere Effekte beschränkt. Bestimmte Viren sind völlig harmlos, weil sie mit Ausnahme der Verringerung des freien Festplattenspeichers auf Grund ihrer Ausbreitung keinerlei Einfluss auf die Arbeit des Computers haben.

Im Folgenden einige Beispiele der Viren für Unix-Systeme:

ELF_SNOOPY – Ein Virus, der ausführbare Unix-Dateien infiziert.

Funktionsalgorithmus des Virus: Er sucht auf der Workstation alle ausführbaren Dateien, benennt diese in Dateien mit der Erweiterung .X23 um und verschiebt sie in das erstellte Verzeichnis /E. Danach kopiert der Virus seinen Code in die Originaldateien und ändert deren Attribute in **777**. Parallel dazu wird in der Hauptkennwortliste auf der infizierten Workstation der Benutzer **snoopy** mit den Rechten **777** angelegt.

Linux.Bliss – Eine Gruppe nicht residenter Viren, die ausführbare Linux-Dateien infizieren. Diese Viren sind in GNU C geschrieben und besitzen das Format ELF.

Funktionsalgorithmus des Virus: Beim Start sucht der Virus auf der Workstation ausführbare Dateien und infiziert diese, indem er den Dateiinhalt nach unten verschiebt, seinen Code auf den freien Platz schreibt und am Dateiende eine Identifikationszeile hinzufügt. Die Aktion des Virus wird durch die Benutzerrechte beschränkt, mit denen er ausgeführt wird (es sind nur Dateien betroffen, auf die Zugriff besteht). Besitzt der Benutzer Systemprivilegien, dann kann sich der Virus auf den gesamten Computer ausbreiten.

Linux.Diesel – Ungefährlicher nicht residenter Linux-Virus, der ausführbare Linux-Dateien infiziert.

Funktionsalgorithmus des Virus: Nach dem Start liest der Virus seinen binären Code aus der Trägerdatei, sucht ausführbare Linux-Dateien in Systemunterverzeichnissen und schreibt seinen Code in die Mitte des Codes jeder Datei, wodurch die Größe des mittleren Segments erhöht wird.

Linux.Silov – Ungefährlicher Linux-Virus, der ausführbare Dateien infiziert. Er besitzt das Format ELF.

Funktionsalgorithmus des Virus: Er verwendet zwei Methoden zur Infektion von Dateien: eine residente und eine nicht residente. Residente Methode: Der Virus verbleibt im Arbeitsspeicher und infiziert im Hintergrundmodus Dateien. Nicht residente Methode: Der Virus sucht auf der Festplatte nach ausführbaren Dateien und infiziert diese.

Linux.Winter – Harmloser nicht residenter Linux-Virus. Er besitzt eine sehr geringe Größe von nur 341 Byte.

Funktionsalgorithmus des Virus: Beim Start übernimmt der Virus die Kontrolle, sucht im aktuellen Verzeichnis ELF-Dateien (ausführbare Linux-Dateien) und infiziert diese.

B.2. Trojanische Programme

Ein Trojanisches Programm ist ein Programm, das Aktionen ausführt, die vom Benutzer nicht sanktioniert wurden. Ein Trojaner installiert sich beim Start im System und überwacht dann das System, wobei der Benutzer keinerlei Meldungen über die Aktionen des Trojaners im System erhält. Der Computer kann dann im Remote-Modus kontrolliert werden.

Die Ausbreitung von Trojanischen Programmen erfolgt über Netzwerke.

Ein prägnanter Vertreter für die Familie der Trojanischen Programme für Unix-Systeme ist **TROJ_IRCKILL** – Dieser Trojaner besteht aus einer Auswahl von Programmwerkzeugen zur Trennung von Benutzern von IRC-Kanälen. Die Auswahl umfasst vier Dienstprogramme für einen Angriff: FLOOD (flood – Überschwemmung), MCB (Multiple Collide BOTs), SUMO BOTs und FLASH – ein besonderer Typ der "Überschwemmung" zur Verwendung in einer UNIX-Umgebung.

