

KASPERSKY LAB

Kaspersky Anti-Virus 6.0 for Windows Servers

BENUTZERHANDBUCH

KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

Benutzerhandbuch

© Kaspersky Lab Ltd.

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

Erscheinungsdatum: Juli 2007

Inhalt

KAPITEL 1. BEDROHUNGEN FÜR DIE COMPUTERSICHERHEIT	7
1.1. Bedrohungsquellen	7
1.2. Ausbreitung der Bedrohungen	8
1.3. Arten von Bedrohungen	10
KAPITEL 2. KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS	13
2.1. Was ist neu in Kaspersky Anti-Virus 6.0 for Windows Servers	13
2.2. Die Schutzprinzipien von Kaspersky Anti-Virus 6.0 for Windows Servers	15
2.2.1. Datei-Anti-Virus	15
2.2.2. Aufgaben zur Virensuche	16
2.2.3. Servicefunktionen des Programms	16
2.3. Hardware- und Softwarevoraussetzungen	18
2.4. Lieferumfang	19
2.5. Service für registrierte Benutzer	20
KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-VIRUS 6.0	21
3.1. Installation mit Hilfe des Installationsassistenten	22
3.2. Konfigurationsassistent	26
3.2.1. Verwendung von Objekten, die in Version 5.0 gespeichert wurden	27
3.2.2. Aktivierung des Programms	27
3.2.2.1. Auswahl der Methode zur Aktivierung der Anwendung	28
3.2.2.2. Eingabe des Aktivierungscodes	29
3.2.2.3. Download des Lizenzschlüssels	29
3.2.2.4. Auswahl einer Lizenzschlüsseldatei	29
3.2.2.5. Abschluss der Programmaktivierung	30
3.2.3. Konfiguration der Update-Einstellungen	30
3.2.4. Konfiguration des Zeitplans für die Virenuntersuchung	31
3.2.5. Zugriffsbegrenzung auf das Programm	32
3.2.6. Abschluss des Konfigurationsassistenten	32
3.3. Installation der Anwendung aus der Befehlszeile	33
3.4. Installation über den Gruppenrichtlinienobjekt-Editor (Group Policy Object)	34
3.4.1. Installation der Anwendung	34

3.4.2. Upgrade der Anwendung	35
3.4.3. Löschen der Anwendung	35
3.5. Aktualisierung der Anwendung von Version 5.0 auf Version 6.0	36
KAPITEL 4. PROGRAMMOBERFLÄCHE	37
4.1. Symbol im Infobereich	37
4.2. Kontextmenü	38
4.3. Programmhauptfenster	39
4.4. Konfigurationsfenster der Anwendung	41
KAPITEL 5. ERSTE SCHRITTE	43
5.1. Welchen Schutzstatus hat der Server?	43
5.1.1. Schutzindikatoren	44
5.1.2. Status einer einzelnen Komponente von Kaspersky Anti-Virus	47
5.1.3. Statistik der Programmarbeit	48
5.2. Wie der Server auf Viren untersucht wird	49
5.3. Wie kritische Serverbereiche untersucht werden	50
5.4. Wie eine Datei, ein Ordner oder ein Laufwerk auf Viren untersucht werden	50
5.5. Wie das Programm aktualisiert wird	51
5.6. Was tun, wenn der Schutz nicht funktioniert?	52
KAPITEL 6. KOMPLEXE STEUERUNG DES SCHUTZES	54
6.1. Serverschutz deaktivieren/ aktivieren	54
6.1.1. Serverschutz anhalten	55
6.1.2. Serverschutz vollständig deaktivieren	56
6.1.3. Schutzkomponenten oder Aufgaben anhalten/ beenden	57
6.1.4. Serverschutz wiederherstellen	58
6.1.5. Arbeit mit der Anwendung beenden	58
6.2. Typen der zu kontrollierenden schädlichen Programme	59
6.3. Aufbau einer vertrauenswürdigen Zone	60
6.3.1. Ausnahmeregeln	61
6.3.2. Vertrauenswürdige Anwendungen	65
6.4. Start von Aufgaben mit Rechten eines anderen Benutzerkontos	67
6.5. Konfiguration des Zeitplans für Aufgabenstart und Senden von Benachrichtigungen	69
6.6. Leistungseinstellungen	71
6.7. Multiprozessoren-Konfiguration des Servers	72

KAPITEL 7. VIRENSCHUTZ FÜR DAS DATEISYSTEM DES SERVERS	73
7.1. Auswahl der Sicherheitsstufe für den Dateischutz	74
7.2. Konfiguration des Dateischutzes	76
7.2.1. Festlegen der Typen von zu untersuchenden Dateien	76
7.2.2. Festlegen des Schutzbereichs	79
7.2.3. Anpassen zusätzlicher Parameter	80
7.2.4. Wiederherstellen der Standardparameter für den Dateischutz	83
7.2.5. Auswahl der Aktion für Objekte	83
7.2.6. Benachrichtigungsvorlage anpassen	86
7.3. Aufgeschobene Desinfektion von Objekten	86
KAPITEL 8. VIRENSUCHE AUF DEM SERVER	88
8.1. Steuerung von Aufgaben zur Virensuche	89
8.2. Erstellen einer Liste der Untersuchungsobjekte	89
8.3. Erstellen von Aufgaben zur Virensuche	91
8.4. Konfiguration von Aufgaben zur Virensuche	92
8.4.1. Auswahl der Sicherheitsstufe	93
8.4.2. Festlegen der zu untersuchenden Objekttypen	94
8.4.3. Wiederherstellen der standardmäßigen Untersuchungseinstellungen	98
8.4.4. Auswahl der Aktion für Objekte	98
8.4.5. Zusätzliche Optionen für die Virensuche	100
8.4.6. Festlegen einheitlicher Untersuchungsparameter für alle Aufgaben	102
KAPITEL 9. TESTEN DER ARBEIT VON KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS	103
9.1. EICAR-"Testvirus" und seine Modifikationen	103
9.2. Testen des Datei-Anti-Virus	105
9.3. Testen einer Aufgabe zur Virensuche	106
KAPITEL 10. UPDATE DES PROGRAMMS	107
10.1. Starten des Updates	108
10.2. Rückkehr zum vorherigen Update	109
10.3. Erstellen einer Update-Aufgabe	110
10.4. Update-Einstellungen	111
10.4.1. Auswahl der Updatequelle	111
10.4.2. Auswahl von Updatemodus und Update-Objekt	114
10.4.3. Konfiguration der Verbindungsparameter	116
10.4.4. Update-Verteilung	118

10.4.5. Aktionen nach dem Programm-Update	119
KAPITEL 11. ZUSÄTZLICHE OPTIONEN	121
11.1. Quarantäne für möglicherweise infizierte Objekte	122
11.1.1. Aktionen mit Objekten in der Quarantäne	123
11.1.2. Konfiguration der Quarantäne-Einstellungen	126
11.2. Sicherungskopien gefährlicher Objekte	126
11.2.1. Aktionen mit Sicherungskopien	127
11.2.2. Konfiguration der Backup-Einstellungen	129
11.3. Berichte	129
11.3.1. Konfiguration der Berichtsparameter	132
11.3.2. Registerkarte <i>Gefunden</i>	133
11.3.3. Registerkarte <i>Ereignisse</i>	134
11.3.4. Registerkarte <i>Statistik</i>	135
11.3.5. Registerkarte <i>Einstellungen</i>	135
11.3.6. Registerkarte <i>Gesperrte Benutzer</i>	136
11.4. Allgemeine Informationen zum Programm	137
11.5. Lizenzverwaltung	138
11.6. Technischer Support für Benutzer	140
11.7. Konfiguration der Oberfläche von Kaspersky Anti-Virus	142
11.8. Verwendung zusätzlicher Dienste	144
11.8.1. Benachrichtigungen über die Ereignisse von Kaspersky Anti-Virus	145
11.8.1.1. Ereignistypen und Methoden zum Senden von Benachrichtigungen	146
11.8.1.2. Konfiguration des Sendens von Benachrichtigungen per E-Mail	147
11.8.1.3. Parameter des Ereignisberichts	149
11.8.2. Selbstschutz und Zugriffsbeschränkung für das Programm	149
11.8.3. Lösen von Kompatibilitätsproblemen von Kaspersky Anti-Virus mit anderen Anwendungen	151
11.9. Export/Import der Einstellungen von Kaspersky Anti-Virus	152
11.10. Wiederherstellen der Standardeinstellungen	152
KAPITEL 12. VERWALTUNG DER ANWENDUNG ÜBER KASPERSKY ADMINISTRATION KIT	154
12.1. Anwendung verwalten	156
12.1.1. Anwendung starten / beenden	157
12.1.2. Anwendungsparameter anpassen	158

KAPITEL 13. ARBEIT MIT DEM PROGRAMM AUS DER BEFEHLSZEILE	173
13.1. Aktivierung der Anwendung	175
13.2. Steuerung von Datei-Anti-Virus und Aufgaben	175
13.3. Virenuntersuchung von Objekten	178
13.4. Programm-Update.....	183
13.5. Rollback des letzten Programm-Updates.....	184
13.6. Export von Parametern	185
13.7. Import von Parametern	186
13.8. Anwendung starten	187
13.9. Anwendung beenden	187
13.10. Anlegen einer Tracing-Datei	188
13.11. Anzeige der Hilfe	188
13.12. Rückgabecodes der Befehlszeile	189
KAPITEL 14. PROGRAMM ÄNDERN, REPARIEREN ODER LÖSCHEN	190
14.1. Ändern, Reparieren oder Löschen des Programms mit Hilfe des Installationsassistenten.....	190
14.2. Deinstallation des Programms aus der Befehlszeile.....	193
ANHANG A. ZUSÄTZLICHE INFORMATIONEN	194
A.1. Liste der Objekte, die nach Erweiterung untersucht werden.....	194
A.2. Zulässige Ausschlussmasken für Dateien	196
A.3. Zulässige Ausschlussmasken nach der Klassifikation der Viren- Enzyklopädie.....	198
A.4. Beschreibung von Parametern der Datei <i>setup.ini</i>	199
ANHANG B. KASPERSKY LAB.....	201
B.1. Andere Produkte von Kaspersky Lab	202
B.2. Kontaktinformationen	214
ANHANG C. ENDBENUTZER-LIZENZVERTRAG.....	215

KAPITEL 1. BEDROHUNGEN FÜR DIE COMPUTERSICHERHEIT

Aufgrund der rasanten Entwicklung der Informationstechnologien und ihrer Präsenz in allen Lebensbereichen ist die Zahl der Verbrechen, die sich gegen die Informationssicherheit richten, gestiegen.

Auf besonderes Interesse von Cyber-Verbrechern stößt die Tätigkeit staatlicher Einrichtungen und kommerzieller Unternehmen. Ziele sind Diebstahl und Verkauf vertraulicher Informationen, Rufschädigung, Schädigung der Netzwerke und Zugang zu Informationsressourcen einer Organisation. Solche Aktionen verursachen enormen materiellen Schaden und Imageverlust. Diesem Risiko unterliegen nicht nur Großunternehmen, sondern auch private Nutzer. Mit Hilfe unterschiedlicher Mittel verschaffen sich Verbrecher Zugriff auf persönliche Daten.

Diesem Risiko unterliegen nicht nur Großunternehmen, sondern auch private Nutzer. Mit Hilfe unterschiedlicher Mittel verschaffen sich Verbrecher Zugriff auf persönliche Daten wie Kontonummern, Kreditkartennummern und Kennwörter, machen das System funktionsunfähig oder erhalten vollständigen Zugang auf den Computer. Ein solcher Computer kann als Teil eines so genannten Zombie-Netztes benutzt werden, eines Netzwerks von infizierten Computern, das dazu dient, Angriffe auf Server auszuüben, Spam zu versenden, vertrauliche Informationen zu sammeln, neue Viren und Trojaner zu verbreiten.

Es ist heute allgemein anerkannt, dass Informationen ein wertvolles Gut sind und geschützt werden müssen. Gleichzeitig sollen Informationen aber für einen bestimmten Kreis von Benutzern zugänglich sein (beispielsweise für Mitarbeiter, Kunden und Geschäftspartner). Daraus ergibt sich die Notwendigkeit eines komplexen Systems zur Informationssicherheit. Dieses System muss alle bestehenden Bedrohungsquellen berücksichtigen (menschliche, technische und unvorhersehbare Faktoren) und das gesamte Spektrum von Schutzmaßnahmen verwenden, wozu physikalische, administrative und mit Software und Technik verbundene Schutzwerkzeuge zählen.

1.1. Bedrohungsquellen

Als Quellen für die Bedrohung der Informationssicherheit können eine Einzelperson oder eine Personengruppe, sowie Phänomene, die von menschlicher Tätigkeit unabhängig sind, auftreten. Dadurch lassen sich drei Gruppen von Bedrohungsquellen unterscheiden:

- **Menschlicher Faktor.** Diese Gruppe von Bedrohungen steht mit den Aktionen eines Menschen in Verbindung, der rechtmäßigen oder unerlaubten Zugriff auf Informationen besitzt. Die Bedrohungen dieser Gruppe können unterteilt werden in:
 - *externe:* Dazu zählen Aktionen von Cyber-Verbrechern, Hackern, Internetbetrügern und böswilligen Partnern.
 - *interne:* Hierzu gehören die Aktionen von Firmenmitarbeitern. Die Handlungen dieser Personen können vorsätzlich oder zufällig sein.
- **Technischer Faktor.** Diese Gruppe von Bedrohungen ist mit technischen Problemen verbunden. Dazu zählen veraltete Geräte sowie mindere Qualität der benutzten Software und Hardware. Diese Faktoren können zur Fehlfunktion von Geräten und zum teilweisen Verlust von Informationen führen.
- **Unvorhersehbarer Faktor.** Diese Gruppe der Bedrohungen umfasst Naturkatastrophen und sonstige Umstände höherer Gewalt, die nicht von menschlicher Tätigkeit abhängig sind.

Alle drei Bedrohungsquellen sollten bei der Organisation eines Schutzsystems berücksichtigt werden. In diesem Handbuch beschreiben wir allerdings nur die Quelle, die direkt mit der Tätigkeit der Firma Kaspersky Lab verbunden ist: die externen Bedrohungen, die mit menschlicher Tätigkeit in Verbindung stehen.

1.2. Ausbreitung der Bedrohungen

Die Entwicklung der modernen Computertechnologien und Kommunikationsmittel verleiht Angreifern die Möglichkeit, unterschiedliche Verbreitungsquellen für Bedrohungen zu benutzen, die im Folgenden genauer beschrieben werden:

Internet

Das Internet zeichnet sich dadurch aus, dass es niemandem gehört und keine territorialen Grenzen besitzt. Das ermöglicht die Entwicklung zahlreicher Web-Ressourcen und den Austausch von Informationen. Jeder Mensch kann Zugriff auf die im Internet gespeicherten Daten erhalten oder seinen eigenen Web-Service anbieten.

Allerdings wird Angreifern eben durch diese Besonderheiten ermöglicht, im Internet Verbrechen zu verüben, die nur schwer erkannt und verfolgt werden können.

Böswillige Personen platzieren Viren und andere Schadprogramme auf Webseiten und tarnen diese als nützliche und kostenlose Software. Außerdem können Skripte, die beim Öffnen von Webseiten automatisch

gestartet werden, schädliche Aktionen auf dem Computer ausführen, unter anderem Modifikation der Systemregistrierung, Diebstahl persönlicher Daten und Installation schädlicher Programme.

Mit Netzwerktechnologien lassen sich Angriffe auf Unternehmensserver verwirklichen. Das Ergebnis solcher Angriffe kann der vollständige Zugriff auf gespeicherte Informationen, sowie der Missbrauch des Rechners als Teil eines Zombie-Netztes sein.

Intranet

Das Intranet ist ein lokales Netzwerk, das den speziellen Erfordernissen der Informationsverwaltung in einem Unternehmen oder in einem privaten Netzwerk entspricht. Ein Intranet stellt einen einheitlichen Raum zum Speichern, Austausch und Zugriff auf Informationen für alle Computer eines Netzwerks dar. Ist ein Computer des Netzwerks infiziert, dann unterliegen die übrigen Computer einem hohen Infektionsrisiko. Um das zu verhindern, müssen nicht nur die Grenzen des Netzwerks geschützt werden, sondern auch jeder einzelne Computer.

E-Mail

Da praktisch auf jedem Computer ein Mailprogramm installiert ist und schädliche Programme auf der Suche nach neuen Opfern den Inhalt elektronischer Adressbücher verwenden, entstehen günstige Bedingungen für die Ausbreitung von Schadprogrammen. Der Benutzer eines infizierten Computers verschickt – ohne selbst Verdacht zu schöpfen – infizierte E-Mails an Adressaten, die ihrerseits neue infizierte Mails weiterschicken usw. Häufig gelangt ein infiziertes Dokument oder eine Datei durch Unachtsamkeit in eine Verteilerliste für kommerzielle Informationen eines Großunternehmens. In diesem Fall sind nicht nur fünf, sondern hunderte oder tausende von Abonnenten solcher Verteiler betroffen, welche die infizierten Dateien wiederum an zehntausende ihrer Abonnenten weiterreichen.

Wechseldatenträger

Zum Speichern und zur Weitergabe von Informationen sind CDs/DVDs, Disketten und Speichererweiterungskarten (Flash-Cards) weit verbreitet.

Wenn Sie eine Datei, die schädlichen Code enthält, von einem Wechseldatenträger starten, können die auf Ihrem Computer gespeicherten Daten beschädigt werden und ein Virus kann sich auf andere Computerlaufwerke oder Netzwerkcomputer ausbreiten.

1.3. Arten von Bedrohungen

Heutzutage existiert eine große Menge von Bedrohungen, denen Ihr Computer ausgesetzt ist. Dieser Abschnitt bietet eine ausführliche Beschreibung der Bedrohungen, die von Kaspersky Anti-Virus blockiert werden:

Würmer

Diese Kategorie der schädlichen Programme benutzt in erster Linie die Schwachstellen von Betriebssystemen, um sich auszubreiten. Die Klasse erhielt ihren Namen aufgrund ihrer wurmähnlichen Fähigkeit, von Computer zu Computer "weiter zu kriechen", wobei Netzwerke und E-Mails benutzt werden. Deshalb besitzen Würmer eine relativ hohe Ausbreitungsgeschwindigkeit.

Würmer dringen in einen Computer ein, suchen nach Netzwerkadressen anderer Computer und versenden ihre Kopien an diese Adressen. Neben Netzwerkadressen verwenden Würmer häufig auch Daten aus dem Adressbuch von Mailprogrammen. Vertreter dieser Klasse der schädlichen Programme erstellen teilweise Arbeitsdateien auf Systemlaufwerken, können aber auch ohne jeden Zugriff auf Computerressourcen (mit Ausnahme des Arbeitsspeichers) funktionieren.

Viren

Viren sind Programme, die andere Programme infizieren, indem sie ihnen den eigenen Code hinzufügen, um beim Start infizierter Dateien die Kontrolle zu übernehmen. Diese einfache Definition nennt die *Infektion* als von einem Virus ausgeführte Basisaktion.

Trojaner

Trojaner sind Programme, die auf infizierten Computern unerlaubte Aktionen ausführen, d.h. abhängig von bestimmten Bedingungen die Informationen auf Laufwerken vernichten, das System zum Absturz bringen, vertrauliche Informationen stehlen usw. Diese Klasse der schädlichen Programme fällt nicht unter die traditionelle Definition eines Virus (d.h. andere Programme oder Daten werden nicht infiziert). Trojanische Programme können nicht selbständig in einen Computer eindringen. Sie werden getarnt als nützliche Software verbreitet. Dabei kann der verursachte Schaden den eines traditionellen Virusangriffs erheblich übersteigen.

In letzter Zeit haben sich Würmer zum häufigsten Typ der Schadprogramme entwickelt, die Computerdaten beschädigen. Danach folgen Viren und Trojaner-Programme. Einige schädliche Programme verbinden die Merkmale von zwei oder gar drei der oben genannten Klassen.

Adware

Adware sind Programme, die ohne Wissen des Benutzers in anderer Software enthalten sind und die Präsentation von Werbung zum Ziel haben. In der Regel ist Adware in Programme integriert, die kostenlos verbreitet werden. Die Werbung erscheint auf der Benutzeroberfläche. Häufig sammeln solche Programme persönliche Benutzerdaten und senden Sie an den Programmautor, ändern bestimmte Browser-Einstellungen (Start- und Such-Seiten, Sicherheitsstufe u.a.), und verursachen vom Benutzer unkontrollierten Datenverkehr. Dadurch kann die Sicherheitsrichtlinie verletzt werden und es können direkte finanzielle Verluste entstehen.

Spyware

Spyware sammelt heimlich Informationen über einen bestimmten Benutzer oder eine Organisation zu sammeln. Die Existenz von Spyware auf einem Computer kann völlig unbemerkt bleiben. In der Regel verfolgt Spyware folgende Ziele:

- Überwachen der Benutzeraktionen auf einem Computer
- Sammeln von Informationen über den Festplatteninhalt. In diesem Fall werden meistens bestimmte Ordner und die Systemregistrierung des Computers gescannt, um eine Liste der installierten Software zu erstellen.
- Sammeln von Informationen über Verbindungsqualität, Verbindungsmethode, Modemgeschwindigkeit usw.

Potentiell gefährliche Anwendungen (Riskware)

Als potentiell gefährlich gelten Anwendungen, die nicht über schädliche Funktionen verfügen, die aber Teil der Entwicklungsumgebung eines Schadprogramms sein können oder von Angreifern als Hilfskomponenten schädlicher Programme verwendet werden können. Zu dieser Kategorie zählen Programme, die Schwachstellen und Fehler enthalten, sowie Dienstprogramme zur Remote-Administration, Programme zum automatischen Umschalten der Tastaturbelegung, IRC-Clients, FTP-Server und alle Dienstprogramme zum Beenden von Prozessen oder zum Verstecken der Arbeit von Prozessen.

Ein weiterer Typ von Schadprogrammen, die solchen Programmen wie Adware, Spyware und Riskware nahe stehen, sind Programme die in den auf einem Computer installierten Browser integriert werden.

Scherzprogramme (Jokes)

Jokes sind Programme, die dem Computer keinen direkten Schaden zufügen, sondern Meldungen darüber anzeigen, dass bereits Schaden verursacht wurde oder unter bestimmten Bedingungen Schaden angerichtet wird. Solche Programme warnen häufig vor fiktiven Gefahren.

So kann beispielsweise eine Meldung angezeigt werden, die über das Formatieren der Festplatte informiert (obwohl dies nicht der Wirklichkeit entspricht) oder einen Virusfund in Dateien meldet, die aber tatsächlich virenfrei sind.

Rootkits

Rootkits sind Dienstprogramme, die der Tarnung von schädlichen Prozessen dienen. Sie maskieren schädliche Programme, um zu vermeiden, dass diese von Antiviren-Programmen gefunden werden. Rootkits sind außerdem fähig, das Betriebssystem des Computers zu modifizieren und dessen Grundfunktionen zu ersetzen, wodurch sie die eigene Existenz und Aktionen, die ein Angreifer auf dem infizierten Computer vornimmt, verbergen.

Andere gefährliche Programme

Dazu zählen Programme, die der Organisation von DoS-Angriffen auf entfernte Server, dem Eindringen in andere Computer und dem Erstellen schädlicher Software dienen. Zu diesen Programmen gehören Hackerdienstprogramme (Hack-Tools), Virenkonstrukteure, Schwachstellen-Scanner, Programme zum Kennwort-Diebstahl sowie sonstige Programme zum Einbruch in Netzwerkressourcen oder zum Eindringen in ein angegriffenes System.

Hinweis!

Ab hier wird in diesem Handbuch zur Bezeichnung von schädlichen und gefährlichen Programmen der Begriff "Virus" verwendet. Die konkrete Art eines Schadprogramms wird nur dann extra genannt, wenn es erforderlich ist.

KAPITEL 2. KASPERSKY ANTI-VIRUS 6.0 FOR WINDOWS SERVERS

Kaspersky Anti-Virus 6.0 for Windows Servers ist die neue Generation des Informationsschutzes.

2.1. Was ist neu in Kaspersky Anti-Virus 6.0 for Windows Servers

Im Folgenden werden die neuen Optionen von Kaspersky Anti-Virus 6.0 for Windows Servers ausführlich beschrieben.

Neuerungen im Schutz

- Die Technologie für den Schutz der Dateien auf dem Benutzercomputer wurde verbessert: Sie können nun die Belastung des Zentralprozessors und der Laufwerkssysteme senken und die Untersuchungsgeschwindigkeit erhöhen. Dies wird durch die Verwendung der Technologien iChecker™ und iSwift™ erreicht. Dieser Modus schließt die wiederholte Prüfung von Dateien aus.
- Der Prozess zur Virensuche wird nun Ihrer Arbeit auf dem Computer untergeordnet. Eine Untersuchung kann relativ viel Zeit und Systemressourcen beanspruchen, trotzdem kann der Administrator gleichzeitig seine Arbeit ausführen. Wenn das Ausführen einer bestimmten Operation Systemressourcen erfordert, wird die Virensuche bis zum Abschluss dieser Operation angehalten. Danach wird die Untersuchung an der Stelle fortgesetzt, an dem sie angehalten wurde.
- Der Untersuchung kritischer Computerbereiche, deren Infektion ernste Folgen haben kann, ist eine separate Aufgabe zugeordnet. Sie können diese Aufgabe so konfigurieren, dass sie jedes Mal beim Systemstart automatisch gestartet wird.
- Die Funktion zur Benachrichtigung des Benutzers (s. Pkt. 11.8.1 auf S. 145) über bestimmte Ereignisse während der Programmarbeit wurde erweitert. Für jeden Ereignistyp kann eine Benachrichtigungsmethode festgelegt werden: E-Mail-Nachricht, Audiosignal, Pop-upmeldung, Eintrag im Ereignisbericht.

- Eine Technologie zum Selbstschutz der Anwendung, zum Schutz vor unerlaubter Fernsteuerung des Anwendungsdiensts, zum Schutz der Anwendungsdateien vor unerlaubtem Zugriff und Änderungen sowie zum Kennwortschutz für den Zugriff auf die Anwendungseinstellungen wurde hinzugefügt. Dadurch kann verhindert werden, dass schädliche Programme, Angreifer oder unqualifizierte Benutzer den Schutz ausschalten.

Neuerungen auf der Programmoberfläche

- Auf der neuen Oberfläche von Kaspersky Anti-Virus ist der einfache und komfortable Zugriff auf alle Programmfunktionen realisiert. Außerdem lässt sich das Programmdesign durch die Verwendung eigener grafischer Elemente und Farbschemen anpassen.
- Bei der Arbeit mit dem Programm erhalten Sie vollständige Informationen: Kaspersky Anti-Virus zeigt Meldungen über den Schutzstatus an, begleitet seine Arbeit durch Kommentare sowie Tipps und besitzt ein ausführliches Hilfesystem.

Neuerungen beim Programm-Update

- In dieser Anwendungsversion wurde eine optimierte Updateprozedur realisiert: Kaspersky Anti-Virus kontrolliert nun automatisch, ob an der Updatequelle ein neues Updatepaket vorhanden ist. Wenn neue Updates gefunden werden, lädt die Anwendung sie herunter und installiert sie auf dem Computer.
- Nur fehlende Updates werden heruntergeladen. Dadurch lässt sich das Volumen des beim Update notwendigen Netzwerkverkehrs bis um das Zehnfache verringern.
- Die Aktualisierung erfolgt von der effektivsten Updatequelle.
- Eine Option zum Rollback von Updates wurde realisiert. Dadurch wird beispielsweise bei einer Beschädigung von Dateien oder bei einem Kopierfehler erlaubt, zur vorhergehenden Version der Bedrohungssignaturen zurückzukehren.
- Eine Option zum Verwenden eines Diensts für die Update-Verteilung in einen lokalen Ordner wurde hinzugefügt. Wird anderen Netzwerkcomputern Zugriff auf den Ordner gewährt, dann lässt sich Internet-Datenverkehr einsparen.

2.2. Die Schutzprinzipien von Kaspersky Anti-Virus 6.0 for Windows Servers

Der Schutz von Kaspersky Anti-Virus umfasst:

- Datei-Anti-Virus (s. Pkt. 2.2.1 auf S. 15), der die Kontrolle über die Objekte des Computerdateisystems im Echtzeitmodus gewährleistet.
- Aufgaben zur Virensuche (s. Pkt. 2.2.2 auf S. 16), mit deren Hilfe die Untersuchung des Computers und einzelner Dateien, Ordner, Laufwerke oder Bereiche ausgeführt wird.
- Servicefunktionen (s. Pkt. 2.2.3 auf S. 16), die Informationen über die Arbeit mit dem Programm bieten und es erlauben, die Programmfunktionalität zu erweitern.

2.2.1. Datei-Anti-Virus

Der Echtzeitschutz des Servers wird mit Hilfe von **Datei-Anti-Virus** gewährleistet.

Das Dateisystem kann Viren und andere gefährliche Programme enthalten. Nachdem Schadprogramme über einen Wechseldatenträger oder das Internet eingedrungen sind, können sie sich jahrelang im Dateisystem befinden, ohne dass ihre Existenz bemerkt wird. Sobald eine infizierte Datei aber geöffnet wird, kann der Virus aktiv werden.

Datei-Anti-Virus ist eine Komponente, die das Dateisystem des Computers kontrolliert. Er untersucht alle Dateien, die auf dem Server und auf allen angeschlossenen Laufwerken geöffnet, gestartet und gespeichert werden. Jeder Zugriff auf eine Datei wird von Kaspersky Anti-Virus abgefangen und die Datei wird auf die Existenz bekannter Viren untersucht. Die weitere Arbeit mit der Datei ist nur dann möglich, wenn die Datei virenfrei ist oder von Kaspersky Anti-Virus erfolgreich desinfiziert wurde. Wenn die Desinfektion der Datei aus bestimmten Gründen nicht möglich ist, wird sie gelöscht, wobei eine Kopie der Datei im Backup (s. Pkt. 11.2 auf S. 126) abgelegt oder in der Quarantäne (s. Pkt. 11.1 auf S. 122) gespeichert wird.

2.2.2. Aufgaben zur Virensuche

Neben dem Echtzeitschutz mit Hilfe von Datei-Anti-Virus aller Quellen, aus denen Schadprogramme eindringen können, ist es sehr wichtig, regelmäßig die vollständige Virenuntersuchung Ihres Computers durchzuführen. Das ist erforderlich, um zu verhindern, dass sich schädliche Programme ausbreiten, die nicht von Datei-Anti-Virus erkannt wurden, weil beispielsweise eine zu niedrige Schutzstufe eingestellt war.

Zur Virensuche verfügt Kaspersky Anti-Virus über folgende Aufgaben:

Kritische Bereiche

Virenuntersuchung aller kritischen Computerbereiche. Dazu zählen: Systemspeicher, Objekte, die beim Systemstart ausgeführt werden, Laufwerksbootsektoren und die Systemverzeichnisse von *Microsoft Windows*. Das Ziel dieser Aufgaben besteht darin, aktive Viren im System schnell zu erkennen, ohne den Computer vollständig zu untersuchen.

Arbeitsplatz

Virensuche auf Ihrem Computer mit sorgfältiger Untersuchung aller angeschlossenen Laufwerke, des Arbeitsspeichers und der Dateien.

Autostart-Objekte

Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden, sowie des Arbeitsspeichers und der Laufwerksbootsektoren.

Außerdem besteht die Möglichkeit, andere Aufgaben zur Virensuche zu erstellen und einen Startzeitplan dafür anzulegen.

2.2.3. Servicefunktionen des Programms

Kaspersky Anti-Virus verfügt über eine Reihe von Servicefunktionen. Sie dienen dazu, den aktuellen Zustand des Programms aufrechtzuerhalten, die Optionen des Programms zu erweitern und bei der Arbeit Hilfe zu leisten.

Update

Um stets bereit zu sein, Viren oder andere gefährliche Programme unschädlich zu machen, muss der aktuelle Zustand von Kaspersky Anti-Virus aufrechterhalten werden. Dazu ist die Komponente *Update* vorgesehen. Sie dient zur Aktualisierung der Bedrohungssignaturen und Programm-Module von Kaspersky Anti-Virus, die bei der Arbeit des Programms verwendet werden.

Der Dienst zum Verteilen von Updates erlaubt es, die von den Kaspersky-Lab-Servern heruntergeladenen Updates für die Datenbanken der Bedrohungssignaturen sowie für die Programm-Module in einem lokalen Ordner zu speichern, um dann anderen Netzwerkcomputern den Zugriff auf diesen Ordner zu gewähren und dadurch Internet-Datenverkehr einzusparen.

Datenverwaltung

Während der Arbeit des Programms wird für Datei-Anti-Virus, für die Aufgabe zur Virensuche und für Programm-Updates ein Bericht erstellt. Er enthält Informationen über die ausgeführten Operationen und Arbeitsergebnisse. Durch die Verwendung der Funktion *Berichte* können Sie sich jederzeit Details über die Arbeit einer beliebigen Komponente von Kaspersky Anti-Virus informieren. Beim Auftreten von Problemen können Berichte an Kaspersky Lab gesendet werden, um die Situation durch unsere Spezialisten zu analysieren und Ihnen so schnell wie möglich zu helfen.

Alle Objekte, die hinsichtlich der Sicherheit verdächtig sind, werden von Kaspersky Anti-Virus in den speziell dafür vorgesehenen *Quarantäne-Speicher* verschoben. Sie werden in verschlüsselter Form gespeichert, um eine Infektion des Computers zu vermeiden. Sie können diese Objekte auf Viren untersuchen, am ursprünglichen Ort wiederherstellen, löschen und der Quarantäne selbständig Objekte hinzufügen. Alle Objekte, die sich aufgrund von Ergebnissen der Virenuntersuchung als virenfrei erweisen, werden automatisch am ursprünglichen Ort wiederhergestellt.

Im *Backup* werden Kopien der vom Programm desinfizierten und gelöschten Objekte gespeichert. Diese Kopien werden erstellt, um bei Bedarf Objekte oder ein Bild der Infektion wiederherzustellen. Die Sicherungskopien werden in verschlüsselter Form gespeichert, um eine Infektion des Computers zu vermeiden.

Sie können ein Objekt aus dem Backup am ursprünglichen Ort wiederherstellen oder die Kopie löschen.

Support

Alle registrierten Benutzer von Kaspersky Anti-Virus können den Technischen Support-Service in Anspruch nehmen. Verwenden Sie die Funktion *Support*, um zu erfahren, wo Sie technische Unterstützung erhalten können.

Mit Hilfe der entsprechenden Links gelangen Sie zum Forum für die Benutzer von Kaspersky-Lab-Produkten und können eine Liste mit häufigen Fragen (FAQ) konsultieren, die Ihnen bei der Lösung eines Problems behilflich sein können. Außerdem können Sie eine Nachricht über einen Fehler oder ein Feedback über die Arbeit der Anwendung an

den technischen Kundendienst schicken. Dazu dient ein spezielles Formular auf der Webseite.

Daneben steht Ihnen der Online-Service des technischen Kundendienstes zur Verfügung. Natürlich sind unsere Mitarbeiter jederzeit bereit, Ihnen telefonisch bei der Arbeit mit Kaspersky Anti-Virus zu helfen.

2.3. Hardware- und Softwarevoraussetzungen

Um die normale Funktionsfähigkeit von Kaspersky Anti-Virus zu gewährleisten, muss der Computer folgende Systemvoraussetzungen erfüllen.

Allgemeine Voraussetzungen:

- 50 MB freier Speicher auf der Festplatte
- CD-ROM-Laufwerk (zur Installation von Kaspersky Anti-Virus von der Distributions-CD).
- Microsoft Internet Explorer Version 5.5 oder höher (für das Update der Bedrohungssignaturen und Programm-Module über das Internet)
- Microsoft Windows Installer 2.0.

Betriebssystem:

- Microsoft Windows 2000 Server/Advanced Server Service Pack 4 oder höher, alle aktuellen Updates.
- Microsoft Windows NT Server 4.0 Service Pack 6a.
- Microsoft Windows Server 2003 Standard/Enterprise Edition, Microsoft Windows Server 2003 Web Edition, Microsoft Windows Storage Server 2003, Microsoft Small Business Server 2003, alle Service Packs, alle aktuellen Updates.
- Microsoft Windows Server 2003 R2 Standard x64 Edition, Microsoft Windows Server 2003 R2 Enterprise x64 Edition, Microsoft Windows Server 2003 R2 Standard Edition, Microsoft Windows Server 2003 R2 Enterprise Edition.

2.4. Lieferumfang

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

Wenn Sie das Produkt als verpackte Variante erwerben, umfasst der Lieferumfang des Softwareprodukts die folgenden Elemente:

- Versiegelter Umschlag mit Installations-CD, auf der die Dateien der Software gespeichert sind.
- Lizenzschlüssel, der in der Distribution enthalten oder auf einer speziellen Diskette gespeichert ist, oder Aktivierungscode für die Anwendung, der auf dem Umschlag mit der Installations-CD aufgeklebt ist.
- Benutzerhandbuch
- Lizenzvertrag.