Angriffe des Typs FLASH werden zur direkten Trennung des Modems verwendet. Dabei werden **ping**-Befehle mit "fehlerhaften" Daten, die in einer bestimmten Reihenfolge angegeben werden, an eine bestimmte IP-Adresse gesendet. Das Benutzermodem wird diese Daten als Befehl zum Trennen interpretieren und das Internet verlassen. Allerdings kann diese Angriffsart nicht für alle Modemtypen verwendet werden.

Der Angriff MCB erfolgt über IRC-Kanäle. In einem Moment, in dem IRC-Server keine gegenseitige Synchronisation vornehmen können (net split), verdoppelt das Trojanische Programm den Benutzernamen (nickname). Nachdem die Synchronisation zwischen den IRC-Servern wiederhergestellt wurde, wird der betreffende Name fehlerhaft und der Benutzer wird vom IRC-Kanal getrennt.

Der Angriff FLOOD BOTS/SUMO BOTS wird ebenfalls in einem IRC-Netzwerk verwendet, indem zahlreiche Benutzer mit zufällig gewählten Namen (nickname) "geboren" werden. Mit Hilfe dieses Angriffs wird ein IRC-Kanal oder ein Benutzer, der während eines Chats Nachrichten sendet oder empfängt, solange "überflutet", bis die Benutzermaschine eine bestimmte Höchstgrenze für weiterzuleitende Daten erreicht. Danach wird dieser Benutzer ebenfalls vom IRC-Kanal getrennt.

Root kit – Ein Programmpaket, das von Hackern verwendet wird, um root-Zugang auf einen Remote-Computer zu erhalten. Es benutzt die Unix-Standardprogramme ps und ls. Die einzige effektive Methode zur Wiederherstellung nach einem Angriff, der mit Hilfe von Root kit erfolgte, ist die Wiederherstellung wichtiger Daten von einer Sicherheitskopie (Es wird empfohlen regelmäßig Sicherheitskopien anzufertigen), das vollständige Säubern der Festplatte und die Neuinstallation des Systems.

B.3. Netzwürmer

Die zu dieser Kategorie zählenden schädlichen Programme schreiben sich nicht in ausführbare Objekte ein, sondern kopieren sich in Netzwerkressourcen. Ihre Bezeichnung erhielt diese Kategorie eben auf Grund der für Würmer typischen Fähigkeit, durch Netzwerke und andere Informationskanäle zu "kriechen".

Sie dringen aus einem Computernetz in den Speicher eines Computers ein, ermitteln Netzadressen anderer Computer und versenden ihre Kopien an diese Adressen.

Manche Vertreter dieser Klasse legen Arbeitsdateien auf Systemlaufwerken an, funktionieren aber völlig ohne Zugriff auf die Computerressourcen (mit Ausnahme des Arbeitsspeichers).

Worm.Linux.Ramen – Der erste bekannte Wurm, der die Systeme von RedHat Linux infiziert. Er infiziert Remote-Linux-Systeme (RedHat Linux) mit Hilfe eines Pufferüberlaufproblems. Dieses "Loch" in der Software ermöglicht es, ausführbaren Code an einen Remote-Computer zu senden und diesen dort ohne Eingreifen des Administrators (Benutzers) auszuführen.

Ausbreitungsquelle: über Netzwerke in Form des Archivs **tgz**.

Funktionsalgorithmus: Unter Ausnutzung eines Pufferüberlaufproblems sendet der Wurm ein kleines Stück seines Codes an Remote-Computer. Beim Start der Hauptkomponente des Wurms (Datei *start.sh*) werden nacheinander die übrigen Komponenten aufgerufen. Diese ermitteln die Adressen von anzugreifenden Systemen und senden an diese mit Hilfe des "Pufferüberlauf"-Angriffs den "Lademechanismus" des Wurms, der anschließend die restlichen Teile des Wurms nachlädt und den Hauptcode des Wurms startet. Die Startseite des Webserver wird ersetzt durch eine HTML-Datei mit dem Text: "RameN Crew – Hackers loooooooooooooove noodles". Schließlich sendet der Wurm eine E-Mail-Nachricht an zwei Adressen, startet das System neu und beginnt erneut das Internet zu scannen.

Außerdem fügt der Wurm zur Systeminitialisierungsdatei */etc/rc.d/rc.sysinit* den Befehl zum Start seiner Hauptdatei hinzu. Dadurch wird der Wurm bei jedem folgenden Start des infizierten Systems gestartet.

Worm.Linux.Lion – Ein Internet-Wurm, der Linux-Server angreift. Zum Eindringen in einen Computer verwendet der Wurm eine Sicherheitslücke im Service BIND DNS.

Funktionsalgorithmus: Der Wurm scannt das Internet auf der Suche nach Systemen, die eine Sicherheitslücke beim root-Zugriff aufweisen. Beim Fund eines solchen Systems infiziert der Wurm dieses, sammelt Informationen darüber (IP-Adresse, Logins, Kennwörter) in einer Datei

mit dem Namen *mail.log* und sendet die Datei anschließend an die E-Mail-Adresse *1i0nsniffer@china.com*.

Außerdem unternimmt der Wurm Versuche zur Verbindung über das Internet mit der Seite *www.51.net* (Die Domäne *51.net* ist in China registriert) und lädt von dort die Datei *crew.tgz*. Dieses Archiv entpackt sich auf der infizierten Maschine und installiert Prozeduren, bei deren Ausführung der inzwischen erneut infizierte Computer ebenfalls beginnt, die Ressourcen des Internets auf der Suche nach zukünftigen Opfern zu scannen.

mIRC.Acoragil und **mIRC.Simpsalapim** – Die ersten bekannten mIRC-Würmer. Ihre Namen erhielten sie nach den Codewörtern, die von den Würmern verwendet werden: Ist im Text, der über einen Kanal an einen beliebigen Benutzer übertragen wird, die Zeile *Acoragil* enthalten, dann werden alle Benutzer, die mit dem Wurm **mIRC.Acoragil** infiziert sind, automatisch von dem Kanal getrennt. Entsprechend funktioniert auch der Wurm **mIRC.Simpsalapim** – er reagiert auf die Zeile **Simpsalapim**.

Ausbreitungsquelle: über Netzwerke. Mit mIRC-Befehlen versenden die Würmer ihren Code in der Datei *SCRIPT.INI* an jeden neuen Benutzer, der sich mit dem Kanal verbindet.

Funktionsalgorithmus: Die Würmer aktivieren eine Trojanischen Bestandteil. **mIRC.Simpsalapim** enthält einen Code zum Abfangen eines IRC-Kanals: Ist der Inhaber des mIRC-Kanals infiziert, dann übernimmt ein Angreifer mit Hilfe des Codeworts *ananas* die Kontrolle des Kanals.

mIRC.Acoragil versendet mit Hilfe von Codewörtern DOS-, Windows- oder UNIX-Systemdateien. Bestimmte Codewörter wurden so gewählt, dass sie die Aufmerksamkeit der Opfer nicht wecken. z.B. *hi* oder *the*. Eine Modifikation dieses Wurms schickt die UNIX-Kennwortdatei an einen Angreifer.

Worm.Linux.Adm – Ein Internet-Wurm, der Linux-Systeme angreift. Der Wurm sendet ein kleines Stück seines Codes an Remote-Computer, führt diesen dort aus, lädt seinen Hauptcode nach und führt diesen aus.

Ausbreitungsquelle: über Netzwerke. Er verbreitet seine Kopien (infiziert Remote-Linux-Systeme) mit Hilfe einer "Lücke" im Sicherheitssystem von Linux (die sogenannte "Pufferüberlauf"-Lücke). Diese Lücke ermöglicht es, einen ausführbaren Code auf einen Remote-Computer zu senden und ihn dort ohne Eingreifen des Administrators (Benutzers) auszuführen.

ANHANG C. KASPERSKY LABS LTD.

Die Firma Kaspersky Labs Ltd. 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 Labs 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 Labs 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 Labs. 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 Labs entwickelt. Unser führendes Produkt, Kaspersky Anti-Virus®, garantiert zuverlässigen Schutz für alle Objekte, die Virenattacken ausgesetzt sind: Computer-Arbeitsplätze, Dateiserver, Mail Exchanger, Firewalls und 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).