Bitte lesen Sie vor der Installation sorgfältig den Lizenzvertrag im Anhang des Handbuchs.

Beim Kauf von Kaspersky Anti-Virus in einem Online-Shop kopieren Sie das Produkt von der Kaspersky-Lab-Webseite (Abschnitt **Downloads** → **Produkte herunterladen**). Das Benutzerhandbuch kann aus dem Abschnitt **Downloads** → **Dokumentationen** heruntergeladen werden.

Der Lizenzschlüssel oder der Aktivierungscode wird Ihnen nach Eingang der Bezahlung per E-Mail zugeschickt.

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

Bitte lesen Sie den Lizenzvertrag sorgfältig!

Wenn Sie den Bedingungen des Lizenzvertrags nicht zustimmen, können Sie die Packung mit dem Produkt an den Händler zurückgeben, bei dem Sie erworben wurde, und den für das Produkt bezahlten Betrag zurückerhalten. Dies gilt nur unter der Voraussetzung, dass der Umschlag mit der Installations-CD (oder den Disketten) noch versiegelt ist

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

2.5. Service für registrierte Benutzer

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

Durch die Aktivierung des Programms werden Sie zum registrierten Programmbenutzer und können während des Zeitraums der Lizenzgültigkeit folgende Dienste in Anspruch nehmen:

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

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

KAPITEL 3. INSTALLATION VON KASPERSKY ANTI-VIRUS 6.0

Es bestehen mehrere Möglichkeiten, um Kaspersky Anti-Virus 6.0 for Windows Servers auf dem Computer zu installieren:

- lokale Installation – Das Programm wird auf einem einzelnen Computer installiert. Um die Installation durchzuführen, ist der direkte Zugriff auf diesen Computer erforderlich. Für die lokale Installation stehen zwei Modi zur Verfügung:
 - interaktiver Modus mit Hilfe des Installationsassistenten (s. Pkt. 3.1 auf S. 22). In diesem Modus sind während der Installation bestimmte Aktionen des Benutzers erforderlich.
 - Silent-Modus. Hierbei wird die Installation aus der Befehlszeile gestartet und erfordert während der Installation keine weiteren Aktionen des Benutzers (s. Pkt. 3.3 auf S. 33).
- Remote-Installation – Das Programm wird auf einem Netzwerkcomputer installiert. Die Installation wird vom Arbeitsplatz des Administrators aus ferngesteuert. Dabei werden verwendet:
 - das Softwarepaket Kaspersky Administration Kit (siehe "Handbuch zum Einrichten von Kaspersky Administration Kit")
 - Domänen-Gruppenrichtlinien für Microsoft Windows Server 2000/2003 (s. Pkt. 3.4 auf S. 34).

Es wird empfohlen, vor dem Beginn der Installation von Kaspersky Anti-Virus (auch bei der Remote-Installation) alle laufenden Anwendungen zu beenden.

Wenn auf Ihrem Computer bereits Kaspersky Anti-Virus Version 5.0 installiert ist, erfolgt während des Installationsvorgangs das Upgrade auf Version 6.0, wobei die alte Version entfernt wird (Details s. Pkt. 3.5 auf S. 36). Die Aktualisierung von einer 6.0-Version zu einer anderen 6.0-Version weist keine Besonderheiten auf.

3.1. Installation mit Hilfe des Installationsassistenten

Um Kaspersky Anti-Virus auf Ihrem Computer zu installieren, starten Sie die Distributionsdatei von der Installations-CD.

Hinweis.

Die Installation der Anwendung von einer Distribution, die aus dem Internet heruntergeladen wurde, stimmt vollständig mit der Installation der Anwendung von einer Distributions-CD überein.

Das Installationsprogramm funktioniert im Dialogmodus. Jedes Dialogfenster enthält eine Auswahl von Schaltflächen zur Steuerung des Installationsprozesses. Unten finden Sie die Funktionsbeschreibung der wichtigsten Schaltflächen:

- **Weiter >** – Aktion bestätigen und zum folgenden Schritt des Installationsvorgangs weitergehen.
- **Zurück** – zum vorherigen Installationsschritt zurückkehren.
- **Abbrechen** – Installation des Produkts abbrechen.
- **Fertig stellen** – Installationsprozedur des Programms auf dem Computer fertig stellen.

Betrachten wir die einzelnen Schritte des Installationsvorgangs ausführlich:

Schritt 1. Überprüfen des Systems auf die Installations-voraussetzungen für Kaspersky Anti-Virus

Bevor das Programm auf Ihrem Computer installiert wird, werden das installierte Betriebssystem und die vorhandenen Service Packs auf Übereinstimmung mit den Softwarevoraussetzungen für die Installation von Kaspersky Anti-Virus überprüft. Außerdem wird überprüft, ob die erforderlichen Programme auf Ihrem Computer vorhanden sind und ob Sie über die notwendigen Rechte zur Programminstallation verfügen.

Sollte eine bestimmte Voraussetzung nicht erfüllt sein, dann erscheint eine entsprechende Meldung auf dem Bildschirm. Es wird empfohlen, vor der Installation von Kaspersky Anti-Virus die erforderlichen Programme und mit Hilfe des Diensts **Windows Update** die fehlenden Service Packs zu installieren.

Schritt 2. Startfenster des Installationsvorgangs

Wenn Ihr System die Voraussetzungen vollständig erfüllt, erscheint sofort nach dem Start der Distributionsdatei auf dem Bildschirm das Startfenster, das Informationen über den Beginn der Installation von Kaspersky Anti-Virus auf Ihrem Computer enthält.

Klicken Sie auf **Weiter**, um die Installation fortzusetzen, oder klicken Sie auf **Abbrechen**, um die Installation des Produkts zu abbrechen.

Schritt 3. Lesen des Lizenzvertrags

Das folgende Fenster des Installationsprogramms enthält den Lizenzvertrag, der zwischen Ihnen und Kaspersky Lab geschlossen wird. Bitte lesen Sie den Vertrag aufmerksam. Wenn Sie allen Punkten des Vertrags zustimmen, wählen Sie die Variante **Ich akzeptiere die Bedingungen des Lizenzvertrags** und klicken Sie auf die Schaltfläche **Weiter**. Die Installation wird fortgesetzt.

Klicken Sie auf **Abbrechen**, um die Installation abbrechen.

Schritt 4. Auswahl des Installationsordners

Im nächsten Schritt der Installation von Kaspersky Anti-Virus wird festgelegt, in welchem Ordner Ihres Computers das Produkt installiert werden soll. Der standardmäßige Pfad lautet:

- <Laufwerk>\Programme\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers – für 32-Bit-Systeme.
- <Laufwerk>\Programme (x86)\Kaspersky Lab\Kaspersky Anti-Virus 6.0 for Windows Servers – für 64-Bit-Systeme.

Sie können einen anderen Ordner wählen. Klicken Sie dazu auf die Schaltfläche **Durchsuchen** und wählen Sie den Ordner im Standardfenster zur Ordnerauswahl aus oder geben Sie den Pfad des Ordners im entsprechenden Eingabefeld an.

Falls Sie den vollständigen Pfad des Ordners manuell eingeben, beachten Sie, dass er aus maximal 200 Zeichen bestehen und keine Sonderzeichen enthalten darf.

Klicken Sie auf die Schaltfläche **Weiter**, um die Installation fortzusetzen.

Schritt 5. Verwendung von Anwendungsparametern, die von der vorherigen Installation gespeichert wurden

Falls bei der Deinstallation der Vorgängerversion von Kaspersky Anti-Virus 6.0 Schutzparameter und Bedrohungssignaturen gespeichert wurden, können Sie auf dieser Etappe entscheiden, ob diese für die Anwendung verwendet werden sollen.

Die gespeicherten Elemente, die beibehalten werden sollen, werden folgendermaßen ausgewählt.

Wenn auf dem Server bereits eine ältere Version von Kaspersky Anti-Virus installiert war, bei deren Deinstallation die Bedrohungssignaturen gespeichert wurden, können Sie diese Signaturen in der neu installierten Version verwenden. Aktivieren Sie dazu das Kontrollkästchen **Bedrohungssignaturen**. In diesem Fall werden die in der Programmdistribution enthaltenen Signaturen nicht auf den Server kopiert.

Um die Schutzparameter beizubehalten, die in der vorherigen Version benutzt und auf dem Computer gespeichert wurden, aktivieren Sie das Kontrollkästchen **Schutzeinstellungen**.

Schritt 6. Auswahl des Installationstyps

Hier können Sie auswählen, in welchem Umfang das Programm auf Ihrem Computer installiert werden soll. Zwei Installationsvarianten sind vorgesehen:

Vollständig. In diesem Fall werden alle Komponenten von Kaspersky Anti-Virus auf Ihrem Computer installiert. Die weitere Abfolge der Installationsschritte wird in Schritt 8 beschrieben.

Benutzerdefiniert. In diesem Fall wird Ihnen angeboten, die Programmkomponenten auszuwählen, die auf Ihrem Computer installiert werden sollen. Details siehe Schritt 7.

Klicken Sie zur Auswahl eines Installationstyps auf die entsprechende Schaltfläche.

Schritt 7. Auswahl der zu installierenden Programmkomponenten

Dieser Schritt wird nur bei der **benutzerdefinierten** Installation des Programms ausgeführt.

Bei der benutzerdefinierten Installation muss eine Liste der Komponenten von Kaspersky Anti-Virus festgelegt werden, die installiert werden sollen.

Standardmäßig sind zur Installation die Komponente Datei-Anti-Virus, die Komponente zur Virensuche sowie der Konnektor des Administrationsagenten zur entfernten Verwaltung der Anwendung über Kaspersky Administration Kit ausgewählt.

Um eine Komponente zur anschließenden Installation auszuwählen, wird durch Linksklick auf das Symbol neben dem Komponentennamen das Menü geöffnet und der Punkt **Die Komponente wird auf der lokalen Festplatte installiert** gewählt. Eine Beschreibung des Schutzes, den die betreffende Komponente gewährleistet und Informationen über den für ihre Installation auf der Festplatte erforderlichen Platz befinden sich im unteren Bereich dieses Fensters der Programminstallation.

Um die Installation einer Komponente abzulehnen, wählen Sie im Kontextmenü die Variante **Die Komponente wird nicht verfügbar sein**.

Klicken Sie auf die Schaltfläche **Weiter**, nachdem Sie die zu installierenden Komponenten gewählt haben. Um zur Liste der standardmäßig zu installierenden Komponenten zurückzukehren, klicken Sie auf die Schaltfläche **Zurücksetzen**.

Schritt 8. Suche anderer Antiviren-Anwendungen

Auf dieser Etappe erfolgt die Suche nach anderen Antiviren-Produkten (einschließlich Kaspersky-Lab-Produkte), die auf Ihrem Computer installiert sind und deren gemeinsame Verwendung mit Kaspersky Anti-Virus zu Konflikten führen kann.

Wenn auf Ihrem Computer solche Programme gefunden werden, werden Sie auf dem Bildschirm aufgelistet. Sie werden aufgefordert, diese Programme zu löschen, bevor die Installation fortgesetzt wird.

Unter der Liste der gefundenen Antiviren-Anwendungen können Sie wählen, ob diese automatisch oder manuell entfernt werden sollen (nur Kaspersky-Lab-Produkte werden automatisch entfernt).

Klicken Sie auf die Schaltfläche **Weiter**, um die Installation fortzusetzen.

Schritt 9. Abschlussvorbereitungen für die Programminstallation

Nun wird Ihnen angeboten, die Programminstallation auf Ihrem Computer abschließend vorzubereiten.

Bei der Erstinstallation von Kaspersky Anti-Virus 6.0 ist es nicht ratsam, das Kontrollkästchen **Schutz für Module vor der Installation aktivieren** zu entfernen. Der aktivierte Modulschutz erlaubt, falls während der Anwendungsinstallation Fehler auftreten, die Installation auf korrekte Weise rückgängig zu machen. Bei einem wiederholten Versuch zur Installation der Anwendung wird empfohlen, dieses Kontrollkästchen zu entfernen.

Wird die Anwendung im entfernten Modus über **Windows Remote Desktop** auf einem Computer installiert, dann wird empfohlen, das Kontrollkästchen **Schutz für Module vor der Installation aktivieren** zu deaktivieren. Andernfalls besteht die Möglichkeit, dass der Installationsvorgang nicht oder fehlerhaft durchgeführt wird.

Wenn Sie möchten, dass die von der Firma Microsoft für Server empfohlenen Ausnahmen automatisch zur Liste der Ausnahmen hinzugefügt werden, dann aktivieren Sie das Kontrollkästchen der Option **Microsoft-Ausnahmen hinzufügen**.

Wenn Sie möchten, dass der Pfad für avp.com nach der Installation zur Umgebungsvariablen %Path% hinzugefügt wird, aktivieren Sie das Kontrollkästchen der Option **Umgebungsvariable hinzufügen**.

Klicken Sie auf die Schaltfläche **Weiter**, um die Installation fortzusetzen.

Achtung!

Während der Installation von Komponenten für Kaspersky Anti-Virus, die der Überwachung des Netzwerkverkehrs dienen, werden bestehende Netzwerkverbindungen getrennt. Die Mehrzahl der getrennten Verbindungen wird nach einem bestimmten Zeitraum wiederhergestellt.

Schritt 10. Abschluss des Installationsvorgangs

Das Fenster **Installation wird abgeschlossen** enthält Informationen über den Abschluss des Installationsvorgangs von Kaspersky Anti-Virus auf Ihrem Computer.

Um den Konfigurationsassistenten der Anwendung zu starten, klicken Sie auf die Schaltfläche **Weiter** (s. Pkt. 3.2 auf S. 26).

Wenn der Neustart des Computers erforderlich ist, um die Installation korrekt abzuschließen, erscheint eine entsprechende Meldung auf dem Bildschirm.

3.2. Konfigurationsassistent

Der Konfigurationsassistent für Kaspersky Anti-Virus 6.0 wird beim Abschluss der Programminstallation gestartet. Seine Aufgabe ist es, Sie bei der ersten Konfiguration der Programmeinstellungen zu unterstützen und dabei die Besonderheiten der Aufgaben Ihres Computers zu berücksichtigen.

Der Konfigurationsassistent besitzt das Aussehen eines Microsoft Windows-Programmassistenten (Windows Wizard) und besteht aus einer Folge von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die

Schaltflächen **Weiter** und **Zurück**, zum Abschluss des Assistenten klicken Sie auf die Schaltfläche **Fertig stellen**. Die Arbeit des Assistenten kann auf einer beliebigen Etappe durch Klick auf die Schaltfläche **Abbrechen** beendet werden.

Sollten Sie den Vorgang zur erstmaligen Konfiguration abbrechen, in dem Sie das Fenster des Assistenten schließen, dann wird die Anwendung nicht arbeiten. Bei jedem Start der Anwendung wird der Konfigurationsassistent erneut gestartet, bis der Vorgang zur erstmaligen Konfiguration erfolgreich abgeschlossen wurde.

3.2.1. Verwendung von Objekten, die in Version 5.0 gespeichert wurden

Dieses Fenster des Assistenten erscheint, wenn die Anwendung über Kaspersky Anti-Virus Version 5.0 installiert wird. Ihnen wird angeboten, die Daten, die von Version 5.0 verwendet wurden und auf Version 6.0 übertragen werden sollen, auszuwählen. Dazu gehören Quarantäne- und Backup-Objekte sowie Schutzeinstellungen.

Aktivieren Sie die entsprechenden Kontrollkästchen, um diese Daten in Version 6.0 zu verwenden.

3.2.2. Aktivierung des Programms

Vergewissern Sie sich, dass das Systemdatum des Computers korrekt eingestellt ist, bevor Sie das Programm aktivieren.

Der Aktivierungsvorgang des Programms besteht in der Installation eines Schlüssels, auf dessen Grundlage Kaspersky Anti-Virus ermittelt, ob Rechte für die Programmnutzung bestehen und welche Nutzungsdauer vorliegt.

Der Schlüssel enthält Dienstinformationen, die für die volle Funktionsfähigkeit des Programms erforderlich sind, sowie zusätzliche Angaben:

- Informationen über den Support (von wem und wo man technische Unterstützung erhalten kann).
- Bezeichnung, Nummer und Gültigkeitsende des Schlüssels.

3.2.2.1. Auswahl der Methode zur Aktivierung der Anwendung

Abhängig davon, ob Sie über einen Lizenzschlüssel für Kaspersky Anti-Virus verfügen oder ihn von einem Kaspersky-Lab-Server herunterladen müssen, bestehen mehrere Möglichkeiten zur Aktivierung des Programms:

- **Mit Aktivierungscode aktivieren.** Wählen Sie diese Aktivierungsmethode, wenn Sie eine kommerzielle Programmversion erworben haben und Sie einen Aktivierungscode besitzen. Auf Basis dieses Codes bekommen Sie einen Lizenzschlüssel, der Ihnen während der gesamten Gültigkeitsdauer der Lizenz den Zugriff auf die volle Funktionsfähigkeit des Programms bietet.
- **Testversion aktivieren.** Wählen Sie diese Aktivierungsvariante, wenn Sie eine Testversion des Programms installieren möchten, bevor Sie über den Kauf einer kommerziellen Version entscheiden. Sie erhalten einen kostenlosen Lizenzschlüssel, dessen Gültigkeitsdauer durch die Lizenz der Testversion dieser Anwendung beschränkt ist.
- **Vorherigen Lizenzschlüssel verwenden.** Aktivieren Sie die Anwendung mit Hilfe einer bereits vorhandenen Lizenzschlüsseldatei für Kaspersky Anti-Virus 6.0.
- **Das Programm später aktivieren.** Bei der Auswahl dieser Variante wird die Aktivierung des Programms übersprungen. Kaspersky Anti-Virus 6.0 wird auf Ihrem Computer installiert und Sie können alle Programmfunktionen außer dem Update nutzen (Die Bedrohungssignaturen können nach der Programminstallation nur einmal aktualisiert werden).

Bei der Auswahl der ersten beiden Varianten erfolgt die Programmaktivierung über den Kaspersky-Lab-Webserver. Für die Verbindung mit dem Server ist eine Internetverbindung erforderlich. Prüfen Sie vor dem Beginn der Aktivierung im Fenster, das mit der Schaltfläche **LAN-Einstellungen** geöffnet wird, die Einstellungen der Internetverbindung und korrigieren Sie diese bei Bedarf (s. Pkt. 10.4.3 auf S. 116). Wenden Sie sich an Ihren Systemadministrator oder Internetprovider, um weitere Informationen zu den Einstellungen der Netzwerkverbindung zu erhalten.

Ist im Augenblick der Installation keine Internetverbindung vorhanden, dann kann die Aktivierung später über die Programmoberfläche erfolgen (s. Pkt. 11.5 auf S. 138). Außerdem besteht die Möglichkeit, von einem anderen Computer aus ins Internet zu gehen, sich auf der Webseite des Technischen Support-Services von Kaspersky Lab anzumelden und mit Hilfe des Aktivierungscode einen Lizenzschlüssel herunterzuladen.

3.2.2.2. Eingabe des Aktivierungscode

Zur Aktivierung des Programms ist die Eingabe des Aktivierungscode erforderlich. Wenn die Anwendung über das Internet gekauft wurde, erhalten Sie den Aktivierungscode per E-Mail. Wurde die Anwendung als verpackte Variante gekauft, dann ist der Aktivierungscode auf dem Umschlag mit der Installations-CD angegeben.

Der Aktivierungscode besteht aus einer durch Bindestriche getrennten Ziffernfolge (vier Blöcke zu je fünf Ziffern und Buchstaben ohne Leerzeichen, z.B. 11AA1-11AAA-1AA11-1A111). Bitte beachten Sie, dass der Code mit lateinischen Zeichen eingegeben werden muss.

Geben Sie im unteren Teil des Fensters Ihre Kontaktinformationen an: Familienname, Name, E-Mail-Adresse, Land und Wohnort. Diese Informationen können zur Identifikation eines registrierten Benutzers erforderlich sein, wenn beispielsweise ein Schlüssel verloren geht oder gestohlen wird. In diesem Fall können Sie auf Basis der Kontaktinformationen einen anderen Lizenzschlüssel erhalten.

3.2.2.3. Download des Lizenzschlüssels

Der Konfigurationsassistent baut eine Verbindung mit den Kaspersky-Lab-Servern im Internet auf und sendet Ihre Anmeldungsdaten (Aktivierungscode, Kontaktinformationen) zur Überprüfung an den Server.

Bei erfolgreicher Überprüfung des Aktivierungscode erhält der Assistent eine Lizenzschlüsseldatei. Wenn Sie eine Testversion des Programms installieren, erhält der Konfigurationsassistent ohne Aktivierungscode einen Testschlüssel.

Die empfangene Datei wird automatisch für die Arbeit mit der Anwendung installiert und das letzte Fenster des Assistenten, das Angaben über die Lizenz enthält, informiert Sie über den Abschluss der Aktivierung.

Wenn der Aktivierungscode die Überprüfung nicht besteht, erscheint ein entsprechender Hinweis auf dem Bildschirm. Wenden Sie sich in diesem Fall an die Firma, bei der Sie das Programm erworben haben.

3.2.2.4. Auswahl einer Lizenzschlüsseldatei

Wenn Sie bereits eine Lizenzschlüsseldatei für das Programm Kaspersky Anti-Virus 6.0 besitzen, bietet Ihnen der Assistent in diesem Fenster an, den Schlüssel zu installieren. Verwenden Sie dazu die Schaltfläche **Durchsuchen** und wählen Sie im Standardfenster zur Dateiauswahl eine Datei mit der Endung `.key` aus.

Nach der erfolgreichen Installation des Schlüssels erscheinen im unteren Bereich des Fensters Informationen über die Lizenz: Name des Besitzers, Nummer, Typ (kommerziell, für Beta-Test, Test usw.) und Gültigkeitsende des Schlüssels.

3.2.2.5. Abschluss der Programmaktivierung

Der Konfigurationsassistent informiert Sie über den erfolgreichen Abschluss der Programmaktivierung. Außerdem werden Informationen über den installierten Lizenzschlüssel angezeigt: Name des Besitzers, Nummer und Typ (kommerzielle, für Beta-Test, Test usw.) der Lizenz, Gültigkeitsende des Schlüssels.

3.2.3. Konfiguration der Update-Einstellungen

Die Qualität des Schutzes Ihres Computers ist direkt vom rechtzeitigen Download der Updates für die Bedrohungssignaturen und Programm-Module abhängig. In diesem Fenster des Assistenten wird Ihnen angeboten, den Modus für das Programm-Update zu wählen und Einstellungen für den Zeitplan vorzunehmen:

- Automatisch.** Kaspersky Anti-Virus prüft in festgelegten Zeitabständen, ob an der Updatequelle ein neues Updatepaket vorhanden ist. Die Häufigkeit der Überprüfung kann während Virusepidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates vorhanden sind, lädt die Anwendung sie herunter und installiert sie auf dem Computer. Dieser Modus gilt als Standard.
- Alle 2 Stunden** (Das Intervall kann in Abhängigkeit von den Zeitplaneinstellungen variieren). Das Update wird automatisch nach dem festgelegten Zeitplan gestartet. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.
- Manuell.** In diesem Fall starten Sie das Programm-Update selbständig.

Beachten Sie, dass die Datenbanken mit den Bedrohungssignaturen und die Programm-Module, die in der Distribution enthalten sind, zum Zeitpunkt der Programminstallation bereits veraltet sein können. Wir empfehlen deshalb, die aktuellen Programm-Updates herunterzuladen. Klicken Sie dazu auf die Schaltfläche **Jetzt aktualisieren**. In diesem Fall empfängt Kaspersky Anti-Virus die erforderlichen Updates von den Updateseiten im Internet und installiert sie auf Ihrem Computer.

Wenn Sie die Updateparameter anpassen möchten (Netzwerkparameter festlegen, die Ressource wählen, von der das Update erfolgt, den Start der

Aktualisierung unter einem bestimmten Benutzerkonto konfigurieren, den Dienst zur Update-Verteilung in eine lokale Quelle aktivieren), klicken Sie auf die Schaltfläche **Einstellungen**.

3.2.4. Konfiguration des Zeitplans für die Virenuntersuchung

Die Suche von schädlichen Objekten in vorgegebenen Untersuchungsbereichen ist eine der wichtigsten Aufgaben, die den Schutz Ihres Computers gewährleistet.

Bei der Installation von Kaspersky Anti-Virus werden standardmäßig drei Untersuchungsaufgaben erstellt. In diesem Fenster bietet Ihnen der Assistent an, den Startmodus für die Untersuchungsaufgaben festzulegen:

Autostart-Objekte untersuchen

Standardmäßig findet die Untersuchung der Autostart-Objekte automatisch bei jedem Start von Kaspersky Anti-Virus statt. Die Zeiteinstellungen können im Fenster angepasst werden, das mit der Schaltfläche **Ändern** geöffnet wird.

Kritische Bereiche untersuchen

Aktivieren Sie das Kontrollkästchen im entsprechenden Block, damit die Virenuntersuchung der kritischen Computerbereiche (Systemspeicher, Autostart-Objekte, Bootsektoren, Microsoft Windows Server-Systemverzeichnisse) automatisch gestartet wird. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.

Der automatische Start dieser Aufgabe ist standardmäßig deaktiviert.

Vollständig Untersuchung des Computers

Aktivieren Sie das Kontrollkästchen im entsprechenden Block, damit die vollständige Untersuchung Ihres Computers auf Viren automatisch gestartet wird. Der Zeitplan wird in dem Fenster angepasst, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.

Der automatische Start dieser Aufgabe nach Zeitplan ist standardmäßig deaktiviert. Wir empfehlen aber, sofort nach der Programminstallation die vollständige Virenuntersuchung des Servers zu starten.

3.2.5. Zugriffsbegrenzung auf das Programm

Da der PC von verschiedenen Personen benutzt werden kann und weil außerdem die Gefahr besteht, dass Schadprogramme versuchen, den Schutz Ihres Computers auszuschalten, wird Ihnen angeboten, den Zugriff auf das Programm Kaspersky Anti-Virus mit Hilfe eines Kennworts zu beschränken. Das Kennwort erlaubt es, das Programm vor Versuchen zum unerlaubten Abschalten des Schutzes und zum Ändern der Einstellungen zu schützen.

Um den Kennwortschutz zu verwenden, aktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren** und füllen Sie die Felder **Kennwort** und **Kennwort bestätigen** aus.

Geben Sie darunter den Bereich an, auf den sich die Zugriffsbegrenzung beziehen soll:

- Alle Operationen (außer Gefahrenmeldungen).** Bei einer beliebigen Aktion des Benutzers mit dem Programm wird das Kennwort abgefragt. Eine Ausnahme bildet die Arbeit mit Hinweisen über den Fund gefährlicher Objekte.
- Nur für ausgewählte Operationen:**
 - Veränderungen von Programmeinstellungen** – Wenn der Benutzer versucht, geänderte Anwendungseinstellungen zu speichern, wird das Kennwort abgefragt.
 - Programm beenden** – Wenn der Benutzer versucht, die Anwendung zu beenden, wird das Kennwort abgefragt.
 - Schutzkomponenten und Untersuchungsaufgaben anhalten/beenden** – Das Kennwort wird abgefragt, wenn der Benutzer versucht, die Arbeit einer beliebigen Schutzkomponente oder einer Untersuchungsaufgabe anzuhalten oder zu beenden.

3.2.6. Abschluss des Konfigurationsassistenten

Im letzten Fenster des Assistenten werden Sie darüber informiert, dass die Installation und Konfiguration der Anwendung erfolgreich verlaufen sind. Sie können die Anwendung sofort zur Anwendung starten. Aktivieren Sie dazu das Kontrollkästchen **Produkt starten**.

Wenn die Installation fehlerhaft verlaufen ist (beispielsweise beim Fund von inkompatiblen Versionen anderer Antiviren-Anwendungen), wird Ihnen angeboten, den Computer neu zu starten.

3.3. Installation der Anwendung aus der Befehlszeile

Geben Sie zur Installation von Kaspersky Anti-Virus 6.0 for Windows Servers in der Befehlszeile ein:

```
msiexec /i <Paketname>
```

Der Installationsassistent (s. Pkt. 3.1 auf S. 22) wird gestartet. Zum Abschluss der Anwendungsinstallation ist der Neustart des Computers erforderlich.

Um die Anwendung im Silent-Modus (ohne Installationsassistent) zu installieren, geben Sie folgende Befehlszeile ein:

```
msiexec /i <Paketname> /qn
```

In diesem Fall muss der Computer nach Abschluss der Installation manuell neu gestartet werden. Damit der Neustart automatisch ausgeführt wird, geben Sie folgende Parameter ein:

```
msiexec /i <Paketname> ALLOWREBOOT=1 /qn
```

Beachten Sie, dass der automatische Neustart des Computers nur im Silent-Installationsmodus ausgeführt werden kann (mit dem Schlüssel /qn).

Um die Anwendung mit Kennwortangabe für die Deinstallation der Anwendung zu installieren, geben Sie ein:

```
msiexec /i <Paketname> KLUNINSTPASSWD=***** – zur  
Installation im interaktiven Modus.
```

```
msiexec /i <Paketname> KLUNINSTPASSWD=***** /qn – zur  
Installation im Silent-Modus ohne Neustart des Computers.
```

```
msiexec /i <Paketname> KLUNINSTPASSWD=*****  
ALLOWREBOOT=1 /qn – zur Installation im Silent-Modus mit  
anschließendem Neustart des Computers.
```

Bei der Installation von Kaspersky Anti-Virus im Silent-Modus wird das Lesen der Datei *setup.ini*, die generelle Parameter für die Installation der Anwendung enthält (s. Pkt. A.4 auf S. 199), der Konfigurationsdatei *install.cfg* (s. Pkt. 13.7 auf S. 186) sowie der Lizenzschlüsseldatei unterstützt. Beachten Sie, dass sich diese Dateien im Distributionsordner von Kaspersky Anti-Virus befinden müssen.

3.4. Installation über den Gruppenrichtlinienobjekt-Editor (Group Policy Object)

Diese Option wird auf Computern mit dem Betriebssystem Microsoft Windows 2000 und höher unterstützt.

Mit Hilfe des **Gruppenrichtlinienobjekt-Editors** können Sie Kaspersky Anti-Virus auf den Workstations Ihres Unternehmens, die zu der Domäne gehören, installieren, aktualisieren und löschen, ohne Kaspersky Administration Kit zu verwenden.

3.4.1. Installation der Anwendung

Um Kaspersky Anti-Virus zu installieren:

1. Erstellen Sie auf dem Computer, der als Domain Controller funktioniert, einen gemeinsamen Netzwerkordner und speichern Sie darin die Distribution von Kaspersky Anti-Virus im Format *.msi*.

Zusätzlich können in diesem Ordner die Datei *setup.ini*, die eine Liste von Parametern für die Installation von Kaspersky Anti-Virus enthält (ausführliche Beschreibung der Parameter dieser Datei siehe Pkt. A.4 auf S. 199), die Konfigurationsdatei *install.cfg* (s. Pkt. 13.7 auf S. 186) sowie die Schlüsseldatei gespeichert werden.

2. Öffnen Sie den **Gruppenrichtlinienobjekt-Editor** über die MMC-Standardkonsole (zu Details über die Arbeit mit dem Editor siehe Hilfesystem von Microsoft Windows Server).
3. Erstellen Sie ein neues Paket. Wählen Sie dazu in der Konsolenstruktur **Gruppenrichtlinienobjekt/ Computerkonfiguration** (Computer Configuration)/ **Software-Einstellungen** (Software Settings)/ **Software-Installation** (Software installation) und verwenden Sie den Befehl **Neu/ Paket** (New/Package) des Kontextmenüs.

Geben Sie im folgenden Fenster den Pfad des gemeinsamen Netzwerkordners an, der die Distribution von Anti-Virus enthält (s. Pkt. 1). Wählen Sie im Dialogfenster **Einführung des Programms** (Select Deployment Method) den Parameter **Zuweisen** (Assign) und klicken Sie auf die Schaltfläche **OK**.

Die Gruppenrichtlinie wird auf den einzelnen Workstations übernommen, wenn sich die Computer zum nächsten Mal bei der Domäne anmelden. Dadurch wird Kaspersky Anti-Virus auf allen Computern installiert.

3.4.2. Upgrade der Anwendung

Um die Version von Kaspersky Anti-Virus zu aktualisieren:

1. Speichern Sie die Distribution, die das Update von Kaspersky Anti-Virus enthält, im Format *.msi* im gemeinsamen Netzwerkordner.
2. Öffnen Sie den **Gruppenrichtlinienobjekt-Editor** und erstellen wie oben beschrieben ein neues Paket.
3. Markieren Sie das neue Paket in der Liste und verwenden Sie den Befehl **Eigenschaften** (Properties) des Kontextmenüs. Gehen Sie im Eigenschaften-Fenster des Pakets auf die Registerkarte **Upgrades** (Upgrades) und geben Sie das Paket an, das die Distribution der vorhergehenden Version von Kaspersky Anti-Virus enthält. Damit die aktuelle Version von Kaspersky Anti-Virus mit den gespeicherten Schutzparametern installiert wird, wählen Sie die Variante zur Installation über das vorhandene Paket.

Die Gruppenrichtlinie wird auf den einzelnen Workstations übernommen, wenn sich die Computer zum nächsten Mal bei der Domäne anmelden.

Beachten Sie, dass auf Computern mit dem Betriebssystem Microsoft Windows 2000 Server das Upgrade von Kaspersky Anti-Virus über den Gruppenrichtlinienobjekt-Editor nicht unterstützt wird.

3.4.3. Löschen der Anwendung

Um Kaspersky Anti-Virus zu löschen:

1. Öffnen Sie den **Gruppenrichtlinienobjekt-Editor**.
2. Wählen Sie in der Konsolenstruktur **Gruppenrichtlinienobjekt/Computerkonfiguration** (Computer Configuration)/ **Software-Einstellungen** (Software Settings)/ **Software-Installation** (Software installation).

Markieren Sie in der Paketliste das Paket Kaspersky Anti-Virus, öffnen Sie das Kontextmenü und führen Sie den Befehl **Alle Aufgaben** (All Tasks)/ **Löschen** (Remove) aus.

Wählen Sie im Dialogfenster **Anwendungen löschen** (Remove Software) **Sofortige Deinstallation dieser Anwendung von den Computern aller Benutzer** (Immediately uninstall the software from users and computers), damit Kaspersky Anti-Virus beim nächsten Neustart des Computers gelöscht wird.

3.5. Aktualisierung der Anwendung von Version 5.0 auf Version 6.0

Wenn auf Ihrem Computer die Anwendung Kaspersky Anti-Virus for 5.0 Windows File Servers installiert ist, können Sie diese auf Kaspersky Anti-Virus 6.0 aktualisieren.

Nach dem Start des Installationsprogramms für Kaspersky Anti-Virus 6.0 wird Ihnen angeboten, zuerst die Version 5.0 des Produkts zu entfernen. Nach Abschluss der Deinstallation ist der Neustart des Computers notwendig. Danach beginnt die Installation der Anwendung der Version 6.0.

Vorsicht!

Bei der Installation von Kaspersky Anti-Virus 6.0 for Windows Servers ist folgendes zu beachten. Wenn die Installation von Version 6.0 aus einem Netzwerkordner erfolgt, auf den der Zugriff mit Hilfe eines Kennworts eingeschränkt ist, wird zwar Version 5.0 deinstalliert und der Computer wird neu gestartet, die Anwendung der Version 6.0 wird aber nicht installiert. Der Grund dafür liegt in fehlenden Zugriffsrechten des Installationsprogramms für den Netzwerkordner. Um das Problem zu lösen, starten Sie die Anwendungsinstallation nur aus einer lokalen Ressource.

KAPITEL 4. PROGRAMM-OBERFLÄCHE


Kaspersky Anti-Virus verfügt über eine einfache und komfortable Oberfläche. In diesem Kapitel werden die wichtigsten Elemente der Oberfläche ausführlich beschrieben:

- Symbol im Infobereich der Taskleiste (s. Pkt. 4.1 auf S. 37)
- Kontextmenü (s. Pkt. 4.2 auf S. 38)
- Hauptfenster (s. Pkt. 4.3 auf S. 39)
- Konfigurationsfenster der Anwendung (s. Pkt. 4.4 auf S. 41)




4.1. Symbol im Infobereich

Sofort nach der Installation von Kaspersky Anti-Virus erscheint sein Symbol im Infobereich der Taskleiste.

Das Symbol ist ein spezieller Indikator für die Arbeit von Kaspersky Anti-Virus. Er informiert über den Schutzstatus und eine Reihe wichtiger Aufgaben, die vom Programm ausgeführt werden.

Wenn das Symbol aktiv  (farbig) ist, ist der Schutz Ihres Computers aktiviert. Ist das Symbol inaktiv  (schwarz-weiß), dann ist der Echtzeitschutz deaktiviert.

Abhängig von der momentan ausgeführten Operation verändert sich das Symbol von Kaspersky Anti-Virus:

	Die Untersuchung einer Datei, die von Ihnen oder einem Programm geöffnet, gespeichert oder gestartet wird, wird ausgeführt.
	Das Update der Bedrohungssignaturen und Programm-Module von Kaspersky Anti-Virus wird ausgeführt.
	Bei der Arbeit einer Komponente von Kaspersky Anti-Virus ist eine Störung aufgetreten.

Das Symbol bietet außerdem Zugriff auf die grundlegenden Elemente der Programmoberfläche: Kontextmenü (s. Pkt. 4.2 auf S. 38) und Hauptfenster (s. Pkt. 4.3 auf S. 39).

Um das Kontextmenü zu öffnen, klicken Sie mit der rechten Maustaste auf das Programmsymbol.

Um das Hauptfenster von Kaspersky Anti-Virus im Abschnitt **Schutz** zu öffnen (mit diesem Abschnitt startet das Programm standardmäßig), doppelklicken Sie mit der linken Maustaste auf das Programmsymbol. Durch einfaches Klicken wird das Hauptfenster in dem Abschnitt geöffnet, der aktiv war, bevor es geschlossen wurde.

4.2. Kontextmenü

Das Kontextmenü (s. Abb. 1) bietet Zugriff auf die wichtigsten Schutzaufgaben.



Abbildung 1. Kontextmenü

Das Menü von Kaspersky Anti-Virus enthält folgende Punkte:

- Arbeitsplatz** – Starten der vollständigen Untersuchung Ihres Computers auf das Vorhandensein von Viren. Dadurch werden die Objekte auf allen Laufwerken einschließlich der Wechseldatenträger untersucht.
- Virensuche** – In das Fenster zur Auswahl der Untersuchungsobjekte und zum Start der Virensuche wechseln. Standardmäßig enthält die Liste bestimmte Objekte wie beispielsweise Systemspeicher, Autostart-Objekte, Mail-Datenbanken, alle Laufwerke des Servers usw. Sie können die Liste ergänzen, Objekte zur Untersuchung auswählen und die Virensuche starten.
- Update** – Starten der Aktualisierung der Programm-Module und Bedrohungssignaturen für Kaspersky Anti-Virus und der Installation der Updates auf dem Server.
- Aktivierung** – Zum Aktivieren des Programms wechseln. Um den Status eines registrierten Benutzers zu erhalten, auf dessen Basis Ihnen die volle Funktionsfähigkeit der Anwendung und die Leistungen des Technischen Support-Services zur Verfügung gestellt werden, ist es erforderlich, Kaspersky Anti-Virus zu aktivieren. Dieser Menüpunkt ist nur vorhanden, wenn das Programm noch nicht aktiviert wurde.

Einstellungen – Zur Ansicht und Konfiguration der Funktionsparameter von Kaspersky Anti-Virus wechseln.

Kaspersky Anti-Virus – Das Programmhauptfenster öffnen (s. Pkt. 4.3 auf S. 39).

Schutz anhalten / Schutz aktivieren – Die Arbeit von Datei-Anti-Virus (s. Pkt. 2.2.1 auf S. 15) vorübergehend deaktivieren/aktivieren. Dieser Menüpunkt hat keinen Einfluss auf das Programm-Update und die Ausführung der Aufgaben zur Virensuche.

Beenden – Die Arbeit von Kaspersky Anti-Virus beenden (Bei Auswahl dieses Menüpunkts wird die Anwendung aus dem Arbeitsspeicher des Computers entfernt).

Wenn im Moment eine Aufgabe zur Virensuche läuft, wird ihr Name im Kontextmenü mit Prozentangabe des Ausführungsergebnisses angezeigt. Durch die Auswahl der Aufgabe gelangen Sie in das Berichtsfenster mit den aktuellen Ausführungsergebnissen.

4.3. Programmhauptfenster

Das Hauptfenster von Kaspersky Anti-Virus (s. Abb. 2) lässt sich bedingt in zwei Bereiche aufteilen:

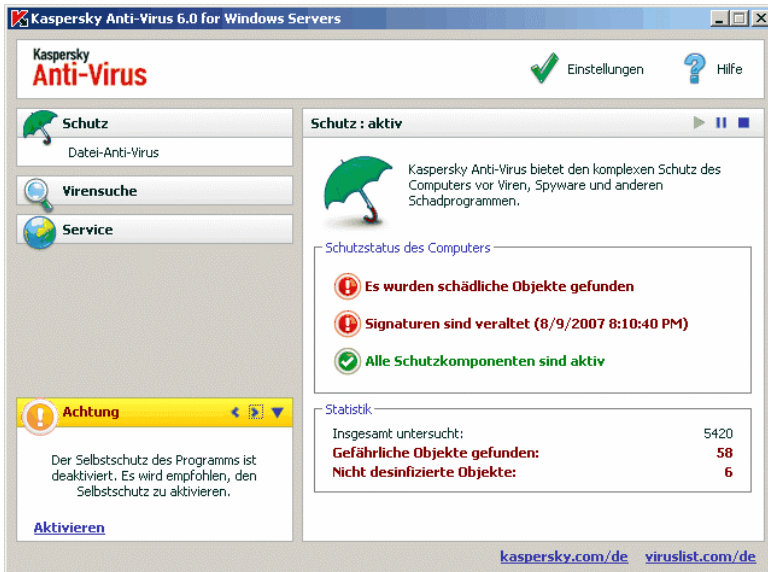

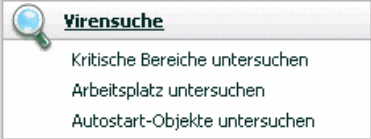



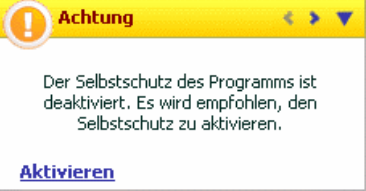
Abbildung 2. Hauptfenster von Kaspersky Anti-Virus

- Die linke Seite des Fensters, der *Navigationsbereich*, erlaubt es, schnell und einfach zu einer beliebigen Komponente, zur Ausführung von Untersuchungs- und Update-Aufgaben oder zu den Servicefunktionen des Programms zu wechseln.
- Die rechte Seite des Fensters, der *Informationsbereich*, enthält Informationen über die auf der linken Seite ausgewählte Schutzkomponente, erlaubt den Wechsel zu den Einstellungen der einzelnen Komponenten, bietet Werkzeuge zur Ausführung der Aufgaben zur Virensuche, zur Arbeit mit Dateien in der Quarantäne und im Backup, zur Verwaltung der Lizenzschlüssel usw.

Wird auf der linken Seite des Fensters ein Abschnitt ausgewählt, dann erhalten Sie auf der rechten Seite vollständige Informationen darüber.

Hier werden die Elemente der Navigationsleiste des Hauptfensters genauer beschrieben.

Abschnitt des Navigationsteils im Hauptfenster	Funktion
<p>Die Hauptaufgabe des Fensters ist es, Sie über den Schutzstatus Ihres Computers zu informieren. Dazu dient der Abschnitt Schutz.</p> 	<p>Wählen Sie im Navigationsteil den Abschnitt Schutz, um allgemeine Informationen über die Arbeit von Kaspersky Anti-Virus zu erhalten, eine zusammenfassende Statistik über die Arbeit des Programms zu lesen oder sich zu vergewissern, ob alles korrekt funktionieren.</p>
<p>Für die Untersuchung des Computers auf die Existenz schädlicher Objekte ist der spezielle Abschnitt Virensuche vorgesehen.</p> 	<p>Dieser Abschnitt enthält eine Liste von Objekten, die Sie auf Viren untersuchen können.</p> <p>Die Aufgaben, die nach Meinung der Kaspersky-Lab-Experten in erster Linie ausgeführt werden sollten, sind in diesem Abschnitt enthalten. Das sind die Aufgaben zur Virensuche in kritischen Bereichen, unter den Autostart-Objekten und die vollständige Untersuchung des Computers.</p>
<p>Der Abschnitt Service enthält zusätzliche Funktionen von Kaspersky Anti-Virus.</p>	<p>Hier können Sie zum Update der Anwendung wechseln, die Berichte über die Arbeit von laufenden und abgeschlossenen Aufgaben und</p>

Abschnitt des Navigationsteils im Hauptfenster	Funktion
	Komponenten ansehen, zur Arbeit mit den Objekten in der Quarantäne und mit den Sicherungskopien, zu Informationen über den technischen Kundendienst oder in das Fenster zur Lizenzschlüsselverwaltung wechseln.
<p>Dieser Bereich begleitet Ihre Arbeit mit dem Programm durch Kommentare und Ratschläge.</p> 	In diesem Abschnitt können Sie jederzeit Ratschläge darüber erhalten, wie die Schutzstufe des Computers erhöht werden kann. Hier befinden sich Kommentare über die laufende Arbeit der Anwendung und ihre Einstellungen. Mit Hilfe der Hyperlinks dieses Abschnitts können Sie direkt zu der Ausführung der im konkreten Fall empfohlenen Aktionen übergehen oder ausführliche Informationen darüber erhalten.

Jedes Element des Navigationsbereichs verfügt über ein spezielles Kontextmenü. Für Datei-Anti-Virus und die Servicefunktionen enthält das Menü beispielsweise Punkte, die es erlauben, schnell zu deren Einstellungen, zur Steuerung oder zur Berichtsansicht zu gelangen. Für die Aufgaben zur Virensuche und die Update-Aufgabe ist ein zusätzlicher Menüpunkt vorgesehen, der es erlaubt, auf Basis der ausgewählten Aufgabe eine neue Aufgabe zu erstellen.

Sie können das Aussehen des Programms anpassen, indem Sie grafische Elemente und Farbschemen erstellen und verwenden.

4.4. Konfigurationsfenster der Anwendung

Das Konfigurationsfenster von Kaspersky Anti-Virus kann vom Hauptfenster aus aufgerufen werden (s. Pkt. 4.3 auf S. 39). Klicken Sie dazu auf den Link Einstellungen im oberen Bereich des Hauptfensters.

Die Struktur des Konfigurationsfensters (s. Abb. 3) entspricht jener des Hauptfensters:

- Die linke Seite des Fensters bietet schnellen und bequemen Zugriff auf die Einstellungen von Datei-Anti-Virus, auf die Untersuchungs- und

Update-Aufgaben sowie auf die Einstellungen für die Servicefunktionen der Anwendung.

- Die rechte Seite des Fensters enthält eine Liste der Parameter für die auf der linken Seite ausgewählte Komponente, Aufgabe usw.

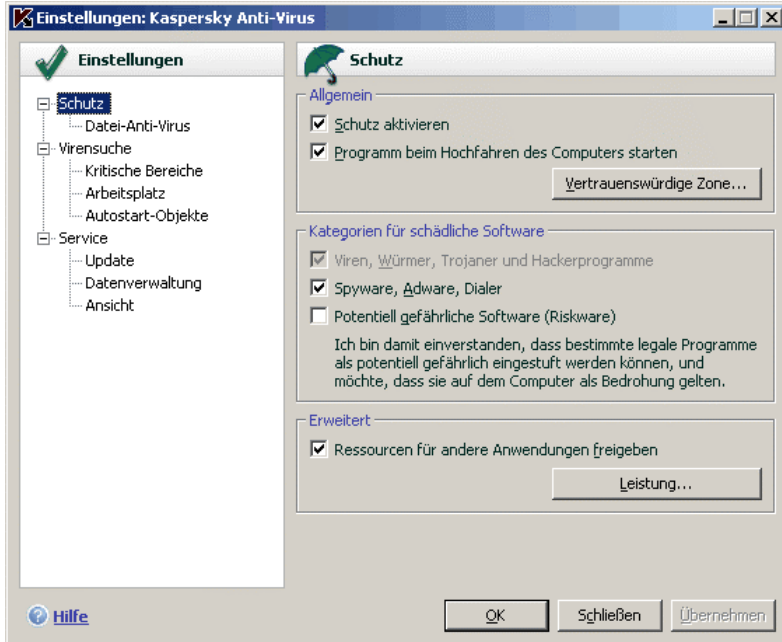


Abbildung 3. Konfigurationsfenster von Kaspersky Anti-Virus

Wird auf der linken Seite des Konfigurationsfensters ein bestimmter Abschnitt, eine Komponente oder eine Aufgabe ausgewählt, dann werden auf der rechten Fensterseite die entsprechenden Parameter angezeigt. Zur Detaileinstellung bestimmter Parameter können Sie die Konfigurationsfenster der zweiten oder dritten Ebene öffnen. Eine ausführliche Beschreibung der Anwendungsparameter finden Sie in den entsprechenden Abschnitten des vorliegenden Benutzerhandbuchs.

KAPITEL 5. ERSTE SCHRITTE

Bei der Entwicklung von Kaspersky Anti-Virus bestand eine der Hauptaufgaben der Spezialisten von Kaspersky Lab in der optimalen Konfiguration aller Programmeinstellungen.

Um die Benutzerfreundlichkeit zu erhöhen, haben wir uns bemüht, die Etappen der vorbereitenden Einstellungen in dem Konfigurationsassistenten (s. Pkt. 3.2 auf S. 26) zusammenzufassen, der am Ende der Anwendungsinstallation gestartet wird. Im Rahmen des Assistenten können Sie die Anwendung aktivieren, Einstellungen für das Update und den Start von Untersuchungsaufgaben vornehmen und den Zugriff auf das Programm mit Hilfe eines Kennworts beschränken.

Wir empfehlen Ihnen, nach der Installation und dem Start des Programms auf Ihrem Computer folgende Aktionen vorzunehmen:

- Bewertung des aktuellen Schutzstatus, um sicherzustellen, dass Kaspersky Anti-Virus den Schutz auf der erforderlichen Stufe gewährleistet (s. Pkt. 5.1 auf S. 43).
- Update des Programms, wenn das Update nicht mit Hilfe des Konfigurationsassistenten oder automatisch sofort nach der Programminstallation erfolgte (s. Pkt. 5.5 auf S. 51).
- Untersuchung des Computers auf das Vorhandensein von Viren (s. Pkt. 5.2 auf S. 49).

5.1. Welchen Schutzstatus hat der Server?


Zusammenfassende Informationen über den Schutz Ihres Computers befinden sich im Hauptfenster von Kaspersky Anti-Virus im Abschnitt **Schutz**. Hier werden der aktuelle *Schutzstatus* des Computers und die *Gesamtstatistik über die Arbeit* des Programms angezeigt.

Der **Schutzstatus** gibt den aktuellen Schutzstatus Ihres Computers mit Hilfe spezieller Indikatoren (s. Pkt. 5.1.1 auf S. 44) wieder. Die Statistik (s. Pkt. 5.1.2 auf S. 47) enthält die Ergebnisse der laufenden Programmarbeit.

5.1.1. Schutzindikatoren

Der **Schutzstatus** wird durch drei Indikatoren bestimmt (s. Abb. Abbildung 4), welche die Schutzstufe Ihres Computers zum aktuellen Zeitpunkt darstellen und auf Probleme in den Einstellungen und bei der Arbeit des Programms hinweisen.

Die Prioritätsstufe eines Ereignisses, das durch den Indikator dargestellt wird, kann einen der folgenden Werte besitzen:

-  – *Der Indikator besitzt informativen Charakter.* Der Schutz Ihres Computers entspricht der erforderlichen Stufe und es wurden keinerlei Probleme in den Programmeinstellungen und bei der Arbeit der Komponenten beobachtet.

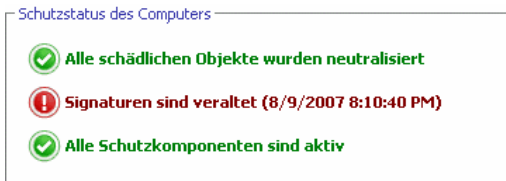






Abbildung 4. Indikatoren, die den Schutzstatus des Computers darstellen

-  – *Der Indikator warnt vor bestimmten Abweichungen* vom empfohlenen Funktionsmodus bei der Arbeit von Kaspersky Anti-Virus, die sich auf den Datenschutz auswirken können. Bitte beachten Sie unbedingt die Empfehlungen der Kaspersky-Lab-Spezialisten, die im Abschnitt für Kommentare und Tipps im Programmhauptfenster angezeigt werden.
-  – *Der Indikator verweist auf kritische Situationen* im Schutz Ihres Computers. Bitte befolgen Sie unbedingt die Empfehlungen der Kaspersky-Lab-Spezialisten, die im Abschnitt für Kommentare und Tipps im Programmhauptfenster angezeigt werden. Sie dienen der Erhöhung des Schutzes Ihres Computers. Die empfohlenen Aktionen besitzen die Form von Links.



Im Folgenden werden die Schutzindikatoren und die ihnen entsprechenden Situationen genauer beschrieben.


Der erste Indikator weist auf eine Situation im Zusammenhang mit schädlichen Objekten auf Ihrem Computer hin. Der Indikator kann folgende Werte annehmen:

	<p><i>Es wurden keine schädlichen Objekte gefunden</i></p> <p>Kaspersky Anti-Virus hat auf Ihrem Computer keinerlei gefährlichen Objekte gefunden.</p>
	<p><i>Alle schädlichen Objekte wurden neutralisiert</i></p>


	Kaspersky Anti-Virus hat alle von Viren infizierten Objekte desinfiziert und irreparable Objekte gelöscht.
	<p><i>Es wurden schädliche Objekte gefunden</i></p> <p>Auf Ihrem Computer besteht momentan das Risiko einer Infektion. Kaspersky Anti-Virus hat schädliche Objekte gefunden, deren Desinfektion erforderlich ist. Verwenden Sie dazu den Link <u>Alle desinfizieren</u>. Mit dem Link <u>Details</u> erhalten Sie Detailinformationen über die schädlichen Objekte.</p>


Der zweite Indikator gibt an, wie aktuell der Schutz Ihres Computers momentan ist. Der Indikator kann folgende Werte annehmen:

	<p><i>Signaturen sind erschienen am (Datum, Uhrzeit)</i></p> <p>Das Programm benötigt keine Aktualisierung. Alle Dankenbanken, die bei der Arbeit von Kaspersky Anti-Virus verwendet werden, enthalten aktuelle Informationen für den Schutz Ihres Computers.</p>
	<p><i>Signaturen sind nicht aktuell</i></p> <p>Die Programm-Module und die Bedrohungssignaturen von Kaspersky Anti-Virus wurden seit mehreren Tagen nicht aktualisiert. Sie setzen Ihren Computer dem Risiko einer Infektion durch neue Schadprogramme oder neue Angriffe aus, die seit dem Tag des letzten Programm-Updates aufgetaucht sind. Es wird nachdrücklich empfohlen, Kaspersky Anti-Virus zu aktualisieren. Verwenden Sie dazu den Link <u>Aktualisieren</u>.</p>
	<p><i>Signaturen sind teilweise beschädigt</i></p> <p>Die Dateien mit den Bedrohungssignaturen sind teilweise beschädigt. In diesem Fall wird empfohlen, das Programm-Update erneut zu starten. Wenn der Fehler durch das erneute Update nicht behoben werden kann, wenden Sie sich an den technischen Support-Service von Kaspersky Lab.</p>
	<p><i>Der Neustart des Computers ist erforderlich</i></p> <p>Für die korrekte Aktualisierung des Programms ist der Systemneustart erforderlich. Speichern und schließen Sie alle Dateien, mit denen Sie gearbeitet haben, und verwenden Sie den Link <u>Computer neu starten</u>.</p>

	<p><i>Das Programm-Update ist deaktiviert</i></p> <p>Der Dienst für das Update der Bedrohungssignaturen und Programm-Module ist deaktiviert. Um den aktuellen Zustand des Schutzes aufrechtzuerhalten, wird empfohlen, das Update zu aktivieren.</p>
	<p><i>Signaturen sind veraltet</i></p> <p>Kaspersky Anti-Virus wurde sehr lange nicht aktualisiert. Die Daten auf Ihrem Computer unterliegen einem großen Risiko. Aktualisieren Sie das Programm so schnell wie möglich. Verwenden Sie dazu den Link Aktualisieren.</p>
	<p><i>Signaturen sind beschädigt</i></p> <p>Die Dateien mit den Bedrohungssignaturen sind vollständig beschädigt. In diesem Fall wird empfohlen, das Programm-Update erneut zu starten. Wenn der Fehler durch das erneute Update nicht behoben werden kann, wenden Sie sich an den technischen Support-Service von Kaspersky Lab.</p>

Der dritte Indikator gibt an, inwieweit die Möglichkeiten des Programms genutzt werden. Der Indikator kann folgende Werte annehmen:

	<p><i>Alle Schutzkomponenten sind aktiv</i></p> <p>Kaspersky Anti-Virus schützt Ihren Computer auf allen Kanälen, über die schädliche Programme eindringen können.</p>
	<p><i>Der Schutz ist nicht installiert</i></p> <p>Bei der Installation von Kaspersky Anti-Virus wurde keine der Echtzeitschutz-Komponenten installiert. In diesem Fall steht nur die Virenuntersuchung von Objekten zur Verfügung. Um die maximale Sicherheit des Computers zu gewährleisten, wird empfohlen, die Schutzkomponenten zu installieren.</p>
	<p><i>Alle Schutzkomponenten wurden angehalten</i></p> <p>Die Arbeit der Schutzkomponente wurde für einen bestimmten Zeitraum angehalten. Um die Arbeit der Komponente wiederaufzunehmen, wählen Sie im Kontextmenü den Punkt Schutz aktivieren. Das Kontextmenü wird durch Klick auf das Programmsymbol in der Taskleiste geöffnet.</p>

	<p><i>Alle Schutzkomponenten wurden deaktiviert</i></p> <p>Der Schutz des Computers wurde vollständig abgeschaltet. Die Schutzkomponente arbeitet nicht. Um die Arbeit der Komponente wiederaufzunehmen, wählen Sie im Kontextmenü den Punkt Schutz aktivieren. Das Kontextmenü wird durch Klick auf das Programmsymbol in der Taskleiste geöffnet.</p>
	<p><i>Einige Schutzkomponenten sind beschädigt</i></p> <p>Bei der Arbeit einer Schutzkomponente von Kaspersky Anti-Virus ist eine Störung eingetreten. In dieser Situation wird empfohlen, die Komponente zu aktivieren oder den Computer neu zu starten (möglicherweise ist nach der Übernahme von Updates die Registrierung von Komponententreibern erforderlich).</p>

5.1.2. Status einer einzelnen Komponente von Kaspersky Anti-Virus

Um zu erfahren, wie Kaspersky Anti-Virus das Dateisystem schützt, wie die Aufgaben zur Virensuche arbeiten und wie das Update der Bedrohungssignaturen ausgeführt wird, öffnen Sie einfach den entsprechenden Abschnitt des Programmhauptfensters.


Um beispielsweise den aktuellen Status des Dateischutzes zu überprüfen, wählen Sie den Abschnitt **Datei-Anti-Virus** auf der linken Seite des Programmhauptfensters. Auf der rechten Seite werden zusammenfassende Informationen über die Arbeit der Komponente angezeigt.


Für Datei-Anti-Virus bestehen diese Informationen aus folgenden Elementen: **Statuszeile**, **Status** (für Untersuchungs- und Update-Aufgaben – **Einstellungen**) und **Statistik**.

Betrachten wir die **Statuszeile** von Datei-Anti-Virus:



- *Datei-Anti-Virus* : aktiv – Der Dateischutz funktioniert auf der gewählten Stufe (s. Pkt. 7.1 auf S. 74).
- *Datei-Anti-Virus* : Pause – Der *Datei-Anti-Virus* wurde für einen bestimmten Zeitraum angehalten. Die Komponente nimmt ihre Arbeit automatisch nach Ablauf des festgelegten Zeitraums oder nach dem Neustart des Programms wieder auf. Sie können den Dateischutz

manuell aktivieren. Klicken Sie dazu in der Statuszeile auf die Schaltfläche .

- *Datei-Anti-Virus : deaktiviert* – Die Arbeit der Komponente wurde vom Benutzer beendet. Sie können den Dateischutz aktivieren. Klicken Sie dazu in der Statuszeile auf die Schaltfläche .
- *Datei-Anti-Virus : funktioniert nicht* – Der Dateischutz ist aus bestimmten Gründen nicht verfügbar.
- *Datei-Anti-Virus : Störung*– Die Komponente hat ihre Arbeit fehlerhaft abgeschlossen.

Wenn bei der Arbeit der Komponente ein Fehler auftritt, versuchen Sie sie erneut zu starten. Sollte auch der wiederholte Start fehlerhaft verlaufen, dann prüfen Sie den Bericht über die Arbeit der Komponente. Möglicherweise finden Sie dort den Grund der Störung. Wenn Sie das Problem nicht selbst lösen können, speichern Sie den Bericht über die Arbeit der Komponente mit der Schaltfläche **Aktionen** → **Speichern unter** in einer Datei und wenden Sie sich an den Technischen Support-Service von Kaspersky Lab.

Die Einstellungen, mit denen die Komponente arbeitet, werden im Block **Status** angezeigt:

- *Datei-Anti-Virus* – aktueller Status der Komponente (aktiv, funktioniert nicht, Pause usw.).
- *Sicherheitsstufe* – Auswahl von Funktionsparametern der Komponente, nach denen die Anwendung den Dateischutz gewährleistet. In der Grundeinstellung wird die **Empfohlene** Sicherheitsstufe verwendet, auf der nur jene Objekte des Dateisystems untersucht werden, die infiziert werden können. Dazu zählen beispielsweise ausführbare Dateien (exe-Dateien).
- *Aktion*, die beim Fund eines schädlichen Objekts ausgeführt wird.

Für Aufgaben zur Virensuche und zum Programm-Update ist der Block **Status** nicht vorhanden. Die Sicherheitsstufe, die im Rahmen der Virensuche auf ein gefährliches Programm anzuwendende Aktion und der Update-Startmodus werden im Block **Einstellungen** genannt.

Der Block **Statistik** enthält die Arbeitsergebnisse der Schutzkomponente, des Updates oder der Untersuchungsaufgabe.

5.1.3. Statistik der Programmarbeit

Die Statistik über die Arbeit des Programms wird im Block **Statistik** des Abschnitts **Schutz** im Programmhauptfenster angezeigt (s. Abb. 5) und enthält

Informationen über den Schutz des Computers, die seit der Installation von Kaspersky Anti-Virus aufgezeichnet wurden.

Statistik	
<u>Insgesamt untersucht:</u>	2063
<u>Gefunden:</u>	0
<u>Zuletzt untersuchte Datei:</u>	e2s_temp_sbscr_INFpolicy.ctrl

Abbildung 5. Block mit Gesamtstatistik über die Arbeit des Programms

Durch Linksklick an eine beliebige Stelle des Blocks können Sie einen Bericht mit detaillierten Informationen öffnen. Auf den entsprechenden Registerkarten befinden sich folgende Informationen:

- Informationen über gefundene Objekte (s. Pkt. 11.3.2 auf S. 133) und den Status, der den Objekten zugewiesen wurde.
- Ereignisbericht (s. Pkt. 11.3.3 auf S. 134)
- Zusammenfassende Statistik über die Untersuchung des Computers (s. Pkt. 11.3.4 auf S. 135)
- Einstellungen für die Arbeit des Programms (s. Pkt. 11.3.5 auf S. 135)

5.2. Wie der Server auf Viren untersucht wird

Nach der Installation der Anwendung werden Sie durch eine obligatorische Meldung im unteren linken Bereich des Anwendungsfensters darauf hingewiesen, dass noch keine Untersuchung des Servers ausgeführt wurde, und Ihnen wird empfohlen, ihn umgehend auf Viren zu untersuchen.

Der Lieferumfang von Kaspersky Anti-Virus umfasst eine Aufgabe zur Virensuche auf dem Computer. Diese befindet sich im Abschnitt **Virensuche** des Programmhauptfensters.

Nach der Auswahl der Aufgabe **Arbeitsplatz** können Sie die Statistik der letzten Untersuchung des Computers und die Aufgabenparameter überprüfen: welche Sicherheitsstufe wurde gewählt, welche Aktion wird auf gefährliche Objekte angewandt.

Um den Computer auf die Existenz von schädlichen Objekten zu untersuchen,

1. Öffnen Sie das Programmhauptfenster und wählen Sie im Abschnitt **Virensuche** die Aufgabe **Arbeitsplatz**.
2. Klicken Sie auf die Schaltfläche **Virensuche**.

Dadurch wird die Untersuchung Ihres Computers gestartet. Details der Untersuchung werden in einem speziellen Fenster angezeigt. Durch Klick auf die Schaltfläche **Schließen** wird das Fenster mit Informationen über den Untersuchungsvorgang ausgeblendet. Die Untersuchung wird dadurch nicht beendet.

5.3. Wie kritische Serverbereiche untersucht werden

Es ist äußerst wichtig, die kritischen Bereiche des Computers zu schützen, um seine Funktionsfähigkeit aufrechtzuerhalten. Kaspersky Anti-Virus bietet eine spezielle Aufgabe zur Virensuche in diesen Bereichen. Sie befindet sich im Abschnitt **Virensuche** des Programmhauptfensters.

Nach der Auswahl der Aufgabe **Kritische Bereiche** können Sie die Statistik der letzten Untersuchung dieser Bereiche und die Aufgabenparameter überprüfen: welche Sicherheitsstufe wurde gewählt, welche Aktion wird auf gefährliche Objekte angewandt. Hier kann auch festgelegt werden, welche kritischen Bereiche untersucht werden sollen. Außerdem kann hier die Virensuche in den ausgewählten Bereichen gestartet werden.

Um die kritischen Computerbereiche auf die Existenz von schädlichen Objekten zu untersuchen,

1. Öffnen Sie das Programmhauptfenster und wählen Sie im Abschnitt **Virensuche** die Aufgabe **Kritische Bereiche**.
2. Klicken Sie auf die Schaltfläche **Virensuche**.

Dadurch wird die Untersuchung der ausgewählten Bereiche gestartet. Details der Untersuchung werden in einem speziellen Fenster angezeigt. Durch Klick auf die Schaltfläche **Schließen** wird das Fenster mit Informationen über den Untersuchungsvorgang ausgeblendet. Die Untersuchung wird dadurch nicht beendet.

5.4. Wie eine Datei, ein Ordner oder ein Laufwerk auf Viren untersucht werden

In bestimmten Situationen ist es erforderlich, nicht den gesamten Computer zu untersuchen, sondern nur ein einzelnes Objekt wie beispielsweise eine

Festplatte. Sie können ein Objekt mit den Standardmitteln von Microsoft Windows Server auswählen (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.).

Um die Untersuchung des Objekts zu starten,

führen Sie den Mauscursor auf den Namen des gewählten Objekts, öffnen durch Rechtsklick das Microsoft Windows Server-Kontextmenü und wählen den Punkt **Auf Viren untersuchen** (s. Abb. 6).

Dadurch wird die Untersuchung des ausgewählten Objekts gestartet. Details der Untersuchung werden in einem speziellen Fenster angezeigt. Durch Klick auf die Schaltfläche **Schließen** wird das Fenster mit Informationen über den Untersuchungsvorgang ausgeblendet. Die Untersuchung wird dadurch nicht beendet.



Abbildung 6. Virenuntersuchung eines Objekts, das über Microsoft Windows Server ausgewählt wurde

5.5. Wie das Programm aktualisiert wird

Kaspersky Lab aktualisiert die Bedrohungssignaturen und die Module von Kaspersky Anti-Virus und verwendet dazu spezielle Updateserver.

Kaspersky-Lab-Updateserver sind Internetseiten von Kaspersky Lab, auf denen Programm-Updates zur Verfügung stehen.

Achtung!

Für das Update von Kaspersky Anti-Virus ist eine bestehende Internetverbindung erforderlich.

Kaspersky Anti-Virus überprüft in der Grundeinstellung automatisch, ob auf den Kaspersky-Lab-Servern neue Updates vorhanden sind. Wenn auf dem Server neue Updates angeboten werden, lädt Kaspersky Anti-Virus sie im Hintergrundmodus herunter und installiert sie.

Um Kaspersky Anti-Virus manuell zu aktualisieren,

wählen Sie die Komponente **Update** im Abschnitt **Service** des Programmhauptfensters und klicken Sie auf der rechten Seite auf die Schaltfläche **Update**.

Dadurch wird die Aktualisierung von Kaspersky Anti-Virus gestartet. Alle Details über den Prozess werden in einem speziellen Fenster angezeigt.

5.6. Was tun, wenn der Schutz nicht funktioniert?

Sollten bei der Arbeit von Datei-Anti-Virus Probleme oder Fehler auftreten, beachten Sie unbedingt seinen Status. Wenn der Status *funktioniert nicht* oder *Störung* angezeigt wird, versuchen Sie, die Anwendung neu zu starten.

Sollte das Problem nach dem Neustart der Anwendung weiter bestehen, wird empfohlen, mögliche Fehler mit Hilfe des Reparaturprogramms für die Anwendung zu korrigieren (**Start** → **Programme** → **Kaspersky Anti-Virus 6.0 for Windows Servers** → **Ändern, Reparieren oder Löschen**).

Falls der Reparaturversuch erfolglos sein sollte, wenden Sie sich an den Technischen Support-Service von Kaspersky Lab. Es kann erforderlich sein, den Bericht über die Arbeit der Komponente oder der Anwendung in einer Datei zu speichern und diese Datei an den technischen Kundendienst zu senden, damit die Mitarbeiter das Problem genau analysieren können.

Um den Bericht in einer Datei zu speichern,

1. Wählen Sie Datei-Anti-Virus im Abschnitt **Schutz** des Programmhauptfensters und klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks **Statistik**.
2. Klicken Sie auf die Schaltfläche **Speichern unter** und geben Sie im folgenden Fenster den Namen der Datei an, in welcher die Arbeitsergebnisse der Komponente gespeichert werden sollen.

Um einen Bericht über den Start und Status aller Komponenten von Kaspersky Anti-Virus (Datei-Anti-Virus, Aufgaben zur Virensuche und Servicefunktionen) zu speichern,

1. Wählen Sie den Abschnitt **Schutz** im Programmhauptfenster und klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks **Statistik**.

oder

Verwenden Sie im Berichtsfenster einer beliebigen Komponente den Hyperlink Liste aller Berichte. Dadurch werden die Berichte aller Programmkomponenten auf der Registerkarte **Berichte** angezeigt.

2. Klicken Sie auf die Schaltfläche **Speichern unter** und geben Sie im folgenden Fenster den Namen der Datei an, in welcher die Arbeitsergebnisse des Programms gespeichert werden sollen.

KAPITEL 6. KOMPLEXE STEUERUNG DES SCHUTZES

Kaspersky Anti-Virus bietet Ihnen die Möglichkeit zur komplexen Steuerung seiner Arbeit:

- Aktivieren, Deaktivieren oder Anhalten der Arbeit des Programms (s. Pkt. 6.1 auf S. 54).
- Die Typen gefährlicher Programme festlegen, vor denen Kaspersky Anti-Virus Ihren Computer schützen soll (s. Pkt. 6.2 auf S. 59).
- Erstellen einer Liste von Ausnahmen für den Schutz (s. Pkt. 6.3 auf S. 60).
- Erstellen eigener Aufgaben für die Virensuche und das Update (s. Pkt. 6.4 auf S. 67).
- Festlegen eines eigenen Zeitplans für den Aufgabenstart (s. Pkt. 6.5 auf S. 69).
- Anpassen der Leistungsparameter (s. Pkt. 6.6 auf S. 71) für den Computerschutz.

6.1. Serverschutz deaktivieren/ aktivieren

Kaspersky Anti-Virus wird standardmäßig beim Start des Betriebssystems gestartet, worüber Sie durch den Hinweis *Kaspersky Anti-Virus 6.0* rechts oben auf dem Bildschirm informiert werden, und schützt Ihren Computer während der gesamten Sitzung. Datei-Anti-Virus ist aktiv (s. Pkt. 2.2.1 auf S. 15).

Sie können den von Kaspersky Anti-Virus gewährleisteten Schutz deaktivieren.

Achtung!

Sie Kaspersky-Lab-Spezialisten **warnen ausdrücklich davor, den Schutz zu deaktivieren**, weil dies zur Infektion Ihres Computers und zu Datenverlust führen kann.

Beachten Sie, dass der Schutz hier ausdrücklich im Kontext von Datei-Anti-Virus beschrieben wird. Das Deaktivieren oder das Anhalten der Arbeit von Datei-Anti-Virus übt keinen Einfluss auf die Ausführung von Aufgaben zur Virensuche und auf das Programm-Update aus.

6.1.1. Serverschutz anhalten

Das Anhalten des Schutzes bedeutet, dass Datei-Anti-Virus für einen bestimmten Zeitraum deaktiviert wird.

Um die Arbeit von Kaspersky Anti-Virus anzuhalten,

1. Wählen Sie im Kontextmenü (s. Pkt. 4.2 auf S. 38) des Programms den Punkt **Schutz anhalten**.
2. Wählen Sie im folgenden Fenster zum Deaktivieren des Schutzes (s. Abb. 7) den Zeitraum, nach dem der Schutz wieder aktiviert werden soll:
 - **In <Zeitraum>** – Der Schutz wird nach Ablauf des festgelegten Zeitraums wieder aktiviert. Verwenden Sie die Dropdown-Liste, um den Wert für das Zeitintervall festzulegen.
 - **Nach dem Neustart des Programms** – Der Schutz wird aktiviert, wenn Sie das Programm aus dem Menü **Start** starten oder nachdem das System neu gestartet wurde (unter der Bedingung, dass der Modus zum Anwendungsstart beim Hochfahren des Computers aktiviert ist (s. Pkt. 6.1.5 auf S. 58).
 - **Nur auf Befehl des Benutzers** – Der Schutz wird erst dann wieder aktiviert, wenn Sie ihn starten. Wählen Sie den Punkt **Schutz aktivieren** im Kontextmenü des Programms, um den Schutz zu aktivieren.

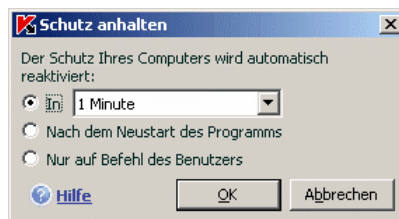



Abbildung 7. Fenster zum Anhalten des Computerschutzes

Hinweis:

Um den Schutz des Servers zu deaktivieren, stehen folgende Methoden zur Verfügung:

- Klicken Sie auf die Schaltfläche **II** im Abschnitt **Schutz**.
- Wählen Sie im Kontextmenü den Punkt **Beenden**. In diesem Fall wird die Anwendung aus dem Arbeitsspeicher entfernt.

Durch das vorübergehende Deaktivieren wird die Arbeit von Datei-Anti-Virus angehalten. Darüber informieren:

- Der inaktive (graue Farbe) Name von Datei-Anti-Virus im Abschnitt **Schutz** des Hauptfensters.
- Das inaktive (graue) Programmsymbol im Infobereich der Taskleiste.
- Der dritte Schutzindikator (s. Pkt. 5.1.1 auf S. 44) Ihres Computers zeigt folgenden Hinweis:  **Alle Schutzkomponenten wurden angehalten**

6.1.2. Serverschutz vollständig deaktivieren


Das vollständige Deaktivieren des Schutzes bedeutet, dass die Arbeit von Datei-Anti-Virus beendet wird. Die Virensuche und das Update funktionieren weiterhin im vorgegebenen Modus.

Wenn der Schutz vollständig deaktiviert wurde, kann er nur auf Befehl des Administrators wieder aktiviert werden. In diesem Fall wird Datei-Anti-Virus nach dem Neustart des Systems oder der Anwendung nicht automatisch aktiviert. Beachten Sie, dass bei Konflikten zwischen Kaspersky Anti-Virus und anderen auf Ihrem Computer installierten Programmen die Arbeit von Datei-Anti-Virus angehalten oder eine Liste von Ausnahmen angelegt werden kann (s. Pkt. 6.3 auf S. 60).

Um den Schutz des Servers vollständig zu deaktivieren,

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Anti-Virus und wählen Sie den Abschnitt **Schutz**.
2. Deaktivieren Sie das Kontrollkästchen **Schutz aktivieren**.


Durch das Deaktivieren des Schutzes wird die Arbeit von Datei-Anti-Virus beendet. Darüber informieren:


1. Der inaktive (graue) Name von Datei-Anti-Virus im Abschnitt **Schutz** des Hauptfensters.
2. Das inaktive (schwarz-weiße) Programmsymbol im Infobereich der Taskleiste.
3. Der dritte Schutzindikator (s. Pkt. 5.1.1 auf S. 44) Ihres Computers, zeigt folgenden Hinweis:  **Alle Schutzkomponenten wurden deaktiviert.**

6.1.3. Schutzkomponenten oder Aufgaben anhalten/ beenden

Es gibt mehrere Methoden, um die Arbeit von Datei-Anti-Virus, einer Aufgabe zur Virensuche oder zum Update zu deaktivieren. Vor dem Deaktivieren sollten die Gründe dafür allerdings genau abgewogen werden. Höchstwahrscheinlich besteht eine andere Möglichkeit zur Lösung des Problems, beispielsweise die Wahl einer anderen Sicherheitsstufe. Wenn Sie beispielsweise mit einer bestimmten Datenbank arbeiten, von der Sie sicher sind, dass sie virenfrei ist, geben Sie das Verzeichnis mit ihren Dateien einfach als Ausnahme an (s. Pkt. 6.3 auf S. 60).


Um die Arbeit von Datei-Anti-Virus, die Ausführung einer Untersuchungsaufgabe oder des Updates anzuhalten,

wählen Sie die Komponente oder die Aufgabe im entsprechenden Abschnitt auf der linken Seite des Hauptfensters aus und klicken Sie in der Statuszeile auf die Schaltfläche .

Der Status der Komponente (Aufgabe) ändert sich in *Pause*. Der Schutz, den die Komponente bietet, oder die ausgeführte Aufgabe wird solange angehalten, bis Sie die Arbeit mit der Schaltfläche  fortsetzen.

Wenn Sie die Arbeit einer Komponente oder Aufgabe anhalten, wird die Statistik in der laufenden Sitzung von Kaspersky Anti-Virus gespeichert. Die Statistik wird fortgeführt, wenn die Arbeit der Komponente oder Aufgabe wieder aufgenommen wird.

Um die Arbeit der Komponente oder einer Aufgabe zu beenden,

klicken Sie in der Statuszeile auf die Schaltfläche . Die Arbeit der Komponenten kann auch im Konfigurationsfenster der Anwendung beendet werden, indem das Kontrollkästchen **<Komponentenname> aktivieren** im Block **Allgemein** deaktiviert wird.

In diesem Fall ändert sich der Status der Komponente (Aufgabe) in *deaktiviert (abgebrochen)*. Der durch die Komponente gewährleistete Schutz oder die ausgeführte Aufgabe wird beendet, bis Sie ihn/sie mit Hilfe der Schaltfläche ► neu starten. Für eine Untersuchungs- und Update-Aufgabe werden Ihnen folgende Aktionen zur Auswahl angeboten: Ausführung der abgebrochenen Aufgabe fortsetzen oder Aufgabe neu starten.

Beim Beenden einer Komponente oder einer Aufgabe wird die gesamte Statistik über die bisherige Arbeit zurückgesetzt und beim Start der Komponente neu erstellt.

6.1.4. Serverschutz wiederherstellen


Wenn Sie zu einem gewissen Zeitpunkt den Schutz Ihres Computers angehalten oder vollständig deaktiviert haben, dann kann er durch eine der folgenden Methoden wieder aktiviert werden:

- *Aus dem Kontextmenü.*

Wählen Sie dazu den Punkt **Schutz aktivieren**.

- *Aus dem Programmhauptfenster.*

Klicken Sie dazu auf die Schaltfläche ► in der Statuszeile des Abschnitts **Schutz** des Hauptfensters.

Der Schutzstatus ändert sich sofort in *aktiv*. Das Programmsymbol im Infobereich wird aktiv (farbig). Der dritte Schutzindikator (s. Pkt. 5.1.1 auf S. 44) des Computers, zeigt folgenden Hinweis:  **Alle Schutzkomponenten sind aktiv.**

6.1.5. Arbeit mit der Anwendung beenden

Wenn es aus einem bestimmten Grund erforderlich ist, die Arbeit von Kaspersky Anti-Virus vollständig zu beenden, wählen Sie den Punkt **Beenden** im Kontextmenü (s. Pkt. 4.2 auf S. 38) des Programms. Dadurch wird das Programm aus dem Arbeitsspeicher entfernt, was bedeutet, dass Ihr Computer dann ungeschützt ist.

Nachdem Sie die Arbeit des Programms beendet haben, kann der Schutz des Computers erneut aktiviert werden, indem das Programm Kaspersky Anti-Virus über das Menü **Start** → **Programme** → **Kaspersky Anti-Virus 6.0 for Windows Servers** → **Kaspersky Anti-Virus 6.0 for Windows Servers** gestartet wird.

Außerdem kann der Schutz nach dem Neustart des Betriebssystems automatisch gestartet werden. Um diesen Modus zu wählen, verwenden Sie im Konfigurationsfenster des Programms den Abschnitt **Schutz** und aktivieren Sie das Kontrollkästchen **Programm beim Hochfahren des Computers starten**.

6.2. Typen der zu kontrollierenden schädlichen Programme

Die Anwendung Kaspersky Anti-Virus bietet Ihnen Schutz vor verschiedenen Arten schädlicher Programme. Unabhängig von den festgelegten Parametern schützt das Programm Ihren Computer stets vor den gefährlichsten Malware-Arten. Dazu zählen Viren, trojanische Programme und Hacker-Utilities. Diese Programme können Ihrem Computer ernststen Schaden zufügen. Um die Sicherheit des Computers zu erhöhen, können Sie die Liste der erkennbaren Bedrohungen erweitern. Aktivieren Sie dazu die Kontrolle über unterschiedliche Arten potentiell gefährlicher Programme.

Um auszuwählen, vor welchen Arten schädlicher Programme Kaspersky Anti-Virus den Computer schützen soll, wählen Sie im Konfigurationsfenster des Programms (s. Pkt. 4.4 auf S. 41) den Abschnitt **Schutz**.

Die Bedrohungstypen (s. Pkt. 1.1 auf S. 7) werden im Block **Kategorien für schädliche Software** genannt:

- Viren, Würmer, Trojaner und Hackerprogramme.** Diese Gruppe umfasst die meistverbreiteten und gefährlichsten Kategorien schädlicher Programme. Der Schutz vor diesen Bedrohungen gewährleistet das minimal erforderliche Sicherheitsniveau. In Übereinstimmung mit den Empfehlungen der Kaspersky-Lab-Spezialisten kontrolliert Kaspersky Anti-Virus die schädlichen Programme dieser Kategorie immer.
- Spyware, Adware, Dialer.** Diese Gruppe enthält potentiell gefährliche Software, die den Benutzer behindern oder dem Computer bedeutenden Schaden zufügen kann.
- Potentiell gefährliche Software (Riskware).** Diese Gruppe umfasst Programme, die nicht schädlich oder gefährlich sind, aber unter bestimmten Umständen benutzt werden können, um Ihrem Computer Schaden zuzufügen.

Die genannten Gruppen regulieren, in welchem Umfang die Bedrohungssignaturen bei der Virensuche auf Ihrem Computer verwendet werden.

Wenn alle Gruppen gewählt wurden, bietet Kaspersky Anti-Virus den maximalen Virenschutz Ihres Computers. Wenn die zweite und dritte Gruppe deaktiviert ist, schützt das Programm Sie nur vor den meistverbreiteten schädlichen Objekten.

Dabei werden potentiell gefährliche und andere Programme nicht kontrolliert, die auf Ihrem Computer installiert werden können und durch ihre Aktionen Imageverlust und materiellen Schaden verursachen können.

Die Kaspersky-Lab-Spezialisten warnen davor, die Kontrolle der zweiten Gruppe zu deaktivieren. Sollte es vorkommen, dass Kaspersky Anti-Virus ein Programm als gefährlich klassifiziert, das Ihrer Meinung nach kein Risiko darstellt, dann wird empfohlen, es als Ausnahme festzulegen (s. Pkt. 6.3 auf S. 60).

6.3. Aufbau einer vertrauenswürdigen Zone

Die *vertrauenswürdige Zone* ist eine vom Administrator erstellte Liste von Objekten, die Kaspersky Anti-Virus bei seiner Arbeit nicht kontrolliert. Mit anderen Worten ist dies eine Auswahl von Ausnahmen für den Schutz des Programms.

Die vertrauenswürdige Zone wird vom Administrator unter Berücksichtigung der Besonderheiten von Objekten, mit denen er arbeitet, sowie von Programmen, die auf seinem Computer installiert sind, aufgebaut. Das Anlegen einer solchen Liste mit Ausnahmen kann beispielsweise erforderlich sein, wenn Kaspersky Anti-Virus den Zugriff auf ein bestimmtes Objekt oder Programm blockiert, Sie aber sicher sind, dass dieses Objekt bzw. Programm absolut unschädlich ist.

Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm), Programmprozesse oder Objekte entsprechend der Klassifikation der Viren-Enzyklopädie (nach dem Status, der dem Objekt bei der Untersuchung von der Anwendung zugewiesen wurde) ausgeschlossen werden.

Achtung!

Ein ausgeschlossenes Objekt unterliegt nicht der Untersuchung, wenn das Laufwerk oder der Ordner untersucht wird, auf dem es sich befindet. Wird allerdings ein konkretes Objekt zur Untersuchung ausgewählt, dann wird die Ausnahmeregel ignoriert.

Um eine Liste von Ausnahmen für den Schutz zu erstellen,

1. Öffnen Sie das Konfigurationsfenster des Programms und wählen Sie den Abschnitt **Echtzeitschutz**.
2. Klicken Sie auf die Schaltfläche **Vertrauenswürdige Zone** im Block **Allgemein**.

Konfigurieren Sie im folgenden Fenster (s. Abb. 8) die Ausnahmeregeln für Objekte und legen Sie die Liste der vertrauenswürdigen Anwendungen an.

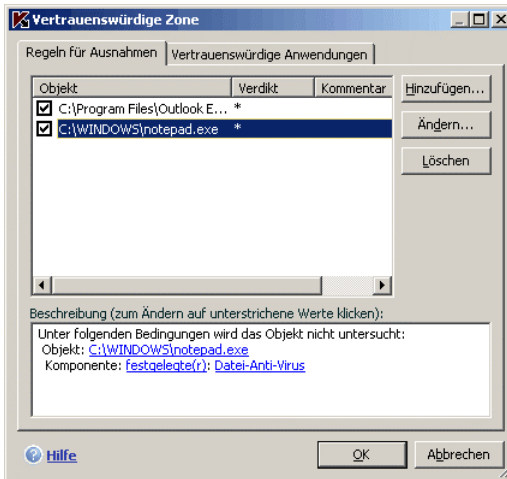


Abbildung 8. Erstellen der vertrauenswürdigen Zone

6.3.1. Ausnahmeregeln

Eine *Ausnahmeregel* ist eine Kombination von Bedingungen, bei deren Vorhandensein ein Objekt nicht von dem Programm Kaspersky Anti-Virus untersucht wird.

Von der Untersuchung können Dateien eines bestimmten Formats, Dateien nach Maske, bestimmte Bereiche (beispielsweise ein Ordner oder Programm), Prozesse oder Objekte entsprechend der Klassifikation der Viren-Enzyklopädie ausgeschlossen werden.

Klassifikation bedeutet den Status, der einem Objekt bei der Untersuchung von der Anwendung Kaspersky Anti-Virus zugewiesen wird. Der Status beruht auf der Klassifikation schädlicher und potentiell gefährlicher Programme, die in der Viren-Enzyklopädie von Kaspersky Lab enthalten ist.

Ein potentiell gefährliches Programm besitzt keine schädliche Funktion, kann aber von einem Schadprogramm als Hilfskomponente benutzt werden, weil es Schwachstellen und Fehler enthält. Zu dieser Kategorie gehören beispielsweise Programme zur entfernten Verwaltung, IRC-Clients, FTP-Server, alle Hilfsprogramme zum Beenden von Prozessen und zum Verstecken ihrer Arbeit, Tastaturspione, Programme zur Kennwortermittlung, Programme zur automatischen Einwahl auf kostenpflichtige Seiten usw. Solche Software wird nicht als Virus klassifiziert (not-a-virus), lässt sich aber beispielsweise in folgende Typen unterteilen: Adware, Joke, Riskware u.a. (ausführliche Informationen über

potentiell gefährliche Programme, die von Kaspersky Anti-Virus entdeckt werden können, finden Sie in der Viren-Enzyklopädie auf der Seite www.viruslist.de. Derartige Programme können aufgrund der Untersuchung gesperrt werden. Da bestimmte Programme, die eine potentielle Gefahr darstellen, von vielen Benutzern verwendet werden, besteht die Möglichkeit, sie von der Untersuchung auszuschließen. Dazu muss der Name oder die Maske der Bedrohung entsprechend der Klassifikation der Viren-Enzyklopädie zur vertrauenswürdigen Zone hinzugefügt werden.

Es kann beispielsweise sein, dass Sie häufig mit dem Programm Remote Administrator arbeiten. Dabei handelt es sich um ein System, das dem entfernten Zugriff dient und die Arbeit auf einem entfernten Computer erlaubt. Diese Anwendungsaktivität wird von Kaspersky Anti-Virus als potentiell gefährlich eingestuft und kann blockiert werden. Um zu verhindern, dass das Programm gesperrt wird, muss eine Ausnahmeregel erstellt werden, in der not-a-virus:RemoteAdmin.Win32.RAdmin.22 als Klassifikation genannt wird.

Beim Hinzufügen einer Ausnahme wird eine Regel erstellt, die danach von Datei-Anti-Virus sowie bei der Ausführung von Aufgaben zur Virensuche verwendet werden kann. Eine Ausnahmeregel kann entweder in dem dafür vorgesehenen Fenster erstellt werden, das aus dem Konfigurationsfenster des Programms geöffnet wird, oder aus der Meldung über den Fund eines Objekts, sowie aus dem Berichtsfenster.

*Hinzufügen einer Ausnahme zu den **Regeln für Ausnahmen**:*

1. Klicken Sie auf der Registerkarte **Regeln für Ausnahmen** auf die Schaltfläche **Hinzufügen**.
2. Legen Sie im folgenden Fenster (s. Abb. 9) im Abschnitt **Parameter** den Typ der Ausnahme fest:

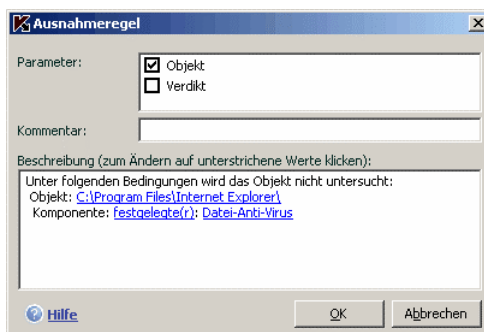


Abbildung 9. Erstellen einer Ausnahmeregel

- Objekt** – Ein bestimmtes Objekt, ein Ordner oder Dateien, die einer bestimmten Maske entsprechen, werden von der Untersuchung ausgeschlossen.
- Klassifikation** – Ein Objekt wird von der Untersuchung ausgeschlossen, wobei sein Status entsprechend der Klassifikation der Viren-Enzyklopädie zugrunde gelegt wird.

Wenn gleichzeitig beide Kontrollkästchen angekreuzt werden, wird eine Regel für das angegebene Objekt mit einem bestimmten Status nach der Klassifikation der Viren-Enzyklopädie erstellt. In diesem Fall gelten folgende Regeln:

- Wenn als **Objekt** eine bestimmte Datei festgelegt wird und als **Klassifikation** ein bestimmter Status, dann wird die gewählte Datei nur dann ausgeschlossen, wenn ihr bei der Untersuchung der Status der festgelegten Bedrohung zugewiesen wurde.
 - Wenn als **Objekt** ein bestimmter Bereich oder ein Ordner angegeben wird und als **Klassifikation** ein Status (oder eine Maske), dann werden nur Objekte des gewählten Status von der Untersuchung ausgeschlossen, die im festgelegten Bereich bzw. Ordner gefunden wurden.
3. Legen Sie Werte für die gewählten Ausnahmetypen fest. Klicken Sie dazu im Abschnitt **Beschreibung** mit der linken Maustaste auf den Link angeben, der sich neben dem Typ der Ausnahme befindet:
- Geben Sie für den Typ **Objekt** im folgenden Fenster den Namen des Objekts an (dabei kann es sich um eine Datei, einen bestimmten Ordner oder eine Dateimaske handeln (s. Anhang A.2 auf S. 196). Aktivieren Sie das Kontrollkästchen **Unterebene einschließen**, damit das festgelegte Objekt (Datei, Dateimaske, Ordner) bei der Untersuchung rekursiv ausgeschlossen wird.
 - Geben Sie als **Klassifikation** den vollständigen Namen der von der Untersuchung auszuschließenden Bedrohung an, wie er in der Viren-Enzyklopädie genannt wird, oder den Namen nach einer Maske (s. Anhang A.3 auf S. 198).
- Für einige Klassifikationsobjekte können im Feld **Erweiterte Einstellungen** zusätzliche Bedingungen für die Verwendung der Regel festgelegt werden.
4. Legen Sie fest, für welche Komponenten von Kaspersky Anti-Virus die neue Regel bei der Arbeit verwendet werden soll. Bei Auswahl des Werts beliebig wird diese Regel für alle Komponenten übernommen. Wenn Sie die Verwendung der Regel auf eine oder mehrere Komponenten beschränken möchten, klicken Sie auf den Link

beliebige. Der Link ändert sich in festgelegte. Durch Klick auf den Link angeben wird ein weiteres Fenster geöffnet. Aktivieren Sie dort die Kontrollkästchen der Komponenten, für welche diese Ausnahmeregel gelten soll.

Hinzufügen einer Ausnahmeregel aus der Programmmeldung über den Fund eines gefährlichen Objekts:

1. Verwenden Sie im Meldungsfenster den Link Zur vertrauenswürdigen Zone hinzufügen.
2. Überprüfen Sie im folgenden Fenster, ob alle Parameter der Ausnahmeregel korrekt sind. Die Felder mit dem Objektnamen und dem zugewiesenen Bedrohungstyp werden aufgrund der Informationen aus der Meldung automatisch ausgefüllt. Klicken Sie auf **OK**, um die Regel zu erstellen.

Erstellen einer Ausnahmeregel vom Berichtsfenster aus:

1. Wählen Sie im Bericht das Objekt aus, das Sie zu den Ausnahmen hinzufügen möchten.
2. Öffnen Sie das Kontextmenü und wählen Sie den Punkt **Zur vertrauenswürdigen Zone hinzufügen** (s. Abb. 10).

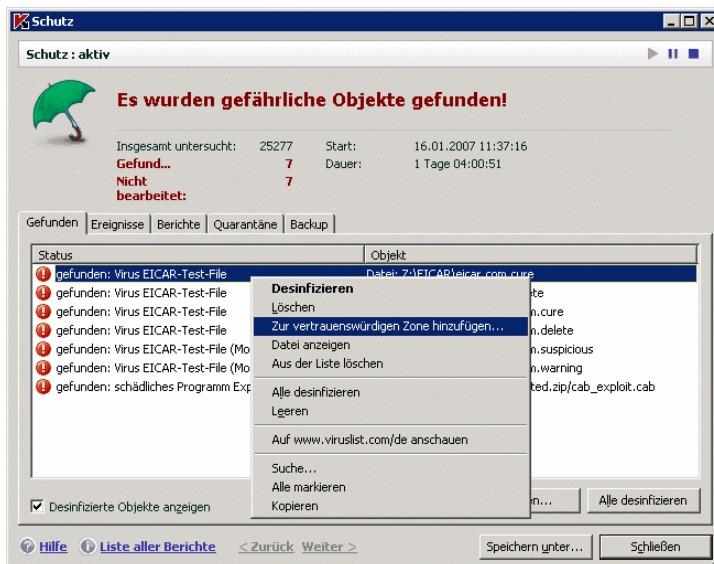


Abbildung 10. Erstellen einer Ausnahmeregel vom Bericht aus

6.3.2. Vertrauenswürdige Anwendungen

Kaspersky Anti-Virus erlaubt es, eine Liste von vertrauenswürdigen Anwendungen zu erstellen, deren Aktivität (einschließlich verdächtiger Aktivität, Dateiaktivität sowie Zugriff auf die Systemregistrierung) nicht kontrolliert werden soll.

Wenn Sie beispielsweise die Objekte, die von dem standardmäßigen Microsoft Windows Server-Programm **Editor** verwendet werden, für ungefährlich und deren Untersuchung im Echtzeitschutz nicht für erforderlich halten, bedeutet das, dass Sie diesem Programm vertrauen. Um die Objekte, die von diesem Prozess benutzt werden, von der Untersuchung auszuschließen, fügen Sie das Programm **Editor** zur Liste der vertrauenswürdigen Anwendungen hinzu. Trotzdem werden aber die ausführbare Datei und der Prozess einer vertrauenswürdigen Anwendung weiterhin auf Viren untersucht. Um eine Anwendung vollständig von der Untersuchung auszuschließen, müssen die Ausnahmeregeln verwendet werden (s. Pkt. 6.3.1 auf S. 61).

Einige Aktionen, die als gefährlich klassifiziert werden, sind im Rahmen der Funktionalität bestimmter Programme normal. Beispielsweise ist das Abfangen eines Texts, den Sie über die Tastatur eingeben, für Programme zum automatischen Umschalten der Tastaturbelegung (Punto Switcher u.ä.) eine normale Aktion. Um die Besonderheit solcher Programme zu berücksichtigen und die Kontrolle ihrer Aktivität abzuschalten, empfehlen wir, sie in die Liste der vertrauenswürdigen Anwendungen aufzunehmen.

Das Ausschließen vertrauenswürdiger Anwendungen aus der Untersuchung erlaubt es außerdem, mögliche Kompatibilitätsprobleme von Kaspersky Anti-Virus mit anderen Anwendungen zu lösen (wenn beispielsweise der Netzwerkverkehr von einem anderen Computer bereits von einer Antiviren-Anwendung untersucht wurde). Außerdem lässt sich auf diese Weise die Leistungsfähigkeit des Computers erhöhen.

Kaspersky Anti-Virus untersucht standardmäßig alle Objekte, die von einem beliebigen Programmprozess geöffnet, gestartet oder gespeichert werden sollen.

Die Liste der vertrauenswürdigen Anwendungen wird auf der Registerkarte **Vertrauenswürdige Anwendungen** erstellt (s. Abb. 11). Bei der Installation von Kaspersky Anti-Virus enthält die Liste der vertrauenswürdigen Anwendungen standardmäßig die Anwendungen, deren Aktivität aufgrund von Empfehlungen der Kaspersky-Lab-Spezialisten nicht analysiert wird. Wenn Sie eine in der Liste enthaltene Anwendung für nicht vertrauenswürdig halten, deaktivieren Sie das entsprechende Kontrollkästchen. Sie können die Liste mit Hilfe der rechts angebrachten Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** bearbeiten.

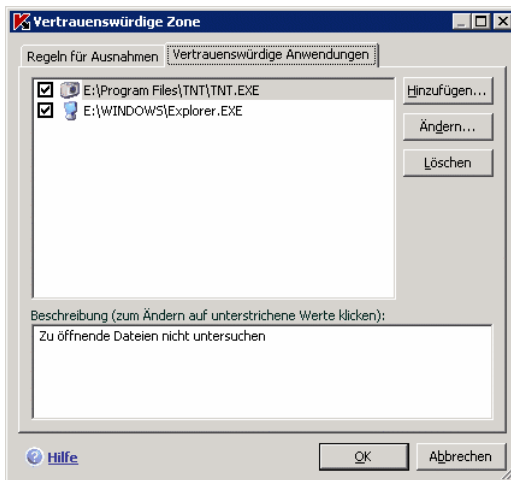


Abbildung 11. Liste der vertrauenswürdigen Anwendungen

Um ein Programm zur Liste der vertrauenswürdigen Anwendungen hinzuzufügen:

1. Klicken Sie auf die Schaltfläche **Hinzufügen**, die sich auf der rechten Seite der Registerkarte **Vertrauenswürdige Anwendung** befindet.
2. Das Fenster **Vertrauenswürdige Anwendung** (s. Abb. 12) wird geöffnet. Klicken Sie zur Auswahl der Anwendung auf die Schaltfläche **Durchsuchen**. Dadurch öffnet sich ein Kontextmenü, in dem Sie mit dem Punkt **Durchsuchen** in das Standardfenster zur Dateiauswahl gelangen und den Pfad der ausführbaren Datei angeben können, oder mit dem Punkt **Anwendungen** zur Liste der momentan aktiven Anwendungen wechseln können, um die gewünschte auszuwählen.

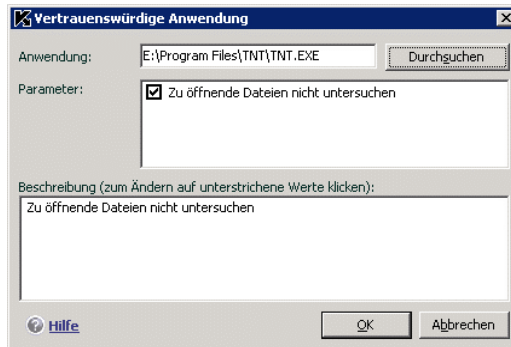


Abbildung 12. Hinzufügen einer Anwendung zur Liste der vertrauenswürdigen Anwendungen

Bei der Auswahl eines Namens speichert Kaspersky Anti-Virus die internen Attribute der ausführbaren Datei, mit denen das Programm bei der Untersuchung als vertrauenswürdige identifiziert wird.

Der Pfad der Datei wird bei der Auswahl des Namens automatisch ergänzt.

3. Geben Sie nun die von diesem Prozess ausführbare Aktion an, die von Kaspersky Anti-Virus nicht kontrolliert werden soll:

- Zu öffnende Dateien nicht untersuchen** – alle Dateien von der Untersuchung ausschließen, die von dem Prozess der vertrauenswürdigen Anwendung geöffnet werden.

6.4. Start von Aufgaben mit Rechten eines anderen Benutzerkontos

In Kaspersky Anti-Virus 6.0 ist ein Dienst zum Aufgabenstart unter einem anderen Benutzerkonto (Impersonalisierung) realisiert. Dieser Dienst ist standardmäßig deaktiviert und Aufgaben werden unter dem aktiven Benutzerkonto gestartet, mit dem Sie sich am System angemeldet haben.

Beispielsweise können beim Ausführen einer Untersuchungsaufgabe Zugriffsrechte für das zu untersuchende Objekt erforderlich sein. Dann können Sie diesen Dienst benutzen, um den Aufgabenstart unter dem Namen eines anderen Benutzerkontos zu starten, der über die erforderlichen Privilegien verfügt.

Das Programm-Update kann aus einer Quelle erfolgen, auf die Sie keinen Zugriff (beispielsweise ein Netzwerkverzeichnis für Updates) oder keine Rechte eines

autorisierten Proxyserverbenutzers besitzen. In diesem Fall können Sie den Dienst benutzen, um das Programm-Update unter dem Namen eines Benutzers mit entsprechender Berechtigung zu starten.

Um den Aufgabenstart unter einem anderen Benutzerkonto festzulegen,

1. Wählen Sie im Abschnitt **Virensuche** (für Untersuchungsaufgaben) oder **Service** (für Update-Aufgaben) des Hauptfensters den Namen der Aufgabe aus und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Aufgabe.
2. Klicken Sie im Konfigurationsfenster auf die Schaltfläche **Einstellungen** und gehen Sie im folgenden Fenster auf die Registerkarte **Erweitert** (s. Abb. 13).
3. Aktivieren Sie das Kontrollkästchen **Aufgabenstart mit anderem Benutzernamen**, um diesen Dienst einzuschalten. Geben Sie darunter das Benutzerkonto an, unter dem die Aufgabe gestartet werden soll: Benutzername und Kennwort.

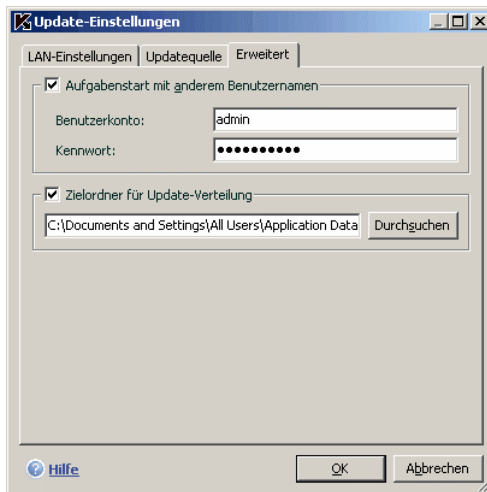


Abbildung 13. Einstellungen für den Start der Update-Aufgabe unter einem anderen Benutzerkonto

6.5. Konfiguration des Zeitplans für Aufgabenstart und Senden von Benachrichtigungen

Die Konfiguration des Zeitplans ist für Aufgaben zur Virensuche, für das Programm-Update und für das Senden von Benachrichtigungen über die Arbeit von Kaspersky Anti-Virus einheitlich.

Der Start der Aufgaben zur Virensuche, die bei der Programminstallation erstellt wurden, ist standardmäßig deaktiviert. Eine Ausnahme bildet die Untersuchungsaufgabe für Autostart-Objekte, die jedes Mal beim Start von Kaspersky Anti-Virus ausgeführt wird. Das Update wird in der Grundeinstellung automatisch ausgeführt, wenn auf den Kaspersky-Lab-Servern neue Updates vorhanden sind.

Sollten die Einstellungen für die Arbeit der Aufgaben nicht Ihren Anforderungen entsprechen, dann können Sie die Zeitplanparameter ändern. Wählen Sie dazu im Programmhauptfenster im Abschnitt **Virensuche** (für Untersuchungsaufgaben) oder im Abschnitt **Service** (für Update-Aufgaben und Aufgaben zur Update-Verteilung) den Namen der Aufgabe und öffnen Sie mit dem Link Einstellungen das entsprechende Konfigurationsfenster.

Um den zeitplangesteuerten Start einer Aufgabe anzuschalten, aktivieren Sie im Block **Startmodus** das Kontrollkästchen mit der Beschreibung der Bedingungen für den automatischen Aufgabenstart. Die Bedingungen für den Start der Untersuchungsaufgabe können im Fenster **Zeitplan** (s. Abb. Abbildung 14) angepasst werden, das durch Klick auf die Schaltfläche **Ändern** geöffnet wird.

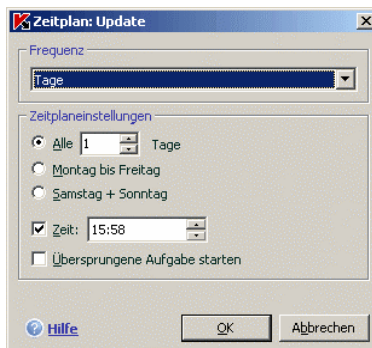


Abbildung 14. Erstellen eines Zeitplans für den Aufgabenstart

Bestimmen Sie zuerst die Frequenz, mit der das betreffende Ereignis (Start einer Aufgabe oder Senden einer Benachrichtigung) ausgeführt werden soll. Wählen Sie dazu im Block **Frequenz** (s. Abb. Abbildung 14) die gewünschte Variante. Geben Sie dann im Block **Zeitplaneinstellungen** die Parameter des Zeitplans für die gewählte Variante an. Folgende Varianten stehen zur Auswahl:

- **Einmal.** Start der Aufgabe oder das Senden einer Benachrichtigung erfolgt an dem angegebenen Tag zur festgelegten Uhrzeit.
- **Bei Programmstart.** Der Start der Aufgabe oder das Senden einer Benachrichtigung erfolgt jedes Mal, wenn Kaspersky Anti-Virus gestartet wird. Zusätzlich kann der Zeitraum nach dem Programmstart festgelegt werden, nach dessen Ablauf der Start ausgeführt werden soll.
- **Nach jedem Update.** Die Aufgabe wird jedes Mal nach dem Update der Bedrohungssignaturen gestartet (Dieser Punkt bezieht sich nur auf Untersuchungsaufgaben).
- **Minuten.** Das Zeitintervall zwischen den Aufgabenstarts oder dem Senden von Benachrichtigungen wird in Minuten festgelegt. Geben Sie in den Zeitplaneinstellungen den Wert für das Intervall in Minuten an. Als Höchstwert gelten 59 Minuten.
- **Stunden.** – Das Intervall zwischen den Aufgabenstarts oder dem Senden von Benachrichtigungen wird in Stunden festgelegt. Wenn Sie diese Frequenz gewählt haben, geben Sie in den Zeitplaneinstellungen das Intervall **Alle n Stunden** an und bestimmen Sie das Intervall *n*. Wählen Sie beispielsweise für den stündlichen Start *Alle 1 Stunden*.
- **Tag.** – Der Aufgabenstart oder das Senden von Benachrichtigungen wird im Abstand einer bestimmten Anzahl von Tagen gestartet. Geben Sie in den Zeitplanparametern den Wert für das Intervall an:
 - Wählen Sie die Variante **Alle n Tage** und geben Sie das Intervall *n* für die Anzahl der Tage an.
 - Wählen Sie die Variante **Montag bis Freitag**, wenn der Start täglich von Montag bis Freitag erfolgen soll.
 - Wählen Sie **Samstag + Sonntag**, damit der Start nur an Samstagen und Sonntagen erfolgt.

Geben Sie neben der Frequenz im Feld **Zeit** die Uhrzeit für den Start der Untersuchungsaufgabe an.
- **Wochen.** – Der Aufgabenstart oder das Senden von Benachrichtigungen erfolgt an bestimmten Wochentagen. Wenn Sie diese Frequenz gewählt haben, aktivieren Sie in den Zeitplaneinstellungen die Kontrollkästchen der Wochentage, an denen der Start ausgeführt werden soll. Geben Sie außerdem im Feld **Zeit** die Uhrzeit an.

- ☉ **Monate** – Der Aufgabenstart oder das Senden von Benachrichtigungen wird einmal monatlich zum festgelegten Zeitpunkt ausgeführt.

Wenn der Start aus einem bestimmten Grund nicht möglich war (wenn beispielsweise kein Mailprogramm installiert oder der Computer zum betreffenden Zeitpunkt ausgeschaltet war), können Sie festlegen, dass die übersprungene Aufgabe automatisch gestartet wird, sobald dies möglich ist. Aktivieren Sie dazu im Zeitplanfenster das Kontrollkästchen **Übersprungene Aufgabe starten**.

6.6. Leistungseinstellungen

Das Ausführen von Untersuchungsaufgaben erhöht die Belastung des Zentralprozessors und der Laufwerkssubsysteme und verlangsamt dadurch die Arbeit anderer Programme. In der Grundeinstellung hält die Anwendung beim Eintreten einer solchen Situation die Ausführung von Untersuchungsaufgaben an und gibt Systemressourcen für Benutzeranwendungen frei.

Allerdings existiert eine Reihe von Programmen, die gestartet werden, wenn Prozessorressourcen frei werden, und im Hintergrundmodus arbeiten. Damit die Virenuntersuchung unabhängig von der Arbeit solcher Programme erfolgt, aktivieren Sie das Kontrollkästchen **Ressourcen für andere Anwendungen freigeben** (s. Abb. Abbildung 15).

Beachten Sie, dass dieser Parameter für jede Untersuchungsaufgabe individuell angepasst werden kann. In diesem Fall besitzt der für eine konkrete Aufgabe festgelegte Parameter die höhere Priorität.

Im Fenster, das mit der Schaltfläche **Leistung** geöffnet wird, können Sie die Parameter von Kaspersky Anti-Virus für die Arbeit auf einem Multiprozessoren-Server anpassen (s. Pkt. 6.7 auf S. 72).

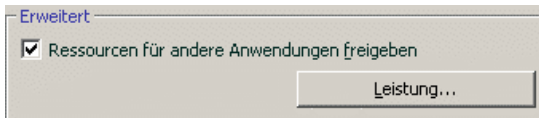


Abbildung 15. Leistungsoptionen

Um die Leistungsparameter anzupassen,

wählen Sie den Abschnitt **Schutz** des Anwendungshauptfensters aus und verwenden Sie den Link Einstellungen. Die Leistungsparameter werden im Block **Erweitert** angepasst.

6.7. Multiprozessoren-Konfiguration des Servers

In diesem Fenster können Sie die Leistungsparameter des Servers bei Verwendung einer Multiprozessoren-Konfiguration anpassen.

Die **Anzahl der Antivirenkernkopien** ist die Anzahl der Exemplare des Antivirenkerns, die beim Start von Kaspersky Anti-Virus auf dem Server geladen werden. Dieser Wert bestimmt die Anzahl der parallel laufenden Antiviren-Prozesse.

Je größer die Anzahl der gestarteten Antivirenkernkopien, desto schneller wird die Antiviren-Bearbeitung der Objekte ausgeführt. Allerdings wirkt sich dies auf die Gesamtleistungsfähigkeit des Servers aus.

Außerdem wird durch mehrere gleichzeitig laufende Antiviren-Prozesse erlaubt, den ununterbrochenen Serverschutz auch dann zu gewährleisten, wenn beispielsweise bei der Arbeit eines Kerns eine Störung auftritt.


Zur automatischen Verteilung der Antiviren-Prozesse auf die Serverprozessoren, aktivieren Sie das Kontrollkästchen **Speziellen Treiber zur Organisation der parallelen Bearbeitung verwenden.**

Wenn das Kontrollkästchen deaktiviert ist, können Sie die Belastung des Servers manuell regulieren. Ein Teil der Prozessoren kann für die Antiviren-Bearbeitung von Objekten, ein anderer Teil für die direkten Serveraufgaben reserviert werden. Deaktivieren Sie dazu im Block **Zu verwendende Prozessoren** die Kontrollkästchen der Prozessoren, die direkt für die Serveraufgaben reserviert werden sollen.

Die Kaspersky-Lab-Experten empfehlen, bei der Arbeit auf einem Multiprozessoren-Server mindestens einen Prozessor für die Serveraufgaben zu reservieren.

KAPITEL 7. VIRENSCHUTZ FÜR DAS DATEISYSTEM DES SERVERS

Kaspersky Anti-Virus verfügt über die Komponente *Datei-Anti-Virus*, die das Dateisystem des Servers vor einer Infektion schützt. Datei-Anti-Virus wird beim Start des Betriebssystems gestartet, befindet sich ständig im Arbeitsspeicher des Computers und untersucht alle Dateien, die geöffnet, gespeichert und gestartet werden.

Als Indikator für die Arbeit der Komponente dient das Symbol von Kaspersky Anti-Virus im Infobereich der Taskleiste, das jedes Mal bei der Untersuchung einer Datei folgendes Aussehen annimmt .

Standardmäßig untersucht Datei-Anti-Virus nur *neue* oder *veränderte* Dateien, d.h. Dateien, die seit dem letzten Zugriff hinzugefügt oder verändert worden sind.

1. Der Zugriff eines Benutzers oder eines bestimmten Programms auf eine beliebige Datei wird von der Komponente abgefangen.
2. Datei-Anti-Virus überprüft, ob die Datenbanken iChecker™ und iSwift™ Informationen über die abgefangene Datei enthalten. Auf Grundlage der ermittelten Informationen wird über die Notwendigkeit der Dateiuntersuchung entschieden.

Der Untersuchungsvorgang umfasst folgende Aktionen:

1. Die Datei wird auf das Vorhandensein von Viren untersucht. Schädliche Objekte werden auf Basis von *Bedrohungssignaturen* erkannt, die bei der Arbeit verwendet werden. Die Signaturen enthalten eine Beschreibung aller momentan bekannten Schadprogramme, Bedrohungen und entsprechende Desinfektionsmethoden.
2. Aufgrund der Analyseergebnisse bestehen folgende Varianten für das weitere Vorgehen der Anwendung:
 - a. Wenn in der Datei schädlicher Code gefunden wird, sperrt Datei-Anti-Virus die Datei, speichert eine Kopie im *Backup* und versucht, die Datei zu desinfizieren. Bei erfolgreicher Desinfektion wird die Datei zum Zugriff freigegeben. Wenn die Desinfektion fehlschlägt, wird die Datei gelöscht.
 - b. Wenn in der Datei ein Code gefunden wird, der Ähnlichkeit mit schädlichem Code besitzt, jedoch keine hundertprozentige

Sicherheit darüber besteht, wird die Datei in den Quarantäne-Speicher verschoben.

- c. Wenn in der Datei kein schädlicher Code gefunden wird, wird sie sofort zum Zugriff freigegeben.

7.1. Auswahl der Sicherheitsstufe für den Dateischutz

Datei-Anti-Virus bietet Schutz für die Dateien, mit denen Sie arbeiten. Dafür stehen folgende Sicherheitsstufen zur Auswahl (s. Abb. 16):

- **Hoch** – Auf dieser Stufe erfolgt die Kontrolle über Dateien, die geöffnet, gespeichert und gestartet werden, mit maximaler Ausführlichkeit.
- **Empfohlen**. Die Parameter dieser Stufe werden von Kaspersky-Lab-Experten empfohlen und umfassen die Untersuchung folgender Objektkategorien:
 - Programme und Objekte nach ihrem Inhalt
 - nur neue und seit der letzten Objektuntersuchung veränderte Objekte
 - eingebettete OLE-Objekte
- **Niedrig** – Diese Stufe erlaubt Ihnen, komfortabel mit Anwendungen zu arbeiten, die den Arbeitsspeicher stark beanspruchen, weil die Auswahl der untersuchten Dateien auf dieser Stufe eingeschränkt wird.

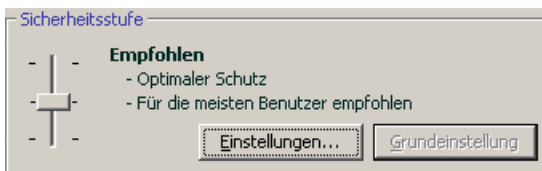


Abbildung 16. Sicherheitsstufe von Datei-Anti-Virus

Der Dateischutz erfolgt standardmäßig auf der **Empfohlenen** Stufe.

Sie können die Schutzstufe für Dateien, mit denen Sie arbeiten, erhöhen oder senken, indem Sie eine andere Stufe wählen oder die Einstellungen der aktuellen Stufe ändern.

Um die Sicherheitsstufe zu ändern,

verschieben Sie den Zeiger auf der Skala. Durch das Anpassen der Sicherheitsstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Dateien bestimmt: Je weniger Dateien der Virusanalyse unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit.

Wenn keine der vordefinierten Stufen für den Dateischutz Ihren Anforderungen entspricht, können Sie die Schutzparameter zusätzlich anpassen. Wählen Sie dazu die Stufe, die Ihren Anforderungen am nächsten kommt, als Ausgangsstufe und ändern Sie ihre Parameter entsprechend. In diesem Fall ändert sich die Stufe in **Benutzerdefiniert**. Betrachten wir ein Beispiel, in dem die benutzerdefinierte Sicherheitsstufe für den Dateischutz nützlich sein kann.

Beispiel:

Aufgrund von Besonderheiten Ihrer Tätigkeit arbeiten Sie mit einer großen Menge von Dateien unterschiedlicher Typen, darunter auch relativ umfangreiche Dateien. Sie möchten es nicht riskieren, Dateien entsprechend der Namenserverlängerung oder Größe von der Untersuchung auszuschließen, selbst wenn dadurch die Leistungsfähigkeit Ihres Computers beeinflusst wird.

Empfehlung zur Auswahl der Stufe:

Die Analyse der Situation lässt darauf schließen, dass die Infektionsgefahr durch ein Schadprogramm im beschriebenen Beispiel sehr groß ist. Größe und Typ von bei der Arbeit verwendeten Dateien sind sehr vielfältig, weshalb das Festlegen solcher Ausnahmen ein Risiko für die Daten auf dem Computer darstellt. Ein wichtiger Aspekt der Untersuchung besteht in der Analyse von bei der Arbeit verwendeten Dateien nach ihrem Inhalt und nicht nach der Erweiterung.

Es wird empfohlen, die vordefinierte Schutzstufe **Empfohlen** folgendermaßen anzupassen: Die Größenbeschränkung für zu untersuchende Dateien wird deaktiviert. Die Arbeit von Datei-Anti-Virus wird dadurch optimiert, dass nur neue und veränderte Dateien untersucht werden. Dadurch wird die Belastung des Computers bei der Dateiuntersuchung gesenkt, was die komfortable Arbeit mit anderen Anwendungen erlaubt.

Um die Einstellungen der aktuellen Sicherheitsstufe anzupassen,

klicken Sie im Konfigurationsfenster von Datei-Anti-Virus auf die Schaltfläche **Einstellungen**, passen Sie im folgenden Fenster die Einstellungen für den Dateischutz an und klicken Sie auf **OK**.

Dadurch wird eine vierte Sicherheitsstufe mit der Bezeichnung **Benutzerdefiniert** erstellt, welche die von Ihnen definierten Schutzparameter enthält.

7.2. Konfiguration des Dateischutzes

Die Einstellungen, nach denen der Dateischutz auf Ihrem Computer erfolgt, lassen sich in folgende Gruppen aufteilen:

- Parameter, welche die Typen der Dateien festlegen, die der Virusanalyse unterzogen werden (s. Pkt. 7.2.1 auf S. 76).
- Parameter, die den geschützten Bereich festlegen (s. Pkt. 7.2.2 auf S. 79).
- Parameter, welche die Aktion für ein gefährliches Objekt festlegen (s. Pkt. 7.2.5 auf S. 83).
- zusätzliche Parameter für die Arbeit von Datei-Anti-Virus (s. Pkt. 7.2.3 auf S. 80).

In diesem Abschnitt des Handbuchs werden alle oben genannten Gruppen ausführlich beschrieben.

7.2.1. Festlegen der Typen von zu untersuchenden Dateien

Durch die Angabe des Typs der zu untersuchenden Dateien definieren Sie das Format, die Größe und die Laufwerke der Dateien, die beim Öffnen, Ausführen und Speichern auf Viren untersucht werden sollen.

Zur Vereinfachung der Konfiguration werden alle Dateien in zwei Gruppen eingeteilt: *einfache* und *zusammengesetzte*. Einfache Dateien enthalten kein anderes Objekt (z.B. eine txt-Datei). Zusammengesetzte Objekte können mehrere Objekte umfassen, die wiederum jeweils mehrere Anhänge enthalten können. Hierfür gibt es viele Beispiele: Archive, Dateien, die Makros, Tabellen, Nachrichten mit Anlagen usw. enthalten.

Der Dateityp für die Virusanalyse wird im Abschnitt **Dateitypen** (s. Abb. 17) festgelegt. Wählen Sie eine der drei Varianten:

- **Alle Dateien untersuchen.** In diesem Fall werden alle Objekte des Dateisystems, die geöffnet, gestartet und gespeichert werden ohne Ausnahmen der Analyse unterzogen.
- **Programme und Dokumente (nach Inhalt) untersuchen.** Bei der Auswahl dieser Dateigruppe untersucht Datei-Anti-Virus nur potentiell infizierbare Dateien, d.h. Dateien, in die ein Virus eindringen kann.

Hinweis.

Es gibt eine Reihe von Dateiformaten, für die das Risiko des Eindringens von schädlichem Code und der späteren Aktivierung relativ gering ist. Dazu zählen beispielsweise Dateien im *txt*-Format.

Im Gegensatz dazu gibt es Dateiformate, die ausführbaren Code enthalten oder enthalten können. Als Beispiele für solche Objekte dienen die Dateien der Formate *exe*, *dll*, *doc*. Das Risiko des Eindringens und der Aktivierung von schädlichem Code in solche Dateien ist relativ hoch.

Bevor die Virensuche in einer Datei beginnt, wird die interne Kopfzeile der Datei hinsichtlich des Dateiformats untersucht (*txt*, *doc*, *exe* usw.). Wenn sich aufgrund der Analyse ergibt, dass eine Datei dieses Formats nicht infiziert werden kann, dann wird sie nicht auf Viren untersucht und sofort für den Zugriff freigegeben. Besteht aber aufgrund des Dateiformats für einen Virus die Möglichkeit des Eindringens, dann wird die Datei auf Viren untersucht.

- ☉ **Programme und Dokumente (nach Erweiterung) untersuchen.** In diesem Fall untersucht Datei-Anti-Virus nur potentiell infizierbare Dateien, wobei das Format auf Basis der Dateinamenserweiterung ermittelt wird. Wenn Sie dem Link [Erweiterung](#) folgen, gelangen Sie zu einer Liste der Dateierweiterungen (s. Anhang A.1 auf S. 194), die in diesem Fall untersucht werden.

Hinweis.

Es sollte beachtet werden, dass ein Angreifer einen Virus in einer Datei mit der Erweiterung *txt* an Ihren Computer senden kann, obwohl es sich in Wirklichkeit um eine ausführbare Datei handelt, die in eine *txt*-Datei umbenannt wurde. Wenn Sie die Variante ☉ **Programme und Dokumente (nach Erweiterung) untersuchen** wählen, wird eine solche Datei bei der Untersuchung übersprungen. Wenn Sie die Variante ☉ **Programme und Dokumente (nach Inhalt) untersuchen** gewählt haben, analysiert Datei-Anti-Virus ungeachtet der Erweiterung die Kopfzeile der Datei, wodurch sich ergibt, dass die Datei das Format *exe* besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

Im Abschnitt **Optimierung** lässt sich festlegen, dass nur Dateien untersucht werden sollen, die neu sind oder seit ihrer letzten Untersuchung verändert wurden. Dieser Modus erlaubt es, die Untersuchungszeit wesentlich zu verkürzen und die Arbeitsgeschwindigkeit des Programms zu erhöhen. Aktivieren Sie dazu das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**. Dieser Modus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

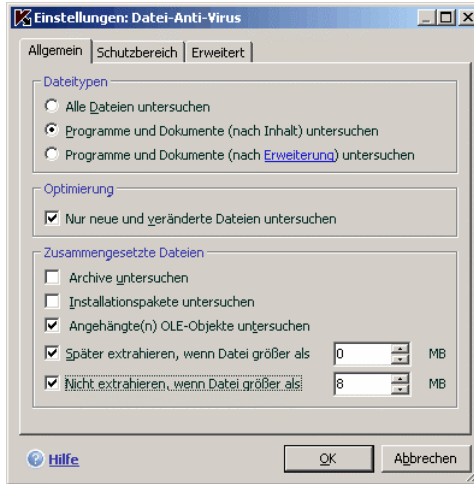


Abbildung 17. Auswahl der Dateitypen, die der Virenuntersuchung unterzogen werden sollen

Geben Sie im Abschnitt **Zusammengesetzte Dateien** an, welche zusammengesetzten Dateien auf Viren untersucht werden sollen:

- Alle/Nur neue Archive untersuchen** – Archive der Formate ZIP, CAB, RAR, ARJ untersuchen.
- Alle/Nur neue Installationspakete untersuchen** – selbstextrahierende Archive auf Viren untersuchen.
- Alle/Nur neue angehängte(n) OLE-Objekte untersuchen** – Objekte, die in eine Datei eingebettet sind, untersuchen (z.B. eine Excel-Tabelle oder ein Makro, das in eine Datei des Typs Microsoft Office Word eingebettet ist, Anhänge von E-Mail-Nachrichten, usw.).

Für jeden Typ einer zusammengesetzten Datei können sie wählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie dazu den Link neben der Bezeichnung des Objekts. Der Link verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn im Abschnitt **Optimierung** festgelegt wurde, dass nur neue und veränderte Dateien untersucht werden sollen, steht die Auswahl des Typs der zusammengesetzten Dateien nicht zur Verfügung.

Um festzulegen, welche zusammengesetzten Dateien nicht auf Viren untersucht werden sollen, verwenden Sie folgende Parameter:

- Später extrahieren, wenn Datei größer als ... MB.** Wenn die Größe eines zusammengesetzten Objekts diesen Wert überschreitet, wird es vom Programm wie ein einzelnes Objekt untersucht (Kopfzeile wird analysiert)

und zur Arbeit freigegeben. Die Untersuchung der Objekte, die dazu gehören, erfolgt später. Wenn dieses Kontrollkästchen nicht aktiviert ist, wird der Zugriff auf Dateien, die über der angegebenen Größe liegen, bis zum Abschluss der Objektuntersuchung blockiert.

- Nicht extrahieren, wenn Datei größer als ... MB.** In diesem Fall wird eine Datei mit der angegebenen Größe bei der Virenuntersuchung übersprungen.

7.2.2. Festlegen des Schutzbereichs

Datei-Anti-Virus untersucht standardmäßig alle Dateien, auf die zugegriffen wird, unabhängig davon, auf welchem Datenträger sie sich befinden (Festplatte, CD/DVD-ROM, Flash-Card).

Sie können den Schutzbereich folgendermaßen einschränken:

1. Wählen Sie im Hauptfenster **Datei-Anti-Virus** und wechseln Sie über den Link Einstellungen zum Konfigurationsfenster der Komponente.
2. Klicken Sie auf die Schaltfläche **Einstellungen** und wählen Sie im folgenden Fenster die Registerkarte **Schutzbereich** (s. Abb. 18).

Auf der Registerkarte befindet sich eine Liste der Objekte, die der Untersuchung durch Datei-Anti-Virus unterliegen. Standardmäßig ist der Schutz aller Objekte aktiviert, die sich auf Festplatten, Wechseldatenträgern und Netzwerklaufwerken befinden, die an Ihren Computer angeschlossen sind. Sie können die Liste mit Hilfe der Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** ergänzen oder anpassen.

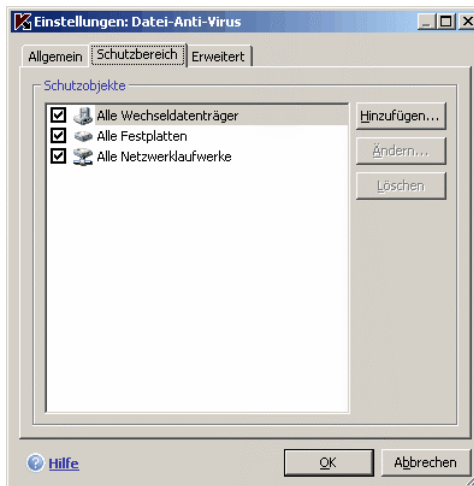


Abbildung 18. Festlegen des Schutzbereichs

Wenn Sie den Bereich der zu schützenden Objekte einschränken möchten, können Sie folgendermaßen vorgehen:

- Nur die Verzeichnisse, Laufwerke oder Dateien angeben, die geschützt werden sollen.
- Eine Liste der Objekte anlegen, die nicht geschützt werden sollen (s. Pkt. 6.3 auf S. 60).
- Die erste und zweite Methode vereinigen, d.h. einen Schutzbereich erstellen, aus dem bestimmte Objekte ausgeschlossen werden.

Beim Hinzufügen eines Untersuchungsobjekts können Masken verwendet werden. Beachten Sie, dass Masken nur mit den absoluten Pfaden der Objekte angegeben werden dürfen:

- **C:\dir\.*** oder **C:\dir*** oder **C:\dir** – alle Dateien im Ordner *C:\dir*
- **C:\dir*.exe** – alle Dateien mit der Endung *.exe* im Ordner *C:\dir*
- **C:\dir*.ex?** – alle Dateien mit der Endung *.ex?* im Ordner *C:\dir*, wobei anstelle von *?* ein beliebiges Zeichen stehen kann.
- **C:\dir\test** – nur die Datei *C:\dir\test*
- Damit die rekursive Untersuchung des gewählten Objekts ausgeführt wird, aktivieren Sie das Kontrollkästchen **Untereordner einschließen**.

Achtung.

Beachten Sie, dass Datei-Anti-Virus nur jene Dateien auf Viren untersucht, die zu dem erstellten Schutzbereich gehören. Dateien, die nicht in diesen Bereich fallen, werden ohne Untersuchung zur Arbeit freigegeben. Dadurch steigt das Risiko einer Infektion Ihres Computers!

7.2.3. Anpassen zusätzlicher Parameter

Als zusätzliche Parameter für Datei-Anti-Virus können Sie den Untersuchungsmodus für die Objekte des Dateisystems festlegen und bestimmen, unter welchen Bedingungen die Arbeit der Komponente vorübergehend angehalten werden soll.

Um die zusätzlichen Parameter von Datei-Anti-Virus anzupassen:

1. Wählen Sie im Hauptfenster die Komponente **Datei-Anti-Virus** aus und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Komponente.

2. Klicken Sie auf die Schaltfläche **Einstellungen** und wählen Sie im folgenden Fenster die Registerkarte **Erweitert** (s. Abb. 19).

Durch den Untersuchungsmodus für Objekte werden die Bedingungen für die Reaktion von Datei-Anti-Virus bestimmt. Folgende Varianten stehen zur Auswahl:

- **Intelligenter Modus.** Dieser Modus dient dazu, die Objektbearbeitung und die Verfügbarkeit von Objekten für den Benutzer zu beschleunigen. Bei der Auswahl dieser Variante wird aufgrund der Analyse der Operationen, die mit einem Objekt ausgeführt werden sollen, über die Untersuchung entschieden.

Bei der Arbeit mit einem Microsoft Office-Dokument untersucht Kaspersky Anti-Virus die Datei, wenn sie zum ersten Mal geöffnet und zum letzten Mal geschlossen wird. Alle dazwischen liegenden Operationen, bei denen die Datei verändert wird, werden von der Untersuchung ausgeschlossen.

Der intelligente Untersuchungsmodus wird standardmäßig verwendet.

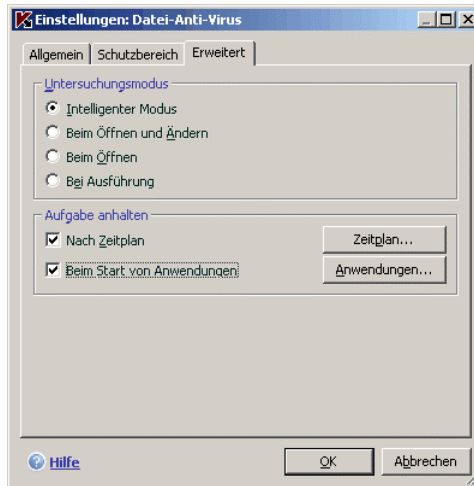


Abbildung 19. Anpassen der zusätzlichen Parameter für Datei-Anti-Virus

- **Beim Öffnen und Ändern** – Datei-Anti-Virus untersucht Objekte, wenn sie geöffnet und verändert werden.
- **Beim Öffnen** – Objekte werden nur untersucht, wenn versucht wird, sie zu öffnen.
- **Bei Ausführung** – Objekte werden nur in dem Moment untersucht, wenn versucht wird, sie zu starten.

Das vorübergehende Anhalten von Datei-Anti-Virus kann erforderlich sein, wenn Arbeiten ausgeführt werden, die die Betriebssystemressourcen stark beanspruchen. Um die Belastung zu verringern und den schnellen Zugriff des Benutzers auf Objekte zu gewährleisten, wird empfohlen, das Abschalten der Komponente für einen bestimmten Zeitraum oder bei der Arbeit mit bestimmten Programmen festzulegen.

Damit die Arbeit der Komponente für einen bestimmten Zeitraum angehalten wird, aktivieren Sie das Kontrollkästchen **Nach Zeitplan** und legen Sie im Fenster (s. Abb. Abbildung 9), das mit der Schaltfläche **Zeitplan** geöffnet wird, den Zeitraum fest, für den die Arbeit der Komponente angehalten und nach dem sie fortgesetzt werden soll. Geben Sie in den entsprechenden Feldern die Werte im Format HH:MM ein.

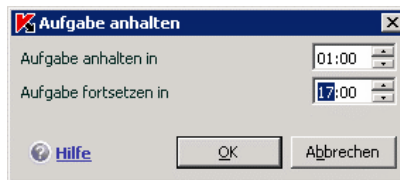


Abbildung 20. Die Arbeit der Komponente anhalten

Damit die Arbeit der Komponente bei der Arbeit mit ressourcenaufwändigen Programmen angehalten wird, aktivieren Sie das Kontrollkästchen **Beim Start von Anwendungen** und legen Sie im Fenster (s. Abb. 21), das mit der Schaltfläche **Liste** geöffnet wird, die Liste der Programme an.

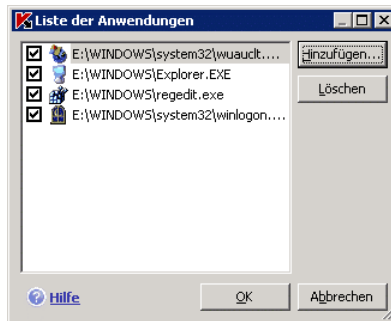


Abbildung 21. Liste der Anwendungen erstellen

Verwenden Sie die Schaltfläche **Hinzufügen**, um der Liste eine Anwendung hinzuzufügen. Dadurch wird das Kontextmenü geöffnet. Wechseln Sie entweder mit dem Punkt **Durchsuchen** in das Standardfenster zur Dateiauswahl und geben Sie die ausführbare Datei der betreffenden Anwendung an oder verwenden Sie den Punkt **Anwendungen**, um zur Liste der momentan aktiven

Anwendungen zu gelangen, und wählen Sie dort die gewünschte Anwendung aus.

Um eine Anwendung aus der Liste zu löschen, wählen Sie sie in der Liste aus und klicken Sie auf die Schaltfläche **Löschen**.

Um die Bedingung für das Anhalten von Datei-Anti-Virus bei der Arbeit einer konkreten Anwendung vorübergehend aufzuheben, ist es ausreichend, das Kontrollkästchen neben dem Namen der Anwendung zu deaktivieren, ohne diese aus der Liste zu löschen.

7.2.4. Wiederherstellen der Standardparameter für den Dateischutz

Während Sie die Arbeit von Datei-Anti-Virus konfigurieren, können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Um die standardmäßigen Einstellungen für den Dateischutz wiederherzustellen,

1. Wählen Sie im Hauptfenster die Komponente **Datei-Anti-Virus** und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Komponente.
2. Klicken Sie im Abschnitt **Sicherheitsstufe** auf die Schaltfläche **Grundeinstellung**.

Wenn Sie bei der Konfiguration von Datei-Anti-Virus die Liste der Objekte verändert haben, die zum Schutzbereich gehören, dann wird Ihnen beim Wiederherstellen der ursprünglichen Einstellungen vorgeschlagen, diese Liste zur späteren Verwendung beizubehalten. Um die Liste der Objekte zu speichern, aktivieren Sie im folgenden Fenster **Einstellungen wiederherstellen** das Kontrollkästchen **Schutzbereich**.

7.2.5. Auswahl der Aktion für Objekte

Wenn sich durch die Virenuntersuchung einer Datei herausstellt, dass sie infiziert oder einer Infektion verdächtig ist, hängen die weiteren Operationen von Datei-Anti-Virus vom Status des Objekts und der ausgewählten Aktion ab.

Datei-Anti-Virus kann einem Objekt aufgrund der Untersuchung einen der folgenden Status zuweisen:

- Status eines der schädlichen Programme (beispielsweise *Virus, trojanisches Programm*) (s. Pkt. 1.1 auf S. 7).
- *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Das bedeutet, dass in der Datei die Codefolge eines unbekanntes Virus oder der modifizierte Code eines bekannten Virus gefunden wurde.

Standardmäßig werden alle infizierten Dateien der Desinfektion unterzogen. Alle möglicherweise infizierten Dateien werden in die Quarantäne verschoben.

Um die Aktion für ein Objekt zu ändern,

wählen Sie im Hauptfenster **Datei-Anti-Virus** und wechseln Sie über den Link Einstellungen in das Konfigurationsfenster der Komponente. Alle verfügbaren Aktionen sind im entsprechenden Abschnitt angegeben (s. Abb. 22).

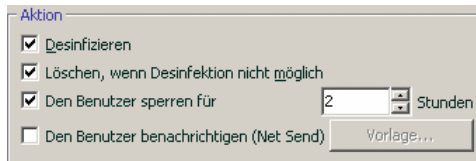


Abbildung 22. Mögliche Aktionen von Datei-Anti-Virus für ein gefährliches Objekt

Gewählte Aktion	Was geschieht beim Fund eines gefährlichen Objekts?
<input checked="" type="checkbox"/> Desinfizieren <input type="checkbox"/> Löschen, wenn Desinfektion nicht möglich	<p>Der Zugriff auf das Objekt wird gesperrt und es erfolgt ein Desinfektionsversuch, wobei eine Kopie des Objekts im Backup gespeichert wird. Bei erfolgreicher Desinfektion wird das Objekt für den Benutzer zur Arbeit freigegeben. Kann das Objekt nicht desinfiziert werden, wird es in die Quarantäne verschoben. Informationen darüber werden im Bericht aufgezeichnet. Später kann versucht werden, das Objekt zu desinfizieren.</p>

Gewählte Aktion	Was geschieht beim Fund eines gefährlichen Objekts?
<input checked="" type="checkbox"/> Desinfizieren <input checked="" type="checkbox"/> Löschen, wenn Desinfektion nicht möglich	<p>Der Zugriff auf das Objekt wird gesperrt und es erfolgt ein Desinfektionsversuch, wobei eine Kopie des Objekts im Backup gespeichert wird. Bei erfolgreicher Desinfektion wird das Objekt für den Benutzer zur Arbeit freigegeben. Kann das Objekt nicht desinfiziert werden, wird es gelöscht.</p>
<input type="checkbox"/> Desinfizieren <input checked="" type="checkbox"/> Löschen	<p>Datei-Anti-Virus blockiert den Zugriff auf das Objekt und löscht es.</p>
<input checked="" type="checkbox"/> Den Benutzer sperren für ... Stunden	<p>Wenn versucht wird, ein infiziertes oder möglicherweise infiziertes Objekt zu kopieren, wird die aktive Verbindung des betreffenden Benutzerkontos mit dem Server blockiert.</p> <p>Diese Aktion kann zusätzlich zu den Aktionen angewandt werden, die mit der Objektbearbeitung verbunden sind (Desinfektion oder Löschen).</p> <p>Wenn der Benutzer seine Sitzung beendet und sich erneut beim System anmeldet, wird dies von Kaspersky Anti-Virus als eine andere Verbindung gewertet und die Blockade wird aufgehoben.</p>
<input checked="" type="checkbox"/> Benutzer benachrichtigen (Net Send)	<p>Der Benutzer, von dessen Computer versucht wurde, ein infiziertes oder möglicherweise infiziertes Objekt auf den Server zu kopieren, wird über Net Send benachrichtigt.</p> <p>Verwenden Sie zum Anpassen der Benachrichtigungsvorlage die Schaltfläche Vorlage (s. Pkt. 7.2.6 auf S. 86).</p>

Bevor ein Desinfektionsversuch erfolgt oder das Objekt gelöscht wird, legt Kaspersky Anti-Virus eine Sicherungskopie des Objekts an und speichert diese im Backup. Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

Achtung! Wenn die Anwendung auf einem Computer mit dem Betriebssystem Microsoft Windows NT Server 4.0 installiert ist, stehen die Aktionen **Benutzer sperren** und **Benutzer benachrichtigen (NetSend)** nicht zur Verfügung.

7.2.6. Benachrichtigungsvorlage anpassen

In diesem Fenster können Sie den Vorlagentext für die Benachrichtigung an den Benutzer anpassen, von dessen Computer versucht wurde, ein infiziertes / möglicherweise infiziertes Objekt auf den Server zu kopieren.

Um den Informationsgehalt des Benachrichtigungstexts zu erhöhen, kann er Makros enthalten: Pfad des gefährlichen Objekts und Name der Bedrohung. Verwenden Sie die Schaltfläche **Makros**, um Makros in den Benachrichtigungstext einzufügen.

Verwenden Sie die Schaltfläche **Standard**, um den Text wiederherzustellen, der standardmäßig als Benachrichtigungsvorlage dient.

7.3. Aufgeschobene Desinfektion von Objekten

In Kaspersky Anti-Virus for Windows Servers wird der Zugriff auf infizierte Objekte gesperrt, wenn die Desinfektion fehlschlägt oder wenn das Objekt gelöscht wird.

Um erneut Zugriff auf blockierte Objekte zu erhalten, müssen diese vorher desinfiziert werden. Dazu:

1. Wählen Sie im Programmhauptfenster die Komponente **Datei-Anti-Virus** und klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks **Statistik**.
2. Wählen Sie auf der Registerkarte **Gefunden** die gewünschten Objekte und klicken Sie auf die Schaltfläche **Aktionen** → **Alle desinfizieren**.

Wenn die Desinfektion des Objekts gelingt, wird der Zugriff darauf freigegeben. Kann das Objekt nicht desinfiziert werden, dann wird Ihnen zur Auswahl angeboten, es zu *löschen* oder zu *überspringen*. Beim Überspringen wird die Datei für den Zugriff freigegeben. Allerdings erhöht sich dadurch das Risiko einer

Infektion Ihres Computers erheblich. Es wird ausdrücklich davor gewarnt, schädliche Objekte zu überspringen.

KAPITEL 8. VIRENSUCHE AUF DEM SERVER

Kaspersky Anti-Virus 6.0 for Windows Servers erlaubt es, sowohl einzelne Objekte (Dateien, Ordner, Laufwerke, Wechseldatenträger) als auch den gesamten Computer auf das Vorhandensein von Viren zu untersuchen. Durch die Virensuche lässt sich die Möglichkeit der Ausbreitung eines schädlichen Codes verhindern, der von Datei-Anti-Virus aus bestimmten Gründen nicht erkannt wurde.

Kaspersky Anti-Virus 6.0 verfügt über folgende standardmäßigen Untersuchungsaufgaben:

Kritische Bereiche

Virenuntersuchung aller kritischen Computerbereiche sowie Virenuntersuchung aller Objekte, die am Systemstart beteiligt sind. Dazu gehören: Systemspeicher, Objekte, die beim Systemstart gestartet werden, Laufwerksbootsektoren und *Windows*-Systemverzeichnisse. Das Ziel dieser Aufgabe besteht im schnellen Auffinden von im System aktiven Viren, ohne dazu die vollständige Untersuchung des Computers zu starten.

Arbeitsplatz

Virensuche auf Ihrem Computer mit sorgfältiger Untersuchung aller angeschlossenen Laufwerke, des Arbeitsspeichers und der Dateien.

Autostart-Objekte

Virenuntersuchung der Objekte, die beim Start des Betriebssystems geladen werden.

Diese Aufgaben werden standardmäßig mit den empfohlenen Schutzeinstellungen ausgeführt. Sie können diese Einstellungen ändern (s. Pkt. 8.4 auf S. 92) und einen Zeitplan für den Aufgabenstart festlegen (s. Pkt. 6.5 auf S. 69).

Außerdem besteht die Möglichkeit, eigene Aufgaben zur Virensuche zu erstellen (s. Pkt. 8.3 auf S. 91) und einen Startzeitplan dafür anzulegen. Es kann beispielsweise eine Aufgabe zur wöchentlichen Untersuchung von Mail-Datenbanken oder eine Aufgabe zur Virensuche in einem bestimmten Ordner erstellt werden.

Daneben können Sie ein beliebiges Objekt auf Viren untersuchen, ohne dafür eine spezielle Untersuchungsaufgabe zu erstellen. Das zu untersuchende Objekt


kann aus dem Interface von Kaspersky Anti-Virus 6.0 oder mit den Standardmitteln von Microsoft Windows Server (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) ausgewählt werden.

Eine vollständige Liste der Aufgaben zur Virensuche, die für Ihren Computer erstellt wurden, kann im Abschnitt **Virensuche** auf der linken Seite des Programmhauptfensters angezeigt werden.

8.1. Steuerung von Aufgaben zur Virensuche


Der Start von Aufgaben zur Virensuche erfolgt entweder manuell oder automatisch nach einem festgelegten Zeitplan (s. Pkt. 6.5 auf S. 69).

Um eine Untersuchungsaufgabe manuell zu starten,


wählen Sie im Abschnitt **Virensuche** des Programmhauptfensters den Aufgabennamen und klicken Sie in der Statuszeile auf die Schaltfläche .

Aufgaben, die momentan ausgeführt werden (einschließlich Aufgaben, die über Kaspersky Administration Kit erstellt wurden), werden im Kontextmenü angezeigt, das durch Rechtsklick auf das Symbol der Anwendung in der Taskleiste geöffnet wird.

Um eine Untersuchungsaufgabe anzuhalten,

klicken Sie in der Statuszeile auf die Schaltfläche . Dabei ändert sich der Status der Aufgabenausführung in *Pause*. Die Untersuchung wird angehalten, bis die Aufgabe manuell oder nach Zeitplan erneut gestartet wird.

Um eine Untersuchungsaufgabe zu beenden,

klicken Sie in der Statuszeile auf die Schaltfläche . Der Status der Aufgabenausführung ändert sich in *abgebrochen*. Die Untersuchung wird angehalten, bis die Aufgabe manuell oder nach Zeitplan erneut gestartet wird. Beim folgenden Start der Aufgabe wird Ihnen vorgeschlagen, die abgebrochene Untersuchung fortzusetzen oder erneut zu beginnen.

8.2. Erstellen einer Liste der Untersuchungsobjekte

Um eine Liste der Objekte anzuzeigen, die bei der Ausführung dieser Aufgabe untersucht werden, wählen Sie im Abschnitt **Virensuche** des Programmhauptfensters den Namen einer Aufgabe (z.B. **Arbeitsplatz**). Die Liste

der Objekte wird auf der rechten Seite des Fensters unter der Statuszeile angezeigt (s. Abb. 23).



Abbildung 23. Liste der Untersuchungsobjekte

Für Aufgaben, die standardmäßig bei der Programminstallation erstellt wurden, besteht bereits eine Liste der zu untersuchenden Objekte. Beim Erstellen eigener Aufgaben oder bei der Auswahl eines Objekts im Rahmen einer Aufgabe zur Virenuntersuchung eines separaten Objekts erstellen Sie die Liste der Objekte selbst.

Zum Ergänzen und Ändern der Liste der Untersuchungsobjekte dienen die Schaltflächen, die rechts von der Liste angebracht sind. Klicken Sie auf die Schaltfläche **Hinzufügen**, um der Liste ein neues Untersuchungsobjekt hinzuzufügen und geben Sie im folgenden Fenster das Untersuchungsobjekt an.

Aus Gründen der Bedienungsfreundlichkeit können dem Untersuchungsbereich solche Kategorien wie Mailboxen des Benutzers, Systemspeicher, Autostart-Objekte, Sicherungsdateien des Betriebssystems, und Objekte, die sich im Quarantäneordner von Kaspersky Anti-Virus befinden, hinzugefügt werden.

Außerdem kann beim Hinzufügen eines Ordners, der untergeordnete Objekte enthält, die Option zur rekursiven Untersuchung geändert werden. Wählen Sie das Objekt dazu in der Liste der Untersuchungsobjekte aus, öffnen Sie das Kontextmenü und verwenden Sie den Befehl **Unterordner einschließen**.

Um ein Objekt zu löschen, markieren Sie es in der Liste (dabei wird der Objektname durch grauen Hintergrund hervorgehoben) und klicken Sie auf die Schaltfläche **Löschen**. Sie können die Untersuchung einzelner Objekte bei der Ausführung einer bestimmten Aufgabe vorübergehend abschalten, ohne die Objekte aus der Liste zu löschen. Deaktivieren Sie dazu einfach das Kontrollkästchen neben dem Objekt, das nicht untersucht werden soll.

Klicken Sie zum Starten der Untersuchungsaufgabe auf die Schaltfläche **Virensuche** oder wählen Sie im Menü, das durch Klick auf die Schaltfläche **Aktionen** geöffnet wird, den Punkt **Start**.

Außerdem können Sie ein Untersuchungsobjekt mit den Standardmitteln von Microsoft Windows Server (beispielsweise im Fenster des Programms **Explorer** oder auf dem **Arbeitsplatz** usw.) auswählen (s. Abb. 24). Führen Sie dazu den Mauszeiger auf den Namen des gewünschten Objekts, öffnen Sie mit der rechten Maustaste das Microsoft Windows Server-Kontextmenü und wählen Sie den Punkt **Auf Viren untersuchen**.



Abbildung 24. Untersuchung eines Objekts aus dem Kontextmenü von Microsoft Windows

8.3. Erstellen von Aufgaben zur Virensuche

Zur Virenuntersuchung von Objekten Ihres Computers können Sie die vordefinierten Untersuchungsaufgaben verwenden, die zum Lieferumfang des Programms gehören, sowie eigene Aufgaben erstellen. Eine neue Aufgabe wird auf der Basis von bereits vorhandenen Untersuchungsaufgaben erstellt.

Um eine neue Untersuchungsaufgabe zu erstellen,

1. Wählen Sie im Abschnitt **Virensuche** des Programmhauptfensters die Aufgabe, deren Parameter Ihren Anforderungen am nächsten kommen.
2. Öffnen Sie durch Rechtsklick das Kontextmenü oder klicken Sie auf die Schaltfläche **Aktionen**, die sich rechts neben der Liste der Untersuchungsobjekte befindet, und wählen Sie den Punkt **Speichern unter**.
3. Geben Sie im folgenden Fenster den Namen der neuen Aufgabe an und klicken Sie auf die Schaltfläche **OK**. Danach erscheint die Aufgabe mit dem festgelegten Namen in der Aufgabenliste des Abschnitts **Virensuche** im Programmhauptfenster.

Achtung.

Die maximale Anzahl der Aufgaben, die vom Benutzer in der Anwendung erstellt werden können, ist auf vier beschränkt.

Eine neu erstellte Aufgabe erbt alle Parameter der Aufgabe, auf deren Basis sie erstellt wurde. Deshalb ist die zusätzliche Konfiguration erforderlich: Erstellen Sie eine Liste der Untersuchungsobjekte (s. Pkt. 8.2 auf S. 89), legen Sie die Parameter fest (s. Pkt. 8.4 auf S. 92), mit denen die Aufgabe ausgeführt werden soll, und erstellen Sie den Zeitplan (s. Pkt. 6.5 auf S. 69) für den automatischen Start.

Um eine erstellte Aufgabe umzubenennen,

wählen Sie die Aufgabe im Abschnitt **Virensuche** des Programmhauptfensters, öffnen Sie durch Rechtsklick das Kontextmenü oder klicken Sie auf die Schaltfläche **Aktionen**, die sich rechts neben der Liste der Untersuchungsobjekte befindet, und wählen Sie den Punkt **Umbenennen**.

Geben Sie im folgenden Fenster den neuen Namen für die Aufgabe an und klicken Sie auf die Schaltfläche **OK**. Dadurch wird der Aufgabenname im Abschnitt **Virensuche** geändert.

Um eine erstellte Aufgabe zu löschen,

wählen Sie die Aufgabe im Abschnitt **Virensuche** des Programmhauptfensters, öffnen Sie durch Rechtsklick das Kontextmenü oder klicken Sie auf die Schaltfläche **Aktionen**, die sich rechts neben der Liste der Untersuchungsobjekte befindet, und wählen Sie den Punkt **Löschen**.

Bestätigen Sie im Bestätigungsfenster, dass die Aufgabe gelöscht werden soll. Dadurch wird die Aufgabe aus der Aufgabenliste im Abschnitt **Virensuche** gelöscht.

Achtung.

Nur Aufgaben, die von Ihnen selbst erstellt wurden, können umbenannt und gelöscht werden.

8.4. Konfiguration von Aufgaben zur Virensuche

Auf welche Weise die Untersuchung von Objekten auf Ihrem Computer erfolgt, wird durch eine Auswahl von Parametern bestimmt, die für jede Aufgabe festgelegt werden.

Um zur Konfiguration der Aufgabenparameter zu wechseln,

öffnen Sie das Konfigurationsfenster des Programms und wählen Sie im Abschnitt **Virensuche** den Namen der Aufgabe.

Im Konfigurationsfenster können Sie für jede der Aufgaben:

- die Sicherheitsstufe wählen, auf deren Basis die Aufgabe ausgeführt werden soll (s. Pkt. 8.4.1 auf S. 93).
- zur detaillierten Konfiguration der Stufe wechseln:
 - die Parameter angeben, welche die Dateitypen bestimmen, die der Virusanalyse unterzogen werden (s. Pkt. 8.4.2 auf S. 94).
 - den Start von Aufgaben unter einem anderen Benutzerkonto konfigurieren (s. Pkt. 6.4 auf S. 67).
 - zusätzliche Parameter für die Untersuchung angeben (s. Pkt. 8.4.5 auf S. 100).
- die standardmäßig verwendeten Untersuchungsparameter wiederherstellen (s. Pkt. 8.4.3 auf S. 98).
- die Aktion wählen, die vom Programm beim Fund eines infizierten bzw. möglicherweise infizierten Objekts angewandt wird (s. Pkt. 8.4.4 auf S. 98).
- einen Zeitplan für den automatischen Aufgabenstart erstellen (s. Pkt. 6.5 auf S. 69).

Außerdem können Sie einheitliche Parameter für den Start aller Aufgaben festlegen (s. Pkt. 8.4.6 auf S. 102).

Im Folgenden werden alle oben aufgezählten Parameter zur Konfiguration einer Aufgabe ausführlich beschrieben.

8.4.1. Auswahl der Sicherheitsstufe

Jede Aufgabe zur Virensuche gewährleistet die Untersuchung von Objekten auf einer der folgenden Stufen (s. Abb. 25):

Hoch – Untersuchung des gesamten Computers oder eines Laufwerks, Ordners oder einer Datei mit maximaler Ausführlichkeit. Die Verwendung dieser Stufe wird empfohlen, wenn der Verdacht auf eine Virusinfektion Ihres Computers besteht.

Empfohlen - Die Parameter dieser Stufe entsprechen den von den Kaspersky-Lab-Experten empfohlenen Einstellungen. Sie umfassen die Untersuchung der gleichen Objekte wie bei der Stufe **Hoch** unter Ausnahme von Dateien in Mailformaten.

Niedrig – Da die Auswahl der untersuchten Dateien auf dieser Stufe eingeschränkt wird, erlaubt Ihnen diese Stufe, komfortabel mit Anwendungen zu arbeiten, die den Arbeitsspeicher stark beanspruchen.



Abbildung 25. Auswahl der Sicherheitsstufe für die Virenuntersuchung von Objekten

Die Untersuchung von Objekten erfolgt standardmäßig auf der **Empfohlenen** Stufe.

Sie können die Stufe für die Untersuchung von Dateien erhöhen oder senken, indem Sie eine andere Stufe wählen oder die Einstellungen der aktuellen Stufe ändern.

Um die Sicherheitsstufe zu ändern,

verschieben Sie den Zeiger auf der Skala. Durch das Anpassen der Sicherheitsstufe wird das Verhältnis zwischen der Ausführungsgeschwindigkeit der Untersuchung und der Anzahl der zu untersuchenden Dateien bestimmt: Je weniger Dateien der Virusanalyse unterzogen werden, desto höher ist die Untersuchungsgeschwindigkeit.

Wenn keine der genannten Sicherheitsstufen für die Untersuchung Ihren Anforderungen entspricht, können Sie die Untersuchungsparameter zusätzlich anpassen. Wählen Sie dazu die Stufe, die Ihren Anforderungen am nächsten kommt, als Ausgangsstufe und ändern Sie ihre Parameter entsprechend. In diesem Fall ändert sich die Stufe in **Benutzerdefiniert**.

Um die Einstellungen der aktuellen Sicherheitsstufe anzupassen,

klicken Sie im Konfigurationsfenster der Aufgabe auf die Schaltfläche **Einstellungen**, passen im folgenden Fenster die Einstellungen für die Untersuchung an und klicken auf die Schaltfläche **OK**.

Dadurch wird eine vierte Sicherheitsstufe mit der Bezeichnung **Benutzerdefiniert** erstellt, welche die von Ihnen definierten Untersuchungsparameter enthält.

8.4.2. Festlegen der zu untersuchenden Objekttypen

Durch die Angabe der Typen der zu untersuchenden Objekte bestimmen Sie das Format, die Größe und die Laufwerke der Dateien die beim Ausführen dieser Aufgabe untersucht werden sollen.

Der Typ der zu untersuchenden Dateien wird im Abschnitt **Dateitypen** festgelegt (s. Abb. 26). Wählen Sie eine der drei Varianten:

- ☛ **Alle Dateien untersuchen.** In diesem Fall werden alle Dateien ohne Ausnahme der Untersuchung unterzogen.
- ☛ **Programme und Dokumente (nach Inhalt) untersuchen.** Bei der Auswahl dieser Gruppe untersucht das Programm nur potentiell infizierbare Dateien, d.h. Dateien, in die ein Virus eindringen kann.

Bevor die Virensuche in einem Objekt beginnt, wird die interne Kopfzeile des Objekts hinsichtlich des Dateiformats analysiert (txt, doc, exe usw.).

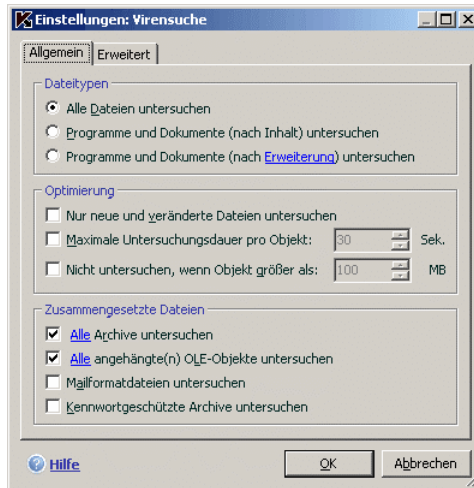


Abbildung 26. UntersuchungseinstellungenIm

Hinweis.



Es gibt eine Reihe von Dateiformaten, für die das Risiko des Eindringens von schädlichem Code und der späteren Aktivierung relativ gering ist. Dazu zählen beispielsweise Dateien im *txt*-Format.

Im Gegensatz dazu gibt es Dateiformate, die ausführbaren Code enthalten oder enthalten können. Als Beispiele für solche Objekte dienen Dateien der Formate *exe*, *dll*, *doc*. Das Risiko des Eindringens und der Aktivierung von schädlichem Code ist für solche Dateien relativ hoch.

- ☛ **Programme und Dokumente (nach Erweiterung) untersuchen.** In diesem Fall untersucht das Programm nur potentiell infizierbare Dateien, wobei das Dateiformat auf Basis der Dateinamenserweiterung ermittelt wird. Wenn Sie dem Link Erweiterung folgen, gelangen Sie zu einer Liste der

Dateierweiterungen, die in diesem Fall untersucht werden (s. Anhang A.1 auf S. 194).

Hinweis.

Es sollte beachtet werden, dass ein Virus in einer Datei mit der Endung txt in Wirklichkeit eine ausführbare Datei sein kann, die in eine txt-Datei umbenannt wurde. Wenn Sie die Variante  **Programme und Dokumente (nach Erweiterung) untersuchen** wählen, wird eine solche Datei bei der Untersuchung übersprungen. Wenn Sie die Variante  **Programme und Dokumente (nach Inhalt) untersuchen** gewählt haben, analysiert das Programm ungeachtet der Erweiterung die Kopfzeile der Datei, wodurch sich ergibt, dass die Datei das Format exe besitzt. Eine solche Datei wird der sorgfältigen Virusuntersuchung unterzogen.

Abschnitt **Optimierung** lässt sich festlegen, dass nur Dateien untersucht werden sollen, die neu sind oder seit ihrer letzten Analyse verändert wurden. Dieser Modus erlaubt es, die Untersuchungszeit wesentlich zu verkürzen und die Arbeitsgeschwindigkeit des Programms zu erhöhen. Aktivieren Sie dazu das Kontrollkästchen **Nur neue und veränderte Dateien untersuchen**. Dieser Modus erstreckt sich auf gewöhnliche und zusammengesetzte Dateien.

Außerdem kann im Abschnitt **Optimierung** eine Begrenzung für die Untersuchungszeit und die maximale Größe eines einzelnen Objekts festgelegt werden.

Maximale Untersuchungsdauer pro Objekt ... Sek. Aktivieren Sie das Kontrollkästchen, um die Untersuchung eines einzelnen Objekts in zeitlicher Hinsicht zu begrenzen, und geben Sie die maximale Untersuchungsdauer für ein Objekt im Feld rechts an. Bei einer Überschreitung der Zeitbegrenzung wird das Objekt von der Untersuchung ausgeschlossen.

Nicht untersuchen, wenn Objekt größer als ... MB. Aktivieren Sie das Kontrollkästchen, um die Untersuchung eines einzelnen Objekts hinsichtlich der Größe zu begrenzen, und geben Sie die maximal zulässige Größe eines Objekts im Feld rechts an. Bei einer Überschreitung der Größenbegrenzung wird das Objekt von der Untersuchung ausgeschlossen.

Geben Sie im Abschnitt **Zusammengesetzte Dateien** an, welche zusammengesetzten Dateien auf Viren analysiert werden sollen:

Alle/Nur neue Archive untersuchen – Archive der Formate RAR, ARJ, ZIP, CAB, LHA, JAR, ICE untersuchen.

Achtung!

Archive, in denen Kaspersky Anti-Virus die Desinfektion nicht unterstützt (z.B. HA, UUE, TAR), werden nicht automatisch gelöscht, selbst wenn als Aktion die automatische Desinfektion oder das Löschen irreparabler Objekte gewählt wurde.

Verwenden den Link [Archiv löschen](#) im Meldungsfenster über den Fund des gefährlichen Objekts, um solche Archive zu löschen. Dieser Hinweis erscheint nur unter der Bedingung auf dem Bildschirm, dass die Aktion **Während der Untersuchung erfragen / Nach Abschluss der Untersuchung erfragen** ausgewählt wurden (s. Pkt. 8.4.4 auf S.98). Außerdem kann ein infiziertes Archiv manuell vom Computer gelöscht werden.

- Alle/Nur neue angehängte(n) OLE-Objekte untersuchen** – Objekte, die in eine Datei eingebettet sind, untersuchen (beispielsweise eine Excel-Tabelle oder ein Makro, das in eine Microsoft Word-Datei eingebettet ist, der Anhang einer E-Mail-Nachricht, usw.).

Für jeden Typ einer zusammengesetzten Datei können Sie wählen, ob alle oder nur neue Dateien untersucht werden sollen. Verwenden Sie dazu den Link neben der Bezeichnung des Objekts. Der Link verändert seinen Wert, wenn mit der linken Maustaste darauf geklickt wird. Wenn im Abschnitt **Optimierung** festgelegt wurde, dass nur neue und veränderte Dateien untersucht werden sollen, steht die Auswahl des Typs der zusammengesetzten Dateien nicht zur Verfügung.

- Mailformatdateien untersuchen** – Dateien in Mailformaten und Mail-Datenbanken untersuchen. Wenn das Kontrollkästchen deaktiviert ist, werden Mailformatdateien wie binäre Dateien untersucht (ohne Formatanalyse). Ist die Datei virenfrei und der Parameter **Alle Dateien untersuchen** wurde ausgewählt, dann wird der Status *ok* im Bericht eingetragen. Wenn hingegen Parameter zur Dateiuntersuchung nach Typ und Erweiterung festgelegt wurden, wird das Objekt mit dem Status *nicht bearbeitet nach Typ* übersprungen.

Beachten Sie folgende Besonderheiten bei der Untersuchung von Mail-Datenbanken, die durch Kennwort geschützt sind:

- Kaspersky Anti-Virus erkennt schädlichen Code in Datenbanken für Microsoft Office Outlook 2000, desinfiziert diesen aber nicht.
- Das Programm unterstützt die Suche nach schädlichem Code in geschützten Mail-Datenbanken für Microsoft Office Outlook 2003 nicht.

- Kennwortgeschützte Archive untersuchen** – Untersuchung von Archiven, die durch Kennwort geschützt sind. In diesem Fall erfolgt vor der Untersuchung von Objekten, die in dem Archiv enthalten sind, auf dem

Bildschirm eine Kennwortabfrage. Wenn das Kontrollkästchen nicht aktiviert ist, werden kennwortgeschützte Archive bei der Untersuchung übersprungen.

8.4.3. Wiederherstellen der standardmäßigen Untersuchungseinstellungen

Während der Konfiguration der Parameter für die Aufgabenausführung können Sie jederzeit zu den empfohlenen Einstellungen zurückkehren. Diese gelten als optimal, werden von den Kaspersky-Lab-Spezialisten empfohlen und sind in der Sicherheitsstufe **Empfohlen** zusammengefasst.

Um die standardmäßigen Untersuchungseinstellungen für Objekte wiederherzustellen,

1. Wählen Sie den Namen der Datei im Abschnitt **Virensuche** des Hauptfensters und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Aufgabe.
2. Klicken Sie im Abschnitt **Sicherheitsstufe** auf die Schaltfläche **Grundeinstellung**.

8.4.4. Auswahl der Aktion für Objekte

Wenn sich durch die Virenuntersuchung eines Objekts herausstellt, dass es infiziert oder verdächtig ist, hängen die weiteren Operationen des Programms vom Status des Objekts und von der ausgewählten Aktion ab.

Ein Objekt kann aufgrund der Untersuchung einen der folgenden Status erhalten:

- Status eines der schädlichen Programme (beispielsweise *Virus*, *trojanisches Programm*).
- *möglicherweise infiziert*, wenn sich aufgrund der Untersuchung nicht eindeutig feststellen lässt, ob das Objekt infiziert ist oder nicht. Möglicherweise wurde in der Datei die Folge eines Codes eines unbekanntes Virus oder der modifizierte Code eines bekannten Virus gefunden.

Standardmäßig werden alle infizierten Dateien der Desinfektion unterzogen und alle möglicherweise infizierten Dateien in die Quarantäne verschoben.

Um die Aktion für ein Objekt zu ändern,

wählen Sie den Namen der Aufgabe im Abschnitt **Virensuche** des Programmhauptfensters und wechseln Sie mit dem Link Einstellungen in das Konfigurationsfenster der Aufgabe. Alle verfügbaren Aktionen werden im entsprechenden Abschnitt genannt (s. Abb. 27).

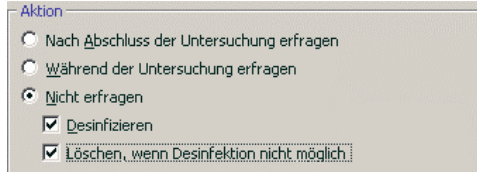


Abbildung 27. Auswahl der Aktion für ein gefährliches Objekt

Gewählte Aktion	Was geschieht beim Fund eines infizierten/ möglicherweise infizierten Objekts?
<input checked="" type="radio"/> Nach Abschluss der Untersuchung erfragen	Die Anwendung schiebt die Bearbeitung von Objekten bis zum Ende der Untersuchung auf. Nach dem Abschluss der Untersuchung erscheint nacheinander für jedes Objekt eine Aktionsanfrage.
<input checked="" type="radio"/> Während der Untersuchung erfragen	Die Anwendung zeigt eine Warnmeldung auf dem Bildschirm an, die Informationen darüber enthält, von welchem schädlichen Code das Objekt infiziert/möglicherweise infiziert ist, und bietet Aktionen zur Auswahl an.
<input checked="" type="radio"/> Nicht erfragen	Die Anwendung protokolliert im Bericht Informationen über die gefundenen Objekte. Die Objekte werden nicht bearbeitet und es erfolgt keine Meldung. Es wird davor gewarnt, diesen Funktionsmodus für das Programm zu wählen, weil infizierte und möglicherweise infizierte Objekte dann auf Ihrem Computer verbleiben und es praktisch unmöglich ist, eine Infektion zu verhindern.

<input checked="" type="radio"/> Nicht erfragen <input checked="" type="checkbox"/> Desinfizieren	Die Anwendung führt ohne Bestätigungsabfrage einen Desinfektionsversuch mit dem gefundenen Objekt aus. Wenn ein Objekt desinfiziert werden kann, wird es zur nachfolgenden Desinfektion in den Backup-Speicher verschoben. Wenn der Desinfektionsversuch fehlschlägt, wird der Zugriff auf das Objekt gesperrt.
<input checked="" type="radio"/> Nicht erfragen <input checked="" type="checkbox"/> Desinfizieren <input checked="" type="checkbox"/> Löschen, Desinfektion möglich	Die Anwendung führt ohne Bestätigungsabfrage einen Desinfektionsversuch mit dem gefundenen Objekt aus. Wenn der Desinfektionsversuch fehlschlägt, wird das Objekt gelöscht. Eine Kopie des Objekts wird im Backup-Speicher abgelegt.
<input checked="" type="radio"/> Nicht erfragen <input type="checkbox"/> Desinfizieren <input checked="" type="checkbox"/> Löschen	Die Anwendung löscht das Objekt automatisch.

Bevor ein Desinfektionsversuch erfolgt oder das Objekt gelöscht wird, legt Kaspersky Anti-Virus eine Sicherungskopie des Objekts an und speichert diese im Backup (s. Pkt. 11.2 auf S. 126). Dadurch wird erlaubt, das Objekt bei Bedarf wiederherzustellen oder später zu desinfizieren.

Ein Objekt mit dem Status *möglicherweise infiziert* wird ohne vorherigen Desinfektionsversuch in die Quarantäne verschoben.

8.4.5. Zusätzliche Optionen für die Virensuche

Neben der Konfiguration der grundlegenden Parameter für die Virenuntersuchung können Sie noch zusätzliche Parameter festlegen (s. Abb. 28):

- iChecker-Technologie aktivieren** – Die Verwendung dieser Technologie erlaubt eine Steigerung der Untersuchungsgeschwindigkeit, weil bestimmte Objekte von der Untersuchung ausgeschlossen werden. Das Ausschließen eines Objekts von der Untersuchung erfolgt nach einem speziellen Algorithmus, der das Erscheinungsdatum der Bedrohungssignaturen, das Datum der letzten Untersuchung des Objekts und die Änderung von Untersuchungseinstellungen berücksichtigt.

Wurde beispielsweise eine Archivdatei vom Programm untersucht und ihr wurde der Status virenfrei zugewiesen, dann wird das Archiv von der folgenden Untersuchung ausgeschlossen, wenn es nicht verändert wurde und die Untersuchungsparameter gleich geblieben sind. Wenn Sie die Zusammensetzung des Archivs durch das Hinzufügen eines neuen Objekts verändert, die Untersuchungsparameter geändert haben, oder wenn die Datenbanken für die Bedrohungssignaturen aktualisiert wurden, wird das Archiv erneut untersucht.

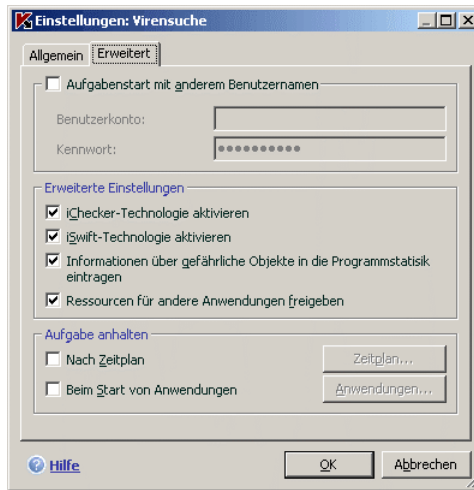


Abbildung 28. Erweiterte Untersuchungseinstellungen

Die Technologie iChecker™ besitzt Einschränkungen: Sie funktioniert nicht mit großen Dateien und kann nur auf Objekte angewandt werden, deren Struktur der Anwendung Kaspersky Anti-Virus bekannt ist (z.B. die Dateiformate *exe, dll, lnk, ttf, inf, sys, com, chm, zip, rar*).

- iSwift-Technologie aktivieren** – Diese Technologie stellt eine Weiterentwicklung der iChecker-Technologie für Computer mit NTFS-Dateisystem dar. Die Technologie iSwift besitzt folgende Einschränkungen: Sie ist an einen konkreten Ort der Datei im Dateisystem gebunden und kann nur auf Objekte angewandt werden, die sich in einem NTFS-Dateisystem befinden.
- Informationen über gefährliche Objekte in die Programmstatistik eintragen** – Informationen über den Fund gefährlicher Objekte in der generellen Programmstatistik speichern und in der Liste der gefährlichen Bedrohungen auf der Registerkarte Gefunden im Berichtsfenster (s. Pkt. 11.3.2 auf S. 133) anzeigen. Wenn das Kontrollkästchen deaktiviert ist, werden keine Informationen über gefährliche Objekte im Bericht angezeigt und folglich ist die Bearbeitung dieser Objekte nicht möglich.

- Ressourcen für andere Anwendungen freigeben** – Die Ausführung dieser Untersuchungsaufgabe anhalten, wenn die Prozessorressourcen von anderen Anwendungen beansprucht werden.

8.4.6. Festlegen einheitlicher Untersuchungsparameter für alle Aufgaben

Jede Untersuchungsaufgabe wird mit eigenen Parametern ausgeführt. Für die Aufgaben, die bei der Programminstallation auf dem Computer erstellt wurden, gelten standardmäßig die von den Kaspersky-Lab-Spezialisten empfohlenen Parameter.

Sie können einheitliche Untersuchungsparameter für alle Aufgaben festlegen. Als Grundlage gilt dabei die Auswahl der Parameter, die bei der Virenuntersuchung eines einzelnen Objekts verwendet werden.


Um einheitliche Untersuchungsparameter für alle Aufgaben festzulegen:

1. Wählen Sie den Abschnitt **Virensuche** auf der linken Seite des Programmhauptfensters und verwenden Sie den Link Einstellungen.
2. Legen Sie im folgenden Konfigurationsfenster die Untersuchungsparameter fest: Wählen Sie die Sicherheitsstufe (s. Pkt. 8.4.1 auf S. 93), nehmen Sie die erweiterten Einstellungen für die Sicherheitsstufe vor und bestimmen Sie die Aktion für Objekte (s. Pkt. 8.4.4 auf S. 98).
3. Klicken Sie auf die Schaltfläche **Übernehmen** im Abschnitt **Einstellungen anderer Aufgaben**, um die vorgenommenen Änderungen für alle Aufgaben zu übernehmen. Bestätigen Sie das Festlegen der einheitlichen Parameter.

KAPITEL 9. TESTEN DER ARBEIT VON KASPERSKY ANTI-VIRUS FOR WINDOWS SERVERS

Nach Installation und Konfiguration von Kaspersky Anti-Virus wird empfohlen, die Korrektheit von Einstellungen und Funktion der Anwendung mit Hilfe eines "Testvirus" und seinen Modifikationen zu prüfen.

9.1. EICAR-"Testvirus" und seine Modifikationen

Dieser Testvirus wurde vom Institut  (The European Institute for Computer Antivirus Research) speziell zum Überprüfen der Arbeit von Antiviren-Produkten entwickelt.

Der "Testvirus" IST KEIN VIRUS und enthält keinen Programmcode, der Ihren Rechner beschädigen könnte. Trotzdem wird er von den meisten Antiviren-Softwareprodukten als Virus erkannt.

Verwenden Sie nie echte Viren, um die Funktionsfähigkeit eines Antiviren-Produkts zu testen!

Der "Testvirus" kann von der offiziellen Internetseite des **EICAR**-Instituts heruntergeladen werden: http://www.eicar.org/anti_virus_test_file.htm.

Die von der Webseite des **EICAR**-Instituts heruntergeladene Datei enthält den Code des standardmäßigen "Testvirus". Kaspersky Anti-Virus erkennt diese Datei, weist ihr den Typ **Virus** zu und führt die für diesen Objekttyp festgelegte Aktion aus.

Um die Reaktion von Kaspersky Anti-Virus beim Fund von Objekten eines anderen Typs zu prüfen, können Sie den Inhalt des standardmäßigen "Testvirus" durch Hinzufügen eines Präfixes modifizieren (s. Tabelle).

Präfix	Status des "Testvirus"	Entsprechende Aktion bei der Bearbeitung des Objekts durch die Anwendung
kein Präfix, standardmäßiger "Testvirus"	Die Datei enthält den "Testvirus". Die Desinfektion ist nicht möglich.	Die Anwendung identifiziert dieses Objekt als schädlich und irreparabel. Das Objekt wird gelöscht.
CORR-	Beschädigt.	Die Anwendung hat Zugriff auf das Objekt erhalten, kann es aber nicht untersuchen, weil es beschädigt ist (z.B. Struktur des Objekts ist beschädigt, ungültiges Dateiformat).
SUSP- WARN-	Die Datei enthält den "Testvirus" (Modifikation). Die Desinfektion ist nicht möglich.	Dieses Objekt ist eine Modifikation eines bekannten Virus oder ein unbekannter Virus. Im Moment des Funds enthalten die Datenbanken mit den Bedrohungssignaturen keine Beschreibung zur Desinfektion dieses Objekts. Die Anwendung verschiebt das Objekt in die Quarantäne, um es später mit aktualisierten Bedrohungssignaturen zu bearbeiten.
ERRO-	Bearbeitungsfehler.	Während der Bearbeitung des Objekts ist ein Fehler aufgetreten: Die Anwendung erhält keinen Zugriff auf das Untersuchungsobjekt, weil die Integrität des Objekts beschädigt ist (z.B. kein Endpunkt in einem Multi-Level-Archiv) oder die Verbindung zu dem Objekt fehlt (wenn ein Objekt in einer Netzwerkressource untersucht wird).
CURE-	Die Datei enthält den "Testvirus". Die Desinfektion ist möglich. Das Objekt kann repariert werden, wobei der Text des	Das Objekt enthält einen Virus, der desinfiziert werden kann. Die Anwendung führt die Antiviren-Bearbeitung des Objekts durch. Danach ist das Objekt vollständig repariert.

Präfix	Status des "Testvirus"	Entsprechende Aktion bei der Bearbeitung des Objekts durch die Anwendung
	"Viruskörpers" in CURE geändert wird.	
DELE-	Die Datei enthält den "Testvirus". Die Desinfektion ist nicht möglich.	Dieses Objekt ist irreparabel von einem Virus infiziert oder ist ein trojanisches Programm. Die Anwendung löscht solche Objekte.

Die erste Spalte der Tabelle enthält Präfixe, die dem standardmäßigen "Testvirus" am Zeilenanfang hinzugefügt werden können. In der zweiten Spalte werden für die unterschiedlichen Typen des "Testvirus" der Status und die Reaktion von Kaspersky Anti-Virus beschrieben. Die dritte Spalte bietet Informationen über die vom Status abhängige Bearbeitung der Objekte durch die Anwendung.

Die Aktionen für das jeweilige Objekt werden durch die vorgegebenen Einstellungen für die Antiviren-Untersuchung festgelegt.

9.2. Testen des Datei-Anti-Virus

Um die Funktionsfähigkeit von Datei-Anti-Virus zu testen:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen EICAR-Seite (s. Pkt. 9.1 auf S. 103) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.
2. Erlauben Sie das Protokollieren aller Ereignisse im Bericht, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht werden, in der Berichtsdatei gespeichert werden. Aktivieren Sie dazu im Konfigurationsfenster für Berichte das Kontrollkästchen **Informative Ereignisse protokollieren** (s. Pkt. 11.3.1 auf S. 132).
3. Starten Sie den "Testvirus" oder seine Modifikation zur Ausführung.

Datei-Anti-Virus fängt den Zugriff auf die Datei ab, untersucht und löscht sie:

Die Reaktion von Datei-Anti-Virus auf den Fund der einzelnen Objekttypen kann getestet werden, indem zuvor unterschiedliche Aktionsvarianten gewählt werden.

Das vollständige Arbeitsergebnis von Datei-Anti-Virus ist im Bericht über die Arbeit der Komponente enthalten.

9.3. Testen einer Aufgabe zur Virensuche

Um eine Untersuchungsaufgabe zu testen:

1. Erstellen Sie einen Ordner auf der Festplatte. Kopieren Sie den von der offiziellen EICAR-Seite (s. Pkt. 9.1 auf S. 103) heruntergeladenen "Testvirus" und die von Ihnen erstellten Modifikationen des "Testvirus" in diesen Ordner.
2. Erstellen Sie eine neue Aufgabe (s. Pkt. 8.3 auf S. 91) zur Virensuche und wählen Sie als Untersuchungsobjekt den Ordner (s. Pkt. 9.1 auf S. 103), der die "Testviren" enthält.
3. Erlauben Sie das Protokollieren aller Ereignisse, damit Daten über beschädigte Objekte oder Objekte, die aufgrund einer Störung nicht untersucht wurden, in der Berichtsdatei gespeichert werden. Aktivieren Sie dazu im Konfigurationsfenster für Berichte das Kontrollkästchen **Informative Ereignisse protokollieren**.
4. Starten Sie die Ausführung der Aufgabe zur Virensuche (s. Pkt. 8.1 auf S. 89).

Während der Untersuchung werden beim Fund verdächtiger oder infizierter Objekte auf dem Bildschirm Meldungen mit Informationen über das Objekt und einer Bestätigungsabfrage zur folgenden Aktion angezeigt:



Abbildung 29. Ein gefährliches Objekt wurde gefunden

Die Reaktion von Kaspersky Anti-Virus auf den Fund der einzelnen Objekttypen kann getestet werden, indem zuvor unterschiedliche Aktionsvarianten gewählt werden.

Das vollständige Arbeitsergebnis der Ausführung der Untersuchungsaufgabe ist im Bericht über die Arbeit der Komponente enthalten.

KAPITEL 10. UPDATE DES PROGRAMMS

Eine Voraussetzung für die Sicherheit ist die Pflege des aktuellen Zustands von Kaspersky Anti-Virus. Jeden Tag tauchen neue Viren, Trojaner und andere schädliche Programme auf. Deshalb ist es sehr wichtig sicherzustellen, dass Ihre Informationen zuverlässig geschützt werden.

Die Aktualisierung des Programms umfasst den Download und die Installation folgender Elemente auf Ihren Computer:

- **Bedrohungssignaturen**

Der Schutz der Informationen auf ihrem Computer basiert auf den Signaturen der Bedrohungen. Die Schutzkomponenten verwenden diese bei der Suche und Desinfektion gefährlicher Objekte auf Ihrem Computer. Die Signaturen werden stündlich durch Einträge über neue Bedrohungen und entsprechende Desinfektionsmethoden ergänzt. Deshalb wird ausdrücklich empfohlen, die Signaturen regelmäßig zu aktualisieren.

In den vorhergehenden Versionen der Antiviren-Anwendungen von Kaspersky Lab wurde die Arbeit mit einer unterschiedlichen Auswahl von Bedrohungssignaturen unterstützt: *Standard-* oder *erweiterte Auswahl*. Sie unterschieden sich im Hinblick auf die Typen der gefährlichen Objekte, vor denen Sie Ihren Computer schützten. In Kaspersky Anti-Virus 6.0 brauchen Sie sich nicht um die Auswahl der passenden Art von Bedrohungssignaturen kümmern. Bei der Arbeit unserer Produkte werden jetzt Bedrohungssignaturen verwendet, die nicht nur den Schutz vor unterschiedlichen Arten schädlicher und potentiell gefährlicher Objekte, sondern auch vor Hackerangriffen bieten.

- **Programm-Module**

Neben den Bedrohungssignaturen können Sie auch die Programm-Module von Kaspersky Anti-Virus aktualisieren. Kaspersky Lab gibt periodisch Updatepakete heraus.

Als primäre Updatequelle für Kaspersky Anti-Virus gelten die speziellen Kaspersky-Lab-Updateserver. Für den erfolgreichen Updatedownload von den Updateservern ist eine Verbindung des Servers mit dem Internet erforderlich.

Wenn Sie keinen Zugriff auf die Kaspersky-Lab-Updateserver besitzen (wenn beispielsweise kein Internetzugang vorhanden ist), können Sie unter folgenden Nummern unsere Hauptverwaltung anrufen: +7 (495) 797 87 00, +7 (495) 645 79 39 oder +7 (495) 956 70 00. Dort können Sie die Adressen der Partner von

Kaspersky Lab erfahren, die Ihnen die Updates auf Disketten oder CDs im zip-Format anbieten können.

Der Updatedownload erfolgt in einem der folgenden Modi:

- *Automatisch.* Kaspersky Anti-Virus prüft in festgelegten Zeitabständen, ob an der Updatequelle ein neues Updatepaket vorhanden ist. Die Häufigkeit der Überprüfung kann während Virusepidemien steigen und unter gewöhnlichen Umständen sinken. Wenn neue Updates vorhanden sind, lädt die Anwendung sie herunter und installiert sie auf dem Computer. Dieser Modus gilt als Standard.
- *Nach Zeitplan.* Die Aktualisierung des Programms erfolgt nach einem festgelegten Zeitplan.
- *Manuell.* In diesem Fall starten Sie die Aktualisierung des Programms selbständig.

Beim Updatevorgang werden die Programm-Module und die Bedrohungssignaturen auf Ihrem Computer mit den auf der Updatequelle vorhandenen verglichen. Wenn auf dem Server die aktuelle Version der Signaturen und Module installiert ist, wird im Anwendungsfenster ein entsprechender Eintrag angezeigt. Wenn Signaturen und Module nicht aktuell sind, wird nur der fehlende Teil der Updates auf Ihrem Computer installiert. Signaturen und Module werden nicht vollständig kopiert, wodurch die Updategeschwindigkeit wesentlich gesteigert und der Netzwerkverkehr entlastet wird.

Bevor die Bedrohungssignaturen aktualisiert werden, legt Kaspersky Anti-Virus eine Sicherungskopie davon an. Bei Bedarf können Sie zu den vorhergehenden Signaturen zurückkehren.

Die Möglichkeit des Rollbacks (s. Pkt. 10.2 auf S. 109) ist beispielsweise erforderlich, wenn Sie die Bedrohungssignaturen aktualisiert haben und diese bei der Arbeit beschädigt wurden. Sie können zu der vorhergehenden Variante der Signaturen zurückkehren und ihre Aktualisierung später erneut versuchen.

Während die Anwendung aktualisiert wird, können Sie gleichzeitig die Verteilung der heruntergeladenen Updates in eine lokale Quelle ausführen (s. Pkt. 10.4.4 auf S. 118). Dieser Dienst erlaubt es, die Datenbanken und Module, die von Anwendungen der Version 6.0 verwendet werden, auf den Netzwerkcomputern zu aktualisieren und dadurch Netzwerkverkehr einzusparen.

10.1. Starten des Updates

Sie können das Programm-Update jederzeit starten. Die Aktualisierung erfolgt von der von Ihnen gewählten Updatequelle (s. Pkt. 10.4.1 auf S. 111).

Das Programm-Update kann gestartet werden:

- aus dem Kontextmenü (s. Pkt. 4.2 auf S. 38).
- aus dem Hauptfenster des Programms (s. Pkt. 4.3 auf S. 39).

Um das Programm-Update aus dem Kontextmenü zu starten,

1. Öffnen Sie das Menü durch Rechtsklick auf das Programmsymbol im Infobereich.
2. Wählen Sie den Punkt **Update**.

Um das Update aus dem Programmhauptfenster zu starten,

1. Wählen Sie die Komponente **Update** im Abschnitt **Service**.
2. Klicken Sie auf die Schaltfläche **Update** auf der rechten Seite des Hauptfensters oder auf die Schaltfläche ► in der Statuszeile.

Der Updateprozess des Programms wird in einem speziellen Fenster dargestellt. Sie können das Fenster mit den aktuellen Update-Ergebnissen ausblenden. Klicken Sie dazu auf die Schaltfläche **Schließen**. Der Updatevorgang wird dabei fortgesetzt.

Beachten Sie, dass beim Ausführen des Updates gleichzeitig die Update-Verteilung in eine lokale Quelle erfolgt, falls dieser Dienst aktiviert wurde (s. Pkt. 10.4.4 auf S. 118).

10.2. Rückkehr zum vorherigen Update

Jedes Mal, wenn Sie das Programm-Update starten, erstellt Kaspersky Anti-Virus zuerst eine Sicherungskopie der aktuellen Bedrohungssignaturen und geht erst danach zu deren Update über. Dadurch wird Ihnen erlaubt, zur Verwendung der vorhergehenden Version der Signaturen zurückzukehren, wenn das Update erfolglos war.

Um zur Verwendung der vorhergehenden Version der Bedrohungssignaturen zurückzukehren,

1. Wählen Sie die Komponente **Update** im Abschnitt **Service** des Programmhauptfensters.
2. Klicken Sie auf die Schaltfläche **Rollback** auf der rechten Seite des Hauptfensters.

10.3. Erstellen einer Update-Aufgabe

Kaspersky Anti-Virus verfügt über eine integrierte Update-Aufgabe für die Aktualisierung der Bedrohungssignaturen und Programm-Module. Sie können aber auch eigene Update-Aufgaben mit anderen Parametern oder alternativem Startzeitplan erstellen.

Wenn Sie das Programm Kaspersky Anti-Virus beispielsweise auf einem Laptop installiert haben, den Sie zu Hause und im Büro benutzen, kann das Update zu Hause unter Verwendung der Kaspersky-Lab-Server, im Büro aber aus einem lokalen Ordner, der die erforderlichen Updates enthält, erfolgen. Um die Update-Einstellungen nicht jedes Mal ändern zu müssen, können Sie zwei unterschiedliche Aufgaben verwenden.

Um eine zusätzliche Update-Aufgabe zu erstellen,

1. Wählen Sie im Abschnitt **Service** des Programmhauptfensters den Punkt **Update**, öffnen Sie mit der rechten Maustaste das Kontextmenü und wählen Sie den Punkt **Speichern unter**.
2. Geben Sie im folgenden Fenster den Namen der Aufgabe an und klicken Sie auf **OK**. Dadurch erscheint die Aufgabe mit dem angegebenen Namen im Abschnitt **Service** des Programmhauptfensters.

Achtung!

Es können maximal Update-Aufgaben vom Benutzer erstellt werden.

Die neue Aufgabe übernimmt unter Ausnahme des Zeitplans alle Parameter der Aufgabe, auf deren Grundlage sie erstellt wurde. Der automatische Start der neuen Aufgabe ist in der Grundeinstellung deaktiviert. Deshalb sind folgende Zusatzeinstellungen erforderlich: Angabe der Updatequelle (s. Pkt. 10.4.1 auf S. 111), der Parameter für die Netzwerkverbindung (s. Pkt. 10.4.3 auf S. 116). Falls erforderlich, muss außerdem der Aufgabenstart mit Rechten aktiviert (s. Pkt. 6.4 auf S. 67) und der Zeitplan konfiguriert (s. Pkt. 6.5 auf S. 69) werden.

Um eine Aufgabe umzubenennen,

wählen Sie die Aufgabe im Abschnitt **Service** des Programmhauptfensters aus, öffnen Sie mit der linken Maustaste das Kontextmenü und wählen Sie den Punkt **Umbenennen**.

Geben Sie im folgenden Fenster den neuen Namen für die Aufgabe an und klicken Sie auf die Schaltfläche **OK**. Dadurch wird der Aufgabenname im Abschnitt **Service** geändert.

Um eine Aufgabe zu löschen,

wählen Sie die Aufgabe im Abschnitt **Service** des Programmhauptfensters aus, öffnen Sie mit der linken Maustaste das Kontextmenü und wählen Sie den Punkt **Löschen**.

Bestätigen Sie das Löschen. Dadurch wird die Aufgabe aus der Aufgabenliste im Abschnitt **Service** gelöscht.

Achtung!

Das Umbenennen und Löschen ist nur für Benutzeraufgaben möglich.

10.4. Update-Einstellungen

Das Programm-Update wird genau nach den Parametern ausgeführt, die festlegen:

- von welcher Ressource der Download und die Installation der Programm-Updates erfolgt (s. Pkt. 10.4.1 auf S. 111).
- in welchem Modus die Programmaktualisierung gestartet wird und welche Elemente aktualisiert werden sollen (s. Pkt. 10.4.2 auf S. 114).
- wie oft das Update gestartet werden soll, wenn der Start nach Zeitplan aktiviert ist (s. Pkt. 6.5 auf S. 69).
- unter welchem Benutzerkonto das Update ausgeführt wird (s. Pkt. 6.4 auf S. 67).
- ob die heruntergeladenen Updates in einen lokalen Ordner kopiert werden sollen (s. Pkt. 10.4.4 auf S. 118).
- welche Aktionen nach dem Programm-Update ausgeführt werden sollen (s. Pkt. 10.4.5 auf S. 119).

In diesem Abschnitt des Handbuchs werden alle oben genannten Aspekte ausführlich beschrieben.

10.4.1. Auswahl der Updatequelle

Eine *Updatequelle* ist eine bestimmte Ressource, die Updates der Bedrohungssignaturen und der Module für Kaspersky Anti-Virus enthält.

Als Updatequelle können dienen:

- *Administrationsserver* – zentralisierter Updatespeicher, der sich auf dem Administrationsserver von Kaspersky Administration Kit befindet (Details siehe Administratorhandbuch zu "Kaspersky Administration Kit").
- *Kaspersky-Lab-Updateserver* – spezielle Internetseiten, auf denen die Updates für Bedrohungssignaturen und Programm-Module für alle Kaspersky-Lab-Produkte zur Verfügung gestellt werden.
- *HTTP- oder FTP-Server, lokale Ordner oder Netzwerkordner* – lokaler Server oder Ordner, der die aktuellen Updates enthält.

Wenn Sie keinen Zugriff auf die Kaspersky-Lab-Updateserver besitzen (wenn beispielsweise kein Internetzugang vorhanden ist), können Sie unter folgenden Nummern unsere Hauptverwaltung anrufen: +7 (495) 797 87 00, +7 (495) 645 79 39 oder +7 (495) 956 70 00. Dort können Sie die Adressen der Partner von Kaspersky Lab erfahren, die Ihnen die Updates auf Disketten oder CDs im zip-Format anbieten können.

Achtung!

Geben Sie bei der Bestellung von Updates auf Wechseldatenträgern unbedingt an, ob Sie Updates der Programm-Module erhalten möchten.

Die auf einem Wechseldatenträger erhaltenen Updates können Sie auf einer ftp- oder http-Seite oder in einem lokalen oder Netzwerkordner speichern.

Die Auswahl der Updatequelle erfolgt auf der Registerkarte **Updatequelle** (s. Abb. 30).

Die Aktualisierung erfolgt standardmäßig von den Kaspersky-Lab-Updateservern. Die Serverliste kann nicht verändert werden. Beim Updateprozess greift Kaspersky Anti-Virus auf diese Liste zu, wählt die erste Serveradresse aus und versucht, die Updates von dort herunterzuladen. Wenn die Aktualisierung von der gewählten Adresse erfolglos ist, wendet sich das Programm an die nächste Adresse und versucht erneut, die Updates zu empfangen.

Damit die Aktualisierung von einer bestimmten ftp- oder http-Seite erfolgt,

1. klicken Sie auf die Schaltfläche **Hinzufügen**.
2. wählen Sie die http- oder ftp-Seite im Fenster **Updatequelle wählen** oder geben Sie ihre IP-Adresse, ihren symbolischen Namen oder die URL-Adresse im Feld **Quelle** an. Wenn eine ftp-Ressource als Updatequelle gewählt wird, können in der URL-Adresse des Servers die Autorisierungsparameter im Format <ftp://user:password@server> angegeben werden.

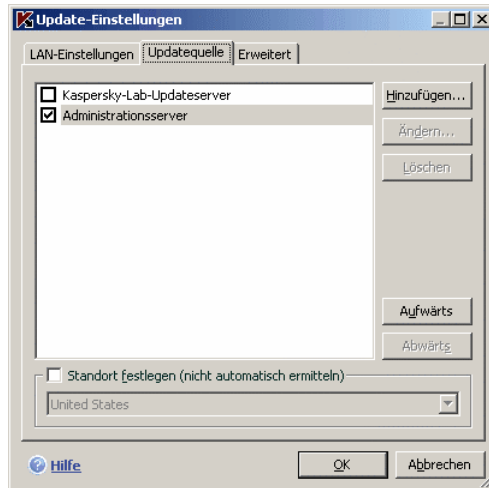


Abbildung 30. Auswahl der Updatequelle

Achtung!

Wenn als Updatequelle eine Ressource gewählt wurde, die sich außerhalb des lokalen Netzwerks befindet, ist für die Aktualisierung eine Internetverbindung erforderlich.

Um das Programm aus einem bestimmten Ordner zu aktualisieren,

1. klicken Sie auf die Schaltfläche **Hinzufügen**.
2. wählen Sie den Ordner im Fenster **Auswahl der Updatequelle** oder geben Sie den vollständigen Pfad des Ordners im Feld **Quelle** an.

Kaspersky Anti-Virus fügt die neue Updatequelle am Anfang der Liste hinzu und aktiviert sie automatisch zur Verwendung (aktiviert das entsprechende Kontrollkästchen).

Wenn als Updatequellen mehrere Ressourcen gewählt wurden, dann greift das Programm bei der Aktualisierung streng nach der Listenreihenfolge darauf zu und aktualisiert sich von der ersten verfügbaren Quelle. Sie können die Anordnung der Quellen in der Liste mit Hilfe der Schaltflächen **Aufwärts/Abwärts** ändern.

Die Quellenliste kann mit den Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** bearbeitet werden. Die Updateserver von Kaspersky Lab und Kaspersky Administration Kit können nicht geändert oder gelöscht werden.

Wenn Sie die Kaspersky-Lab-Server als Updatequelle verwenden, können Sie den für Sie günstigsten Standort des Servers für den Updatedownload auswählen. Kaspersky Lab besitzt Server in mehreren Ländern der Erde. Die Auswahl des geografisch am nächsten gelegenen Kaspersky-Lab-Updateservers kann die Dauer des Updates verkürzen und die Downloadgeschwindigkeit erhöhen.

Um den nächstliegenden Server zu wählen, aktivieren Sie das Kontrollkästchen **Standort berücksichtigen Standort festlegen (nicht automatisch ermitteln)** und wählen Sie aus der Dropdown-Liste das Land aus, in dem Sie sich gerade aufhalten. Wenn das Kontrollkästchen aktiviert ist, erfolgt das Update unter Berücksichtigung des in der Liste ausgewählten Standorts. Standardmäßig ist das Kontrollkästchen deaktiviert und beim Update werden Informationen über den aktuellen Standort aus der Registrierung des Betriebssystems verwendet.

10.4.2. Auswahl von Updatemodus und Update-Objekt

Ein wichtiger Faktor bei der Konfiguration des Programm-Updates ist das Festlegen von Update-Objekt und Updatemodus.

Das Update-Objekt (s. Abb. 31) bestimmt, welche Elemente aktualisiert werden:

- Bedrohungssignaturen
- Programm-Module

Die Bedrohungssignaturen werden immer aktualisiert, die Programm-Module nur dann, wenn der entsprechende Modus aktiviert ist.

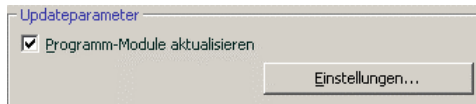


Abbildung 31. Auswahl der Update-Objekte

Damit beim Updateprozess die Updates der Programm-Module auf Ihren Computer kopiert und installiert werden,

aktivieren Sie das Kontrollkästchen **Programm-Module aktualisieren** im Konfigurationsfenster der Komponente **Update**.

Wenn im Augenblick in der Quelle ein Update für die Programm-Module vorhanden ist, lädt das Programm die erforderlichen Updates herunter und installiert sie nach dem Neustart des Computers. Die

heruntergeladenen Updates für die Module werden nicht vor dem Neustart installiert.

Erfolgt das nächste Update vor dem Neustart des Computers und der Installation der bereits heruntergeladenen Updates für die Programm-Module, dann werden nur die Updates der Bedrohungssignaturen heruntergeladen.

Der Updatemodus (s. Abb. 32) bestimmt, auf welche Weise die Aktualisierung gestartet wird. Sie können im Block **Startmodus** einen der folgenden Modi wählen:

- **Automatisch.** Kaspersky Anti-Virus prüft in festgelegten Zeitabständen, ob an der Updatequelle (s. Pkt. 10.4.1 auf S. 111) ein neues Updatepaket vorhanden ist. Wenn neue Updates vorhanden sind, lädt Kaspersky Anti-Virus sie herunter und installiert sie auf dem Computer.

Wenn als Quelle eine Netzwerkressource gewählt wurde, führt Kaspersky Anti-Virus in dem Intervall, das im vorhergehenden Updatepaket angegeben ist, einen Updateversuch durch. Aus einer lokalen Quelle erfolgt das Update im Intervall, das im vorhergehenden Updatepaket angegeben ist. Diese Option erlaubt es, die Updatefrequenz bei Virenepidemien und anderen gefährlichen Situationen automatisch zu regulieren. Das Programm wird rechtzeitig mit aktuellen Updates der Bedrohungssignaturen, Netzwerkangriffe und Programm-Module versorgt, was die Möglichkeit des Eindringens gefährlicher Programme auf Ihren Computer verhindert.



Abbildung 32. Auswahl des Startmodus für das Update

- **Nach Zeitplan.** Die Aktualisierung des Programms erfolgt nach einem festgelegten Zeitplan. Wenn Sie zu diesem Updatemodus wechseln möchten, wird Ihnen standardmäßig angeboten, das Update alle 2 Stunden vorzunehmen. Um den Zeitplan anzupassen, klicken Sie auf die Schaltfläche **Ändern** neben der Bezeichnung des Modus und nehmen Sie im folgenden Fenster entsprechende Änderungen vor (Details s. Pkt. 6.5 auf S. 69). Dieser Updatemodus wird standardmäßig benutzt.
- **Manuell.** In diesem Fall starten Sie die Aktualisierung des Programms selbständig. Kaspersky Anti-Virus informiert Sie bei Bedarf über die Notwendigkeit der Aktualisierung:

- erstens wird über dem Programmsymbol im Infobereich eine entsprechende Meldung eingeblendet (falls der Benachrichtigungsdienst aktiviert ist) (s. Pkt. 11.8.1 auf S. 145).

- zweitens informiert der zweite Indikator im Programmhauptfenster darüber, wenn der Schutz auf ihrem Computer veraltet ist (s. Pkt. 5.1.1 auf S. 44).
- drittens erscheint im Bereich der Kommentare und Empfehlungen des Hauptfensters eine Empfehlung zum Programm-Update (s. Pkt. 4.3 auf S. 39).

10.4.3. Konfiguration der Verbindungsparameter

Wenn Sie als Updatequelle die Kaspersky-Lab-Updateserver oder eine bestimmte ftp- oder http-Seite gewählt haben, ist es empfehlenswert, die Einstellungen für die Internetverbindung zu überprüfen.

Alle Parameter sind auf der speziellen Registerkarte **LAN-Einstellungen** untergebracht (s. Abb. 33).

Der Parameter **Passiven FTP-Modus verwenden, wenn möglich** wird verwendet, wenn Sie Updates von einem ftp-Server herunterladen, mit dem eine Verbindung im passiven Modus ausgeführt wird (beispielsweise über eine Firewall). Wenn der aktive Modus für die FTP-Verbindung benutzt wird, können Sie dieses Kontrollkästchen deaktivieren.

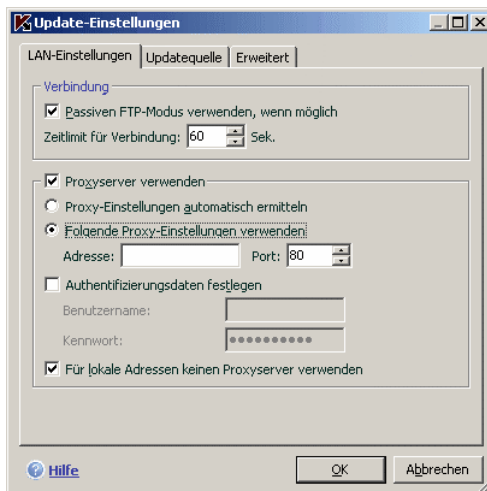


Abbildung 33. Anpassen der Netzwerkeinstellungen für das Update

Geben Sie im Feld **Zeitlimit für Verbindung (Sek.)** den Zeitraum an, der zur Verfügung stehen soll, um eine Verbindung mit dem Updateserver aufzubauen.

Wenn nach Ablauf dieses Zeitraums keine Verbindung hergestellt wurde, erfolgt ein Verbindungsversuch mit dem nächsten Updateserver. Dieser Vorgang wird so lange ausgeführt, bis der Verbindungsaufbau gelingt oder bis alle verfügbaren Updateserver aufgerufen worden sind.

Wenn für die Internetverbindung ein Proxyserver verwendet wird, aktivieren Sie das Kontrollkästchen **Proxyserver verwenden** und passen Sie bei Bedarf folgende Parameter an:

- Wählen Sie, welche Proxyserver-Einstellungen für das Programm-Update verwendet werden sollen:
 - **Proxy-Einstellungen automatisch ermitteln.** Bei Auswahl dieser Variante werden die Parameter des Proxyservers automatisch mit Hilfe des Protokolls WPAD (Web Proxy Auto-Discovery Protocol) ermittelt. Falls die Adresse mit diesem Protokoll nicht ermittelt werden kann, verwendet Kaspersky Anti-Virus die Proxy-Einstellungen, die in Microsoft Internet Explorer angegeben sind.
 - **Folgende Proxy-Einstellungen verwenden** – Einen anderen Proxyserver verwenden, als jenen, der in den Verbindungseinstellungen des Browsers angegeben ist. Geben Sie im Feld **Adresse** die IP-Adresse oder den symbolischen Namen und im Feld **Port** den Port des Proxyservers an.
- Geben Sie an, ob auf dem Proxy eine Authentifizierung verwendet wird. Die *Authentifizierung* ist ein Vorgang, bei dem zum Zweck der Zugriffskontrolle die Anmeldeinformationen des Benutzers geprüft werden.

Wenn für eine Verbindung mit dem Proxyserver die Authentifizierung erforderlich ist, aktivieren Sie das Kontrollkästchen **Authentifizierungsdaten festlegen** und geben Sie in den unten angebrachten Feldern den Benutzernamen und das Kennwort an. In diesem Fall wird zuerst die NTLM-Autorisierung, danach die BASIC-Autorisierung versucht.

Wenn das Kontrollkästchen nicht aktiviert ist oder keine Daten angegeben werden, wird die NTLM-Autorisierung versucht, wobei das Benutzerkonto verwendet wird, in dessen Namen das Update gestartet wurde ist (s. Pkt. 6.4 auf S. 67).

Wenn die Autorisierung auf dem Proxyserver erforderlich ist, Sie aber den Benutzernamen und das Kennwort nicht angegeben haben oder der Proxyserver die angegebenen Daten aus einem beliebigen Grund nicht akzeptiert, erscheint beim Updatestart eine Anfrage nach Benutzername und Kennwort für die Autorisierung. Wenn die Autorisierung erfolgreich verläuft, werden künftig der angegebene Benutzername und das Kennwort verwendet. Andernfalls werden die Autorisierungsparameter erneut abgefragt.

Damit beim Update aus einem lokalen Ordner oder Netzwerkordner kein Proxyserver verwendet wird, aktivieren Sie das Kontrollkästchen **Für lokale Adressen keinen Proxyserver verwenden.**

10.4.4. Update-Verteilung

Der Dienst zur Update-Verteilung ermöglicht es, die Belastung des Netzwerkverkehrs eines Unternehmens zu optimieren. Das Verteilen der Updates wird auf zwei Etappen ausgeführt:

1. Ein Computer des Netzwerks lädt das Paket mit den Updates für Programm-Module und Bedrohungssignaturen von den Kaspersky-Lab-Webservern im Internet oder von einer anderen Webressource, auf der sich die aktuellen Updates befinden, herunter. Die heruntergeladenen Updates werden in einem gemeinsamen Ordner abgelegt.
2. Die übrigen Netzwerkcomputer verwenden den gemeinsamen Ordner zum Download der Updates für die Anwendung.

Um den Dienst zur Update-Verteilung zu aktivieren, kreuzen Sie auf der Registerkarte **Erweitert** (s. Abb. Abbildung 34) das Kontrollkästchen **Zielordner für Update-Verteilung** an und geben Sie im darunter liegenden Feld den Pfad des gemeinsamen Ordners an, in dem die heruntergeladenen Updates abgelegt werden. Der Pfad kann manuell eingegeben oder im Fenster, das mit der Schaltfläche **Durchsuchen** geöffnet wird, gewählt werden. Wenn das Kontrollkästchen aktiviert ist, werden neue Updates beim Download automatisch in diesen Ordner kopiert.

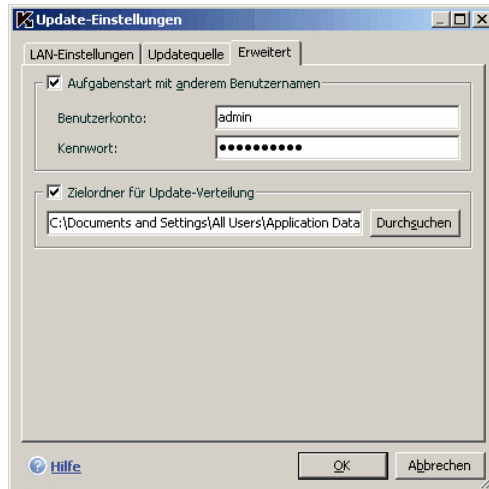


Abbildung 34. Einstellungen für den Dienst zur Update-Verteilung

Beachten Sie, dass Kaspersky Anti-Virus 6.0 von den Kaspersky-Lab-Updateservern nur das Updatepaket für die Anwendungen der Version 6.0 erhält.

Damit die anderen Netzwerkcomputer aus dem Ordner aktualisiert werden, der die aus dem Internet kopierten Updates enthält, sind folgende Einstellungen erforderlich.

1. Der gemeinsame Zugriff auf diesen Ordner muss gewährt werden.
2. Der gemeinsame Ordner muss in den Update-Einstellungen der Netzwerkcomputer als Updatequelle angegeben werden.

10.4.5. Aktionen nach dem Programm-Update

Jedes Update der Bedrohungssignaturen enthält neue Einträge, die es erlauben, Ihren Computer vor neu aufgetauchten Bedrohungen zu schützen.

Die Kaspersky-Lab-Spezialisten empfehlen Ihnen, sofort nach dem Programm-Update die *in der Quarantäne gespeicherten Objekte* und die *Autostart-Objekte* zu untersuchen.

Warum gerade diese Objekte?

In die Quarantäne werden Objekte verschoben, bei deren Untersuchung nicht genau festgestellt werden konnte, von welchen schädlichen Programmen sie infiziert sind (s. Pkt. 11.1 auf S. 122). Möglicherweise kann Kaspersky Anti-Virus die Gefahr eindeutig bestimmen und desinfizieren, nachdem die Bedrohungssignaturen aktualisiert wurden.

Das Programm untersucht die Quarantäneobjekte standardmäßig nach jedem Update der Bedrohungssignaturen. Es wird empfohlen, die Objekte in der Quarantäne regelmäßig zu überprüfen. Aufgrund der Untersuchung kann sich der Status einzelner Objekte ändern. Bestimmte Objekte können am ursprünglichen Ort wiederhergestellt und wieder verwendet werden.

Damit keine Untersuchung der Quarantäneobjekte erfolgt, deaktivieren Sie das Kontrollkästchen **Quarantänedateien untersuchen** im Block **Aktion nach dem Update**.

Die Autostart-Objekte gelten hinsichtlich der Sicherheit Ihres Computers als kritischer Bereich. Wenn dieser Bereich von einem Schadprogramm infiziert wird, ist vielleicht sogar der Start des Betriebssystems nicht mehr möglich. Zur Untersuchung dieses Bereichs verfügt Kaspersky Anti-Virus über eine vordefinierte Aufgabe zur Untersuchung der Autostart-Objekte (s. Kapitel 8 auf S. 88). Es wird empfohlen, den Zeitplan dieser Aufgabe so festzulegen, dass sie jedes Mal nach dem Update der Bedrohungssignaturen automatisch gestartet wird (s. Pkt. 6.5 auf S. 69).

KAPITEL 11. ZUSÄTZLICHE OPTIONEN

Neben dem Schutz Ihrer Daten bietet das Programm zusätzliche Dienste, welche die Funktionalität von Kaspersky Anti-Virus erweitern.

Während der Arbeit verschiebt das Programm bestimmte Objekte in spezielle Speicher. Das Ziel dieses Vorgehens besteht darin, maximalen Datenschutz mit minimalen Verlusten zu gewährleisten.

- Der Backup-Speicher enthält Kopien der Objekte, die aufgrund der Arbeit von Kaspersky Anti-Virus verändert oder gelöscht wurden (s. Pkt. 11.2 auf S. 126). Wenn ein bestimmtes Objekt wichtige Informationen enthielt, die bei der Bearbeitung nicht vollständig erhalten werden konnten, können Sie das Objekt jederzeit über seine Sicherungskopie wiederherstellen.
- Die Quarantäne enthält möglicherweise infizierte Objekte, deren Desinfektion mit der aktuellen Version der Bedrohungssignaturen erfolglos war (s. Pkt. 11.1 auf S. 122).

Es wird empfohlen, die Liste der Objekte immer wieder zu überprüfen. Möglicherweise befinden sich veraltete Objekte darunter oder bestimmte Objekte können wiederhergestellt werden.

Folgende Dienste helfen bei der Arbeit mit dem Programm:

- Der Dienst des Technischen Support-Services bietet umfassende Hilfe bei der Arbeit mit Kaspersky Anti-Virus (s. Pkt. 11.6 auf S. 140). Die Experten von Kaspersky Lab haben sich bemüht, alle vorhandenen Unterstützungsmöglichkeiten zu integrieren: Online-Support, Forum für Fragen und Vorschläge der Programmbenutzer usw.
- Der Benachrichtigungsdienst für Ereignisse hilft Ihnen bei der Konfiguration einer Benachrichtigung des Benutzers über wichtige Momente bei der Arbeit von Kaspersky Anti-Virus (s. Pkt. 11.8.1 auf S. 145). Dies können einerseits Ereignisse informativen Charakters sein, andererseits aber Fehler, die unverzüglich behoben werden müssen und hohe Priorität besitzen.
- Der Dienst für den Selbstschutz des Programms und für die Beschränkung des Zugriffs auf die Arbeit mit dem Programm bietet den programmeigenen Dateien Schutz vor Veränderungen und Beschädigungen durch Angreifer, verbietet die externe Steuerung der Programmdienste und kontrolliert die Beschränkung von Rechten der

Serveradministratoren zum Ausführen bestimmter Aktionen mit Kaspersky Anti-Virus (s. Pkt. 11.8.2 auf S. 149). Beispielsweise kann das Ändern der Schutzstufe wesentlichen Einfluss auf die Informationssicherheit auf Ihrem Computer ausüben.

- Der Dienst zur Verwaltung von Lizenzschlüsseln erlaubt es, ausführliche Informationen über die verwendete Lizenz zu erhalten, Ihre Programmkopie zu aktivieren sowie Lizenzschlüsseldateien zu verwalten (s. Pkt. 11.5 auf S. 138).

Darüber hinaus bietet das Programm ein ausführliches Hilfesystem (s. Pkt. 11.4 auf S. 137) und detaillierte Berichte (s. Pkt. 11.3 auf S. 129) über die Arbeit von Datei-Anti-Virus und die Ausführung aller Aufgaben zur Virensuche und zum Update.

Außerdem besteht die Möglichkeit, das Aussehen von Kaspersky Anti-Virus zu ändern und die Parameter der aktuellen Programmoberfläche zu konfigurieren (s. Pkt. 11.7 auf S. 142).

Im Folgenden werden alle genannten Dienste ausführlich beschrieben.

11.1. Quarantäne für möglicherweise infizierte Objekte

Die **Quarantäne** ist ein spezieller Speicher, in den Objekte verschoben werden, die möglicherweise von Viren infiziert sind.

Möglicherweise infizierte Objekte sind Objekte, die verdächtig sind, von Viren oder Virenmodifikationen infiziert zu sein.

Warum *möglicherweise infiziert*? Es ist nicht immer möglich, eindeutig festzustellen, ob ein Objekt infiziert ist oder nicht. Dafür gibt es folgende Gründe:

- Der Code des analysierten Objekts besitzt Ähnlichkeit mit einer bekannten Bedrohung, wurde aber teilweise verändert.

Die Bedrohungssignaturen enthalten jene Bedrohungen, die bisher von den Kaspersky-Lab-Spezialisten untersucht wurden. Wenn ein Schadprogramm verändert wird und diese Veränderungen noch nicht in die Signaturen aufgenommen wurden, klassifiziert Kaspersky Anti-Virus das Objekt, das von einem veränderten Schadprogramm infiziert ist, als möglicherweise infiziertes Objekt und informiert darüber, welcher Bedrohung diese Infektion ähnelt.

- Der Code des gefundenen Objekts erinnert an die Struktur eines Schadprogramms. Die Bedrohungssignaturen enthalten jedoch keine entsprechenden Einträge.

Es ist durchaus möglich, dass es sich um eine neue Art von Bedrohung handelt. Deshalb klassifiziert Kaspersky Anti-Virus dieses Objekt als möglicherweise infiziertes Objekt.

Der Verdacht, dass eine Datei durch einen Virus infiziert ist, wird mit dem *heuristischen Code Analysator* ermittelt. Dieser Mechanismus ist sehr effektiv und führt nur selten zu einem Fehlalarm.

Ein verdächtiges Objekt kann während der Virensuche sowie bei der Arbeit von Datei-Anti-Virus gefunden und in die Quarantäne verschoben werden.

Sie können eine Datei selbst in die Quarantäne verschieben. Dazu dient die Schaltfläche **Quarantäne** in der speziellen Meldung, die beim Fund eines möglicherweise infizierten Objekts auf dem Bildschirm Ihres Computers erscheint.

Beim Speichern eines Objekts in die Quarantäne wird das Objekt verschoben, nicht kopiert: Das Objekt wird von dem entsprechenden Laufwerk oder aus einer E-Mail-Nachricht gelöscht und im Quarantäneordner gespeichert. Die unter Quarantäne stehenden Dateien werden in einem speziellen Format gespeichert und stellen keine Gefahr dar.

11.1.1. Aktionen mit Objekten in der Quarantäne

Die Gesamtzahl der Objekte, die in die Quarantäne verschoben wurden, wird im Bereich **Datenverwaltung** des Abschnitts **Service** angezeigt. Auf der rechten Seite des Hauptfensters befindet sich der spezielle Block **Quarantäne**, der folgende Daten enthält:

- Anzahl der möglicherweise infizierten Objekte, die während der Arbeit von Kaspersky Anti-Virus gefunden wurden.
- aktuelle Größe des Speichers.

Mit der Schaltfläche **Leeren** können alle Quarantäneobjekte gelöscht werden. Beachten Sie, dass dabei auch die Objekte des Backups und die Berichtsdateien gelöscht werden.

Um zu den Quarantäneobjekten zu wechseln,

klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks **Quarantäne**.

Auf der Registerkarte **Quarantäne** (s. Abb. 35) können Sie folgende Aktionen vornehmen:

- Verschieben einer Datei in die Quarantäne, wenn Sie vermuten, dass die Datei von einem Virus infiziert ist, den das Programm nicht finden konnte. Klicken Sie dazu auf die Schaltfläche **Hinzufügen** und geben Sie im standardmäßigen Auswahlfenster die betreffende Datei an. Sie wird mit dem Status *Vom Benutzer hinzugefügt* zur Liste hinzugefügt.

Wenn eine Datei manuell in die Quarantäne verschoben wurde und bei einer späteren Untersuchung als virenfrei erkannt wird, ändert sich ihr Status nicht sofort nach der Untersuchung in *ok*. Der Status ändert sich nur dann sofort, wenn die Untersuchung mindestens drei Tage, nachdem die Datei unter Quarantäne gestellt wurde, stattfindet

- Alle möglicherweise infizierten Quarantäneobjekte unter Verwendung der aktuellen Version der Bedrohungssignaturen untersuchen und desinfizieren. Klicken Sie dazu auf die Schaltfläche **Alle untersuchen**.

Aufgrund der Untersuchung und Desinfektion eines beliebigen Quarantäne-Objekts kann sich sein Status in *infiziert*, *möglicherweise infiziert*, *Fehlalarm*, *ok* u.a. ändern.

Der Objektstatus *infiziert* bedeutet, dass das Objekt als infiziert erkannt wurde, die Desinfektion aber fehlgeschlagen ist. Wir empfehlen, Objekte mit diesem Status zu löschen.

Alle Objekte mit dem Status *Fehlalarm* können bedenkenlos wiederhergestellt werden, weil ihr vorheriger Status *möglicherweise infiziert* bei einer erneuten Untersuchung vom Programm nicht bestätigt wurde.

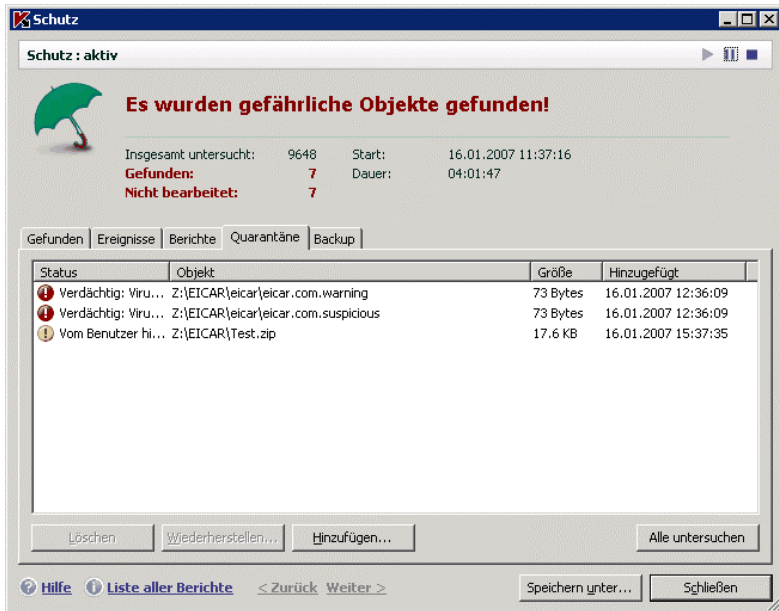


Abbildung 35. Liste der Quarantäneobjekte

- Dateien wiederherstellen – entweder in einem festgelegten Ordner oder in den Ordnern, aus denen sie (standardmäßig) in die Quarantäne verschoben wurden. Zum Wiederherstellen eines Objekts markieren Sie es in der Liste und klicken Sie auf **Wiederherstellen**. Bei der Wiederherstellung von Objekten, die aus Archiven, Mail-Datenbanken und Mail-Format-Dateien in die Quarantäne verschoben wurden, muss zusätzlich der Ordner angegeben werden, in dem sie wiederhergestellt werden sollen.

Empfehlung:

Es wird empfohlen, nur Objekte mit dem Status *Fehlalarm*, *ok* und *desinfiziert* wiederherzustellen, da die Wiederherstellung anderer Objekte zur Infektion Ihres Computers führen kann!

- Ein beliebiges Quarantäne-Objekt oder eine Gruppe ausgewählter Objekte löschen. Löschen Sie nur die Objekte, die nicht desinfiziert werden können. Klicken Sie auf die Schaltfläche **Löschen**, um Objekte zu löschen.

11.1.2. Konfiguration der Quarantäne-Einstellungen

Sie können folgende Parameter für das Erstellen und die Arbeit der Quarantäne anpassen:

- Auswahl des Modus zur automatischen Untersuchung von Objekten in der Quarantäne nach jedem Update der Bedrohungssignaturen (Details s. Pkt. 10.4.4 auf S. 118).

Achtung!

Das Programm kann die Quarantäneobjekte nicht unmittelbar nach der Aktualisierung der Bedrohungssignaturen untersuchen, wenn Sie in diesem Moment mit der Quarantäne arbeiten.

- Festlegen der maximalen Speicherdauer für Objekte in der Quarantäne.
Standardmäßig beträgt die Speicherdauer für Quarantäneobjekte 30 Tage. Danach werden die Objekte gelöscht. Sie können die maximale Speicherdauer für möglicherweise infizierte Objekte ändern oder diese Beschränkung ganz aufheben.

Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Anti-Virus mit der Schaltfläche Einstellungen aus dem Programmhauptfenster.
2. Wählen Sie **Datenverwaltung** in der Konfigurationsstruktur.
3. Legen Sie im Block **Quarantäne und Backup** (s. Abb. 36) den Zeitraum fest, nach dem Quarantäneobjekte automatisch gelöscht werden sollen.

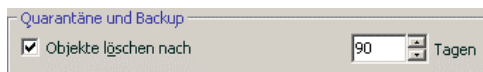


Abbildung 36. Anpassen der Speicherdauer für Quarantäneobjekte

11.2. Sicherungskopien gefährlicher Objekte

Bei der Desinfektion von Objekten kann es vorkommen, dass es nicht gelingt, die Objekte vollständig zu erhalten. Wenn ein desinfiziertes Objekt wichtige Informationen enthielt, die aufgrund der Desinfektion vollständig oder teilweise

verloren gingen, kann versucht werden, das ursprüngliche Objekt über seine Sicherungskopie wiederherzustellen.

Eine **Sicherungskopie** ist die Kopie eines gefährlichen Originalobjekts, die bei der ersten Desinfektion oder beim Löschen des Objekts erstellt und im Backup gespeichert wird.

Der **Backup-Speicher** ist ein spezieller Speicher, der die Sicherungskopien gefährlicher Objekte enthält, die bearbeitet oder gelöscht werden. Die Hauptfunktion des Backups besteht in der Möglichkeit, das ursprüngliche Objekt jederzeit wiederherzustellen. Die Sicherungskopien werden im Backup in einem speziellen Format gespeichert und stellen keine Gefahr dar.

11.2.1. Aktionen mit Sicherungskopien

Die Gesamtzahl der Sicherungskopien von Objekten, die sich im Backup befinden, wird in der **Datenverwaltung** des Abschnitts **Service** genannt. Auf der rechten Seite des Hauptfensters befindet sich der spezielle Block **Backup**, der folgende Daten enthält:

- Anzahl der Kopien von möglicherweise infizierten Objekten, die während der Arbeit von Kaspersky Anti-Virus angelegt wurden.
- aktuelle Größe des Backup-Speichers.

Mit der Schaltfläche **Leeren** können alle Sicherungskopien aus dem Backup gelöscht werden. Beachten Sie, dass dabei auch die Objekte aus der Quarantäne und die Berichtsdateien gelöscht werden.

Um zu den Kopien der gefährlichen Objekte zu wechseln,

klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks **Backup**.

Im mittleren Bereich der Registerkarte **Backup** (s. Abb. 37) befindet sich eine Liste der Sicherungskopien. Für jede Kopie werden folgende Informationen angegeben: vollständiger Name des Objekts mit Pfadangabe des ursprünglichen Speicherorts, Status des Objekts, der ihm aufgrund der Untersuchung zugewiesen wurde, und Größe.

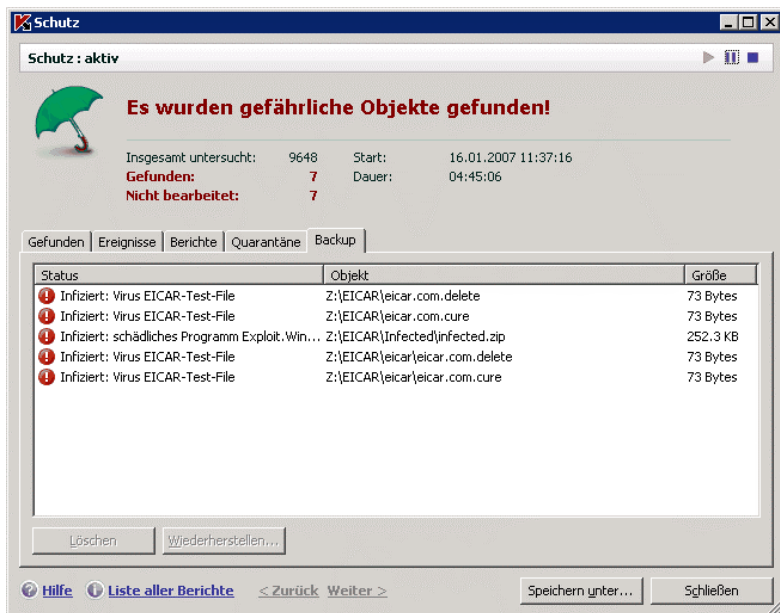


Abbildung 37. Sicherungskopien von gelöschten oder desinfizierten Objekten

Sie können ausgewählte Kopien mit Hilfe der Schaltfläche **Wiederherstellen** wiederherstellen. Das Objekt wird unter dem gleichen Namen aus dem Backup wiederhergestellt, den es vor der Desinfektion trug.

Wenn sich am ursprünglichen Speicherort ein Objekt mit dem gleichen Namen befindet (Diese Situation ist möglich, wenn ein Objekt wiederhergestellt wird, dessen Kopie vor der Desinfektion angelegt wurde), erscheint eine entsprechende Warnung auf dem Bildschirm. Sie können den Speicherort des wiederherzustellenden Objekts ändern oder es umbenennen.

Es wird empfohlen, das Objekt sofort nach der Wiederherstellung auf Viren zu untersuchen. Möglicherweise gelingt es, das Objekt mit den aktualisierten Signaturen ohne Datenverlust zu desinfizieren.

Es wird davor gewarnt, Sicherungskopien von Objekten wiederherzustellen, wenn es nicht absolut erforderlich ist. Dies kann zur Infektion des Computers führen.

Es wird empfohlen, den Speicher in bestimmten Zeitabständen zu überprüfen und überflüssige Objekte mit Hilfe der Schaltfläche **Löschen** zu entfernen. Sie können das Programm auch so konfigurieren, , dass die ältesten Kopien automatisch aus dem Speicher gelöscht werden (s. Pkt. 11.2.2 auf S. 129).

11.2.2. Konfiguration der Backup-Einstellungen

Sie können die maximale Speicherdauer der Kopien im Backup festlegen.

Standardmäßig beträgt die Speicherdauer für Kopien gefährlicher Objekte 90 Tage. Danach werden die Kopien gelöscht. Sie können die maximale Speicherdauer für Kopien ändern oder diese Beschränkung ganz aufheben. Gehen Sie dazu folgendermaßen vor:

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Anti-Virus mit der Schaltfläche Einstellungen aus dem Programmhauptfenster.
2. Wählen Sie **Datenverwaltung** in der Konfigurationsstruktur.
3. Legen Sie die Speicherdauer für Sicherungskopien im Block **Quarantäne und Backup** auf der rechten Seite des Fensters fest (s. Abb. 36).

11.3. Berichte

Die Arbeit des Datei-Anti-Virus von Kaspersky Anti-Virus und die Ausführung jeder Aufgabe zur Virensuche und des Updates werden in einem Bericht aufgezeichnet.

Über die Gesamtzahl der Berichte, die bisher vom Programm erstellt wurden, sowie ihre Gesamtgröße in Bytes wird in der **Datenverwaltung** des Abschnitts **Service** des Programmhauptfensters informiert. Diese Informationen befinden sich im Block **Berichte**.

Um zur Anzeige der Berichte zu wechseln,

klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks **Berichte**.

Dadurch wird das Fenster auf der Registerkarte **Berichte** geöffnet (s. Abb. 38). Hier befinden sich die neuesten Berichte für Datei-Anti-Virus und für die Aufgaben zur Virensuche und zum Update, die in der laufenden Sitzung von Kaspersky Anti-Virus gestartet wurden. Neben dem Namen von Datei-Anti-Virus oder der Aufgabe wird das Arbeitsergebnis genannt (beispielsweise *abgebrochen* oder *abgeschlossen*). Wenn Sie den vollständigen Verlauf der Berichtserstellung für die laufende Programmsitzung lesen möchten, aktivieren Sie das Kontrollkästchen **Verlauf der Berichte anzeigen**.

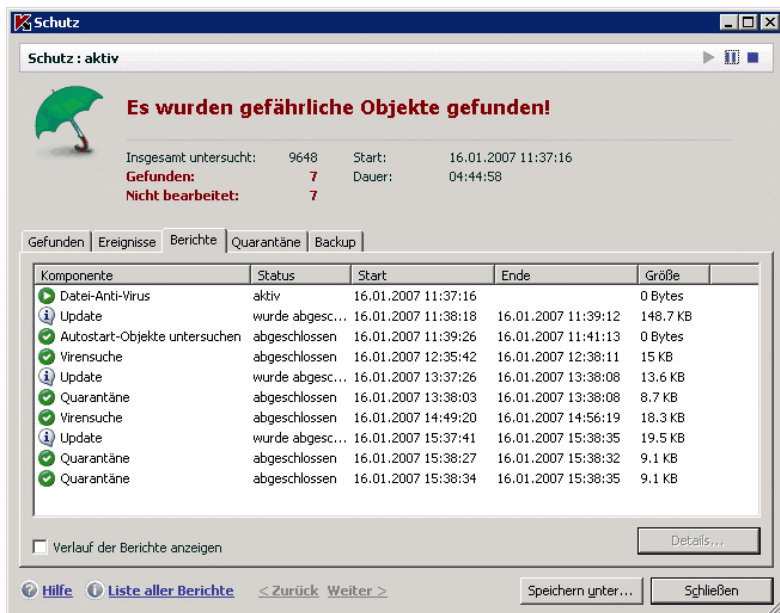


Abbildung 38. Berichte über die Arbeit der Programmkomponenten

Um alle Ereignisse anzuzeigen, die im Bericht über die Arbeit von Datei-Anti-Virus oder die Ausführung einer Aufgabe aufgezeichnet wurden,

wählen Sie Datei-Anti-Virus oder eine Aufgabe auf der Registerkarte **Berichte** aus und klicken Sie auf die Schaltfläche **Details**.

Dadurch wird ein Fenster geöffnet, das Detailinformationen über die Arbeit von Datei-Anti-Virus oder der Aufgabe enthält. Die Ergebnisstatistik der Arbeit befindet sich im oberen Bereich des Fensters, ausführliche Informationen befinden sich auf verschiedenen Registerkarten im zentralen Bereich.

- Die Registerkarte **Gefunden** enthält eine Liste der gefährlichen Objekte, die bei der Arbeit von Datei-Anti-Virus oder beim Ausführen einer Untersuchungsaufgabe gefunden wurden.
- Die Registerkarte **Ereignisse** informiert über die Ereignisse bei der Arbeit von Datei-Anti-Virus oder der Aufgabe.
- Die Registerkarte **Statistik** umfasst eine ausführliche Statistik aller untersuchten Objekte.
- Die Registerkarte **Einstellungen** enthält die Parameter, mit denen Datei-Anti-Virus, die Aufgabe zur Virensuche oder das Update der Bedrohungssignaturen arbeitet.

- Die Registerkarte **Gesperrte Benutzer** zeigt eine Liste der Benutzer, deren Computer gesperrt wurden, als versucht wurde, ein infiziertes oder möglicherweise infiziertes Objekt auf den Server zu kopieren.

Sie können den gesamten Bericht in eine Textdatei importieren. Das kann beispielsweise von Nutzen sein, wenn bei der Arbeit von Datei-Anti-Virus oder bei der Aufgabenausführung ein Fehler aufgetreten ist, den Sie nicht selbständig beseitigen können, und deshalb die Hilfe des Technischen Support-Services erforderlich ist. In diesem Fall wird der Bericht im Textformat an den Support-Service geschickt, damit unsere Spezialisten das Problem genau untersuchen und so schnell wie möglich lösen können.

Um einen Bericht in eine Textdatei zu importieren,

klicken Sie auf die Schaltfläche **Speichern unter** und geben Sie an, wo die Berichtsdatei gespeichert werden soll.

Klicken Sie zum Abschluss der Arbeit mit dem Bericht auf die Schaltfläche **Schließen**.

Alle Registerkarten des Berichts außer **Einstellungen** und **Statistik** verfügen über die Schaltfläche **Aktionen**, mit deren Hilfe Sie eine Reihe von Aktionen mit den Objekten der Liste vornehmen können. Durch Klick auf diese Schaltfläche öffnet sich ein Kontextmenü mit folgenden Punkten (Die Auswahl der Menüpunkte unterscheidet sich in Abhängigkeit von der Komponente, deren Bericht Sie geöffnet haben. Unten werden alle möglichen Punkte genannt):

Desinfizieren – Desinfizieren – Es wird versucht, das gefährliche Objekt zu desinfizieren. Wenn die Desinfektion des Objekts fehlschlägt, können Sie es entweder in der Liste belassen, um es später mit aktualisierten Bedrohungssignaturen zu untersuchen, oder es löschen. Diese Aktion kann sowohl auf ein einzelnes Objekt der Liste als auch auf mehrere ausgewählte Objekte angewandt werden.

Aus der Liste löschen. – Der Eintrag über den Fund des Objekts wird aus dem Bericht gelöscht.

Zur vertrauenswürdigen Zone hinzufügen – Das Objekt wird den Schutzausnahmen hinzugefügt. Dabei wird ein Fenster mit der Ausnahmeregel für dieses Objekt geöffnet.

Alle desinfizieren – Alle Objekte der Liste desinfizieren. Kaspersky Anti-Virus versucht, die Objekte unter Verwendung der Bedrohungssignaturen zu bearbeiten.

Leeren – Den Bericht über gefundene Objekte leeren. Dabei verbleiben alle gefundenen gefährlichen Objekte auf Ihrem Computer.

Datei anzeigen – Öffnen von Microsoft Windows Explorer in dem Ordner, in dem sich das Objekt befindet.

Auf <http://www.viruslist.de> anschauen – Zur Beschreibung des Objekts in der Viren-Enzyklopädie auf der Seite von Kaspersky Lab gehen.

Auf www.google.de nachschauen – Mit Hilfe der Suchmaschine Informationen über das Objekt suchen.

Suche – Die Bedingungen für die Suche nach einem Objekt (nach Name oder Status) in der Liste angeben.

Außerdem können Sie die Informationen dieses Fensters nach jeder Spalte aufsteigend oder absteigend sortieren.

Die Bearbeitung gefährlicher Objekte, die während der Arbeit von Kaspersky Anti-Virus gefunden wurden, erfolgt mit Hilfe der Schaltfläche **Desinfizieren** (für ein Objekt oder eine Gruppe ausgewählter Objekte) oder **Alle desinfizieren** (zur Bearbeitung aller Objekte in der Liste). Bei der Bearbeitung jedes Objekts erscheint auf dem Bildschirm eine Meldung, in der Sie aufgefordert werden, über die Aktion mit dem Objekt zu entscheiden.

Wenn Sie im Meldungsfenster das Kontrollkästchen **In allen ähnlichen Fällen anwenden** ankreuzen, wird die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewandt, die vor dem Beginn der Bearbeitung in der Liste ausgewählt wurden.

11.3.1. Konfiguration der Berichtparameter

Zur Konfiguration der Parameter für das Erstellen und Speichern von Berichten

Öffnen Sie das Konfigurationsfenster von Kaspersky Anti-Virus mit dem Link [Einstellungen](#) aus dem Programmhauptfenster.

1. Wählen Sie in der Konfigurationsstruktur den Punkt **Datenverwaltung**.
2. Nehmen Sie im Block **Berichte** (s. Abb. 39) die erforderlichen Einstellungen vor:
 - Erlauben oder Verbieten Sie das Aufzeichnen von Ereignissen mit rein informativem Charakter im Bericht. In der Regel sind solche Ereignisse nicht für den Schutz wichtig. Aktivieren Sie das Kontrollkästchen **Informative Ereignisse protokollieren**, um das Speichern solcher Ereignisse zu erlauben.
 - Sie können festlegen, dass nur Ereignisse protokolliert werden, die beim letzten Start der Aufgabe eingetreten sind. Dadurch kann Festplattenplatz gespart werden, weil der Bericht eine geringere Größe besitzt. Wenn das Kontrollkästchen **Nur**

aktuelle Ereignisse speichern aktiviert ist, werden die Informationen im Bericht bei jedem Neustart der Aufgabe aktualisiert. Allerdings werden nur Informationen mit rein informativem Charakter überschrieben.

- Bestimmen Sie, wie lange Berichte gespeichert werden sollen. Der Standardwert für die Speicherdauer von Berichten beträgt 90 Tage. Sie können die Speicherdauer ändern oder diese Beschränkung völlig aufheben.

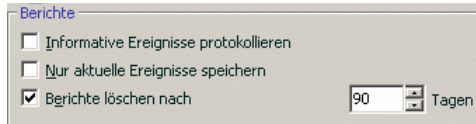


Abbildung 39. Einstellungen für das Erstellen von Berichten

11.3.2. Registerkarte *Gefunden*

Diese Registerkarte (s. Abb. 40) enthält eine Liste der gefährlichen Objekte, die von Kaspersky Anti-Virus gefunden wurden. Für jedes Objekt werden der vollständige Name und der Status angegeben, der ihm vom Programm bei der Untersuchung/Bearbeitung zugewiesen wurde.

Damit in der Liste nicht nur gefährliche Objekte, sondern auch Objekte, die erfolgreich desinfiziert wurden, angezeigt werden, aktivieren Sie das Kontrollkästchen **Desinfizierte Objekte anzeigen**.

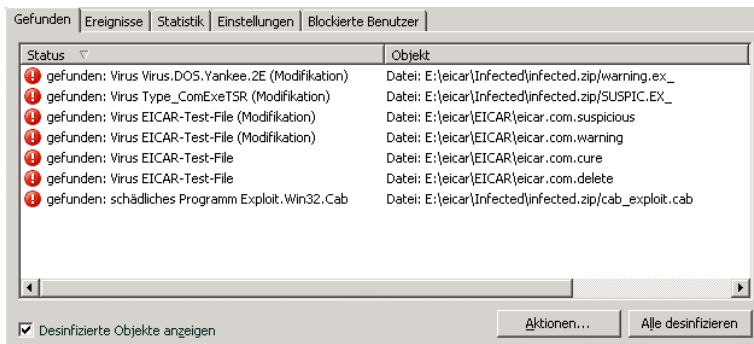


Abbildung 40. Liste der gefundenen gefährlichen Objekte

Die Bearbeitung gefährlicher Objekte, die während der Arbeit von Kaspersky Anti-Virus gefunden wurden, erfolgt mit Hilfe der Schaltfläche **Desinfizieren** (für ein Objekt oder eine Gruppe ausgewählter Objekte) oder **Alle desinfizieren** (zur Bearbeitung aller Objekte in der Liste). Bei der Bearbeitung jedes Objekts

erscheint auf dem Bildschirm eine Meldung, in der Sie aufgefordert werden, über die Aktion mit dem Objekt zu entscheiden.

Wenn Sie im Meldungsfenster das Kontrollkästchen **In allen ähnlichen Fällen anwenden** ankreuzen, wird die ausgewählte Aktion auf alle Objekte mit dem gleichen Status angewandt, die vor dem Beginn der Bearbeitung in der Liste ausgewählt wurden.

11.3.3. Registerkarte *Ereignisse*

Auf dieser Registerkarte (s. Abb. 41) wird eine vollständige Liste aller wichtigen Ereignisse bei der Arbeit von Datei-Anti-Virus oder beim Ausführen einer Aufgabe zur Virensuche oder zum Update für die Bedrohungssignaturen geführt.

Es gibt folgende Ereignistypen:

Kritische Ereignisse – Ereignisse mit kritischer Priorität, die auf Probleme bei der Arbeit des Programms oder auf Schwachstellen im Schutz Ihres Computers hinweisen. Beispiele: *Virus gefunden*, *Funktionsstörung*.

Wichtige Ereignisse – Ereignisse, die unbedingt beachtet werden müssen, weil Sie wichtige Situationen bei der Programmarbeit wiedergeben. Beispiel: *abgebrochen*.

Informative Ereignisse – Ereignisse mit informativem Charakter, die in der Regel keine wichtigen Informationen enthalten. Beispiele: *ok*, *nicht bearbeitet*. Diese Ereignisse erscheinen nur im Ereignisbericht, wenn das Kontrollkästchen **Alle Ereignisse anzeigen** aktiviert ist.

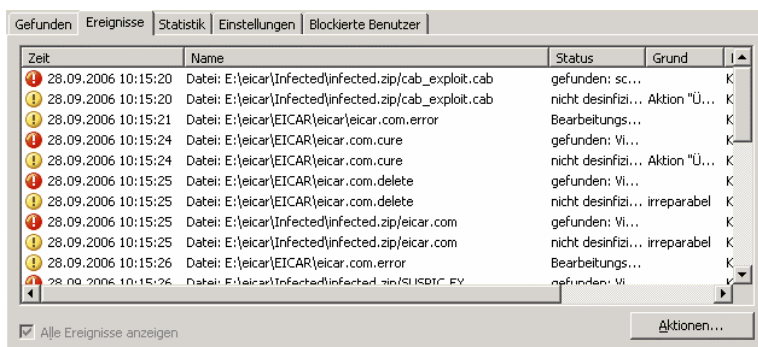


Abbildung 41. Ereignisse, die bei der Arbeit einer Komponente aufgetreten sind

Das Format der im Ereignisbericht enthaltenen Ereignisse kann in Abhängigkeit von der Komponente oder Aufgabe unterschiedlich sein. Für Update-Aufgaben wird beispielsweise angegeben:

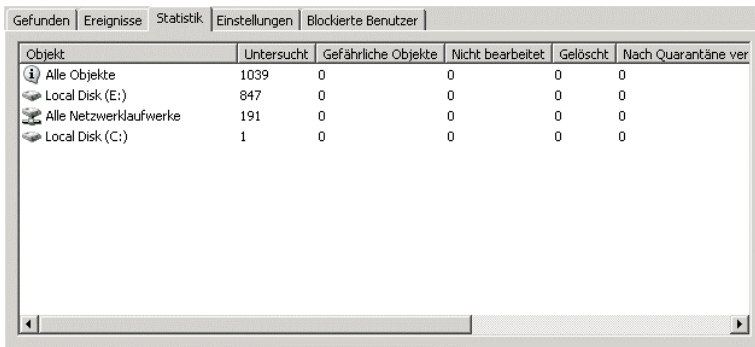
- Ereignisname
- Name des Objekts, für das dieses Ereignis aufgezeichnet wurde.
- Zeitpunkt, zu dem das Ereignis eintrat.
- Größe der heruntergeladenen Datei.

Für eine Aufgabe zur Virensuche enthält der Ereignisbericht den Namen des untersuchten Objekts und den Status, der dem Objekt aufgrund der Untersuchung/Bearbeitung zugewiesen wurde.

11.3.4. Registerkarte *Statistik*

Eine ausführliche Statistik über die Arbeit von Datei-Anti-Virus oder die Ausführung der Aufgabe zur Virensuche wird auf dieser Registerkarte aufgezeichnet (s. Abb. 42). Hier können Sie erfahren:

- Wie viele Objekte während der laufenden Sitzung von Datei-Anti-Virus oder bei der Aufgabenausführung auf das Vorhandensein gefährlicher Objekte untersucht wurden. Außerdem wird die Anzahl der untersuchten Archive, gepackten Dateien, kennwortgeschützten und beschädigten Objekte angegeben.
- Wie viele gefährliche Objekte gefunden wurden. Wie viele davon nicht desinfiziert, gelöscht und in die Quarantäne verschoben wurden.



Objekt	Untersucht	Gefährliche Objekte	Nicht bearbeitet	Gelöscht	Nach Quarantäne ver
Alle Objekte	1039	0	0	0	0
Local Disk (E:)	847	0	0	0	0
Alle Netzwerklaufwerke	191	0	0	0	0
Local Disk (C:)	1	0	0	0	0

Abbildung 42. Statistik über die Arbeit einer Komponente

11.3.5. Registerkarte *Einstellungen*

Die Registerkarte **Einstellungen** (s. Abb. 43) enthält eine vollständige Übersicht der Parameter, mit denen Datei-Anti-Virus arbeitet oder die Untersuchungsaufgabe bzw. das Programm-Update ausgeführt wird. Sie können

erfahren, welche Schutzstufe die Arbeit von Datei-Anti-Virus bietet oder auf welcher Stufe die Virensuche ausgeführt wird, welche Aktion mit einem gefährlichen Objekt ausgeführt wird oder welche Einstellungen beim Programm-Update verwendet werden, usw. Um zur Konfiguration der Parameter zu wechseln, verwenden Sie den Link [Einstellungen ändern](#).

Für die Aufgaben zur Virensuche können zusätzliche Ausführungsbedingungen festgelegt werden:

- Ausführungspriorität der Untersuchungsaufgabe bei Auslastung des Prozessors festlegen. Standardmäßig ist das Kontrollkästchen **Ressourcen für andere Anwendungen freigeben** aktiviert. Das Programm überwacht dabei das Auslastungsniveau des Prozessors und der Laufwerkssysteme im Hinblick auf die Aktivität anderer Anwendungen. Wenn das Auslastungsniveau wesentlich ansteigt und die normale Arbeit der Benutzeranwendungen stört, beendet das Programm die Aktivität zur Ausführung der Untersuchungsaufgaben. Dies führt zur Verlängerung der Untersuchungszeit und zur Überlassung von Ressourcen an Benutzeranwendungen.

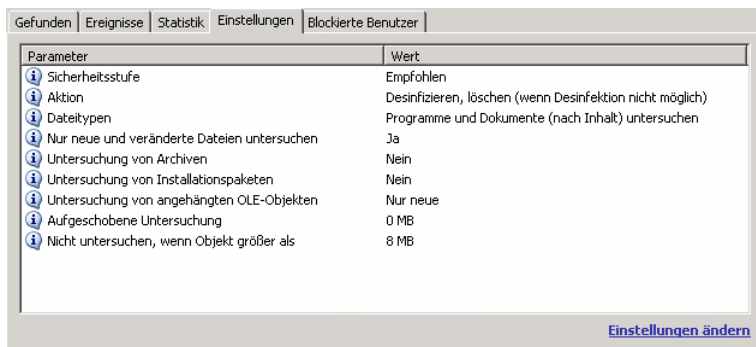


Abbildung 43. Einstellungen für die Arbeit einer Komponente

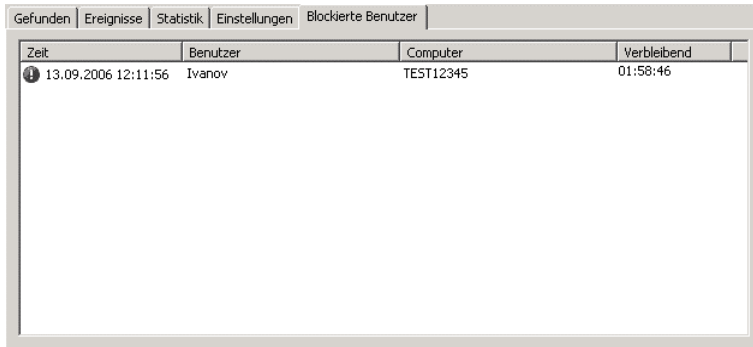
- Modus für die Arbeit des Computers nach dem Abschluss der Untersuchungsaufgabe bestimmen. Sie können festlegen, ob der Computer nach Untersuchungsende ausgeschaltet oder neu gestartet wird oder in den Standbymodus oder Ruhemodus wechselt. Klicken Sie mit der linken Maustaste auf den Hyperlink, bis er den gewünschten Wert annimmt.

11.3.6. Registerkarte *Gesperrte Benutzer*

Die Registerkarte **Gesperrte Benutzer** (s. Abb. Abbildung 44) enthält eine Liste der Benutzer, für die der Zugriff auf den Server vorübergehend gesperrt wurde.

Diese Aktion wird auf jeden Computer angewandt, von dem aus versucht wurde, ein infiziertes oder möglicherweise infiziertes Objekt auf den Server zu kopieren. Das Sperren eines Computers kann zusätzlich zu den Aktionen verwendet werden, die mit der Bearbeitung eines Objekts verbunden sind (Desinfektion und Löschen).

Diese Registerkarte enthält Angaben darüber, welche Computer gesperrt wurden, wann ein Computer gesperrt wurde (Datum und Uhrzeit) und wie viele Stunden verblieben sind, bis der Computer wieder freigegeben wird.



Zeit	Benutzer	Computer	Verbleibend
13.09.2006 12:11:56	Ivanov	TEST12345	01:58:46

Abbildung 44. Liste der gesperrten Benutzer

11.4. Allgemeine Informationen zum Programm

Allgemeine Informationen über das Programm finden Sie im Abschnitt **Service** des Hauptfensters (s. Abb. 45).

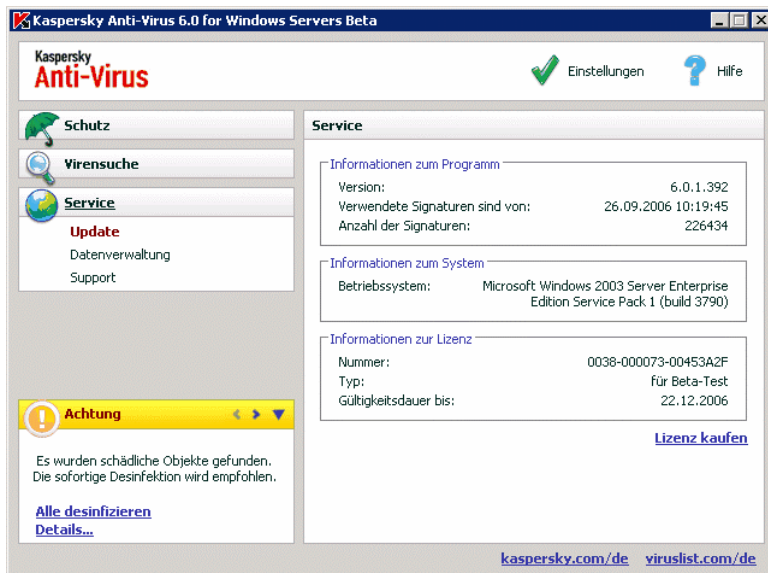


Abbildung 45. Informationen zu Programm, Programmlizenz und Betriebssystem

Die Informationen sind in drei Blöcke unterteilt:

- Der Abschnitt **Informationen zum Programm** informiert über Programmversion, Datum der letzten Aktualisierung und Anzahl der momentan bekannten Bedrohungen.
- Kurze Informationen über das auf Ihrem Computer installierte Betriebssystem befinden sich im Block **Informationen zum System**.
- Die wichtigsten Informationen über die von Ihnen erworbene Lizenz zur Nutzung von Kaspersky Anti-Virus befinden sich