Wir bieten eine breite Palette an Zusatzdienstleistungen an, die ein reibungsloses Funktionieren und die problemlose Anpassung unserer Produkte

an die speziellen Bedürfnisse Ihres Unternehmens gewährleisten. Unser Service reicht von der Projektierung bis hin zur Implementierung und Produktbegleitung für komplexe Virenschutzsysteme in Ihrem Unternehmen. Unsere Virendatenbanken werden zweimal täglich aktualisiert. Für unsere Kunden garantieren wir mehrsprachigen technischen Service rund um die Uhr.

C.1. Andere Produkte von Kaspersky Labs

Kaspersky Anti-Virus® Lite

ist das am einfachsten zu handhabende Virenschutzprogramm von Kaspersky Labs zum Schutz Ihres privat daheim genutzten Computers unter Windows 98/Me, Windows 2000/NT Workstation und Windows XP.

Das Programmpaket von Kaspersky Anti-Virus® Lite umfasst:

- **einen Virens Scanner** zur Virenprüfung sämtlicher lokaler Netzwerke auf Anforderung durch den Anwender;
- **den Antivirus-Monitor**, der automatisch in Echtzeit sämtliche benutzten Dateien auf Viren überprüft;
- **ein Modul zur Virenprüfung für die Dateiodner** unter MS Outlook Express auf Anfrage durch den Anwender.

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus® Personal schützt Ihren daheim genutzten Computer unter Windows 98/ME, Windows 2000/NT und Windows XP vor allen bekannten von Virenarten einschließlich Trojanern, Würmern, Skript-Viren, gefährlichen ActiveX- und Java-Applets etc. Das Programm kontrolliert laufend sämtliche Kanäle für möglichen Virenbefall – E-Mail, Internet, Disketten, CDs u.a. und verfügt über eine Funktion zum täglichen Download von Updates über das Internet. Unser einmaliges heuristisches Datenanalyse-System der zweiten Generation erlaubt, unbekannte Viren wirksam zu neutralisieren. Die einfache Benutzeroberfläche ermöglicht eine schnelle Änderung der Einstellungen und sorgt für größtmöglichen Komfort im Umgang mit dem Programm.

Kaspersky Anti-Virus® Personal gewährleistet:

- **die Virenprüfung** der lokalen Laufwerke auf Anfrage durch den Anwender;
- **die automatische Virenprüfung in Echtzeit** für sämtliche benutzten Dateien;

- **die Überprüfung eingehender und ausgehender E-Mails** durch ein im Hintergrund laufendes Filterprogramm.

Kaspersky Anti-Virus® Personal unterstützt mehr als siebenhundert Formate für Archive und komprimierte Dateien, überprüft deren Inhalt auf Viren und eliminiert gefährliche Codes aus ZIP-Archiven.

Kaspersky Anti-Virus® Personal Pro

Dieses Programmpaket wurde speziell entwickelt, um einen vollwertigen Virenschutz für Computer unter Windows 98/ME, Windows 2000/NT, Windows XP zu gewährleisten, die mit den Business-Editionen von MS Office 2000 arbeiten. Kaspersky Anti-Virus® Personal Pro verfügt über eine Funktion zum täglichen Download von Updates für Virendatenbanken und Programmkomponenten. Unser einmaliges heuristisches Datenanalyse-System der zweiten Generation erlaubt, unbekannte Viren wirksam zu neutralisieren. Die einfache Benutzeroberfläche ermöglicht eine schnelle Änderung der Einstellungen und sorgt für größtmöglichen Komfort im Umgang mit dem Programm.

Außer den Funktionen zur Virenprüfung für benutzte Dateien in Echtzeit und auf Anfrage des Anwenders und dem E-Mail-Filter ist Kaspersky Anti-Virus® Personal Pro mit einem **Behaviour Blocker** ausgestattet, der hundertprozentigen Schutz vor Makroviren garantiert.

Kaspersky® Anti-Hacker

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

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

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

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

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

Kaspersky® Security für PDA

Kaspersky® Security für PDA gewährleistet zuverlässigen Virenschutz für Daten auf Handheld-PCs unter Palm OS oder 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® 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 Windows 98/Me, Windows 2000/NT/XP Workstation, Linux.
- *Dateiserver* unter Windows NT 4.0 Server, Windows 2000 Server/Advanced Server, Novell Netware, FreeBSD и OpenBSD, Linux.
- *Mailsysteme* vom Typ Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, Sendmail und Qmail.

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

¹ Je nach Lieferumfang

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

Kaspersky® Corporate Suite

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

Kaspersky® Corporate Suite bietet Rundumschutz² vor Viren für:

- *Computerarbeitsplätze* unter Windows 98/Me, Windows 2000/NT/XP Workstation und Linux.
- *Dateiserver* unter Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD и Linux.
- *Mailsysteme* vom Typ Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim und Qmail.
- *Datenströme, die über Firewalls ein- und ausgehen.*
- *Handheld-PCs.*

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

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

Kaspersky® Anti-Spam

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

Kaspersky® Anti-Spam ist ein Filterprogramm, das, am „Eingang“ des firmeninternen Netzwerks installiert, sämtliche eingehenden Mitteilungen auf

² Je nach Lieferumfang

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.

C.2. Kontaktinformationen

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

Technischer Support	Informationen über den technischen Support finden Sie unter: www.kaspersky.com/supportinter.html
Allgemeine Informationen	WWW: http://www.kaspersky.com/de/ http://www.viruslist.com E-Mail: sales@kaspersky.com

ANHANG D. ENDBENUTZER- LIZENZVERTRAG FÜR KASPERSKY ANTI-VIRUS®

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

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

Dieser EULA ist ein rechtsgültiger Vertrag zwischen Ihnen, dem Besitzer eines Exemplars von Kaspersky Anti-Virus® (entweder als natürlicher oder als juristischer Person) und Kaspersky Labs. Kaspersky Labs 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.
- Sie sind berechtigt, die installierte SOFTWARE ein Jahr lang zu verwenden (Lizenzdauer).

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.

- Vermietung. Sie sind nicht berechtigt, die SOFTWARE zu vermieten, zu verleasen oder zu verleihen.
- Supportleistungen. Nach Kauf der SOFTWARE erhalten Sie sofort das Recht auf die Supportleistungen für die Lizenzdauer. Supportleistungen verstehen sich wie folgt:
 - tägliches Update der Antiviren-Datenbank
 - kostenloses Update der Software
 - kostenlose technische Unterstützung sowohl per e-Mail als auch per Telefon mit Hot-Line-Service
- Viren-Entdeckung und heilende Updates auf Anfrage innerhalb von 48 Stunden.

3. KÜNDIGUNG. Unbeschadet sonstiger Rechte ist Kaspersky Labs 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 Labs.

5. GEWÄHRLEISTUNG. KASPERSKY LABS gewährleistet, dass:

- die SOFTWARE den Spezifikationen im wesentlichen entspricht.
- der Originaldatenträger frei von Material- und Herstellungsfehlern ist.
- das Programm korrekt auf den Datenträger aufgezeichnet ist, die Dokumentation (sämtliche Informationen enthält, die KASPERSKY LABS für die Benutzung der Software für erforderlich hält).
- die SOFTWARE binnen 6 Monaten ab der ersten Installation oder dem ersten Download, falls richtig behandelt, vollfunktionsfähig ist, der in der beiliegenden Dokumentation bestimmten Funktionalität entsprechend.

Die Gewährleistungsfrist beträgt 6 Monate ab der ersten Installation oder dem ersten Download der Software den beiliegenden Dokumentationen von Kaspersky Labs entsprechend. Gewährleistungspflichtige Mängel werden von KASPERSKY LABS oder dessen Lieferanten nach Entdeckung, auf jeden Fall aber vor Ablauf von der Gewährleistungsfrist, dem Ermessen von Kaspersky Labs nach, durch Ersatz, Reparatur, Umtausch oder Rückzahlung beseitigt, falls eine Mangelrüge rechtzeitig an Kaspersky Labs oder dessen Lieferanten gerichtet wurde. KASPERSKY LABS 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 LABS 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 LABS 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 LABS ODER DESSEN LIEFERANTEN AUF DIE MÖGLICHKEIT SOLCHER SCHÄDEN HINGEWIESEN WORDEN IST. DIESER HAFTUNGS AUSSCHLUSS FÜR SCHÄDEN GILT AUCH DANN, WENN ABHILFEMAßNAHMEN IHREN WESENTLICHEN ZWECK VERFEHLEN.

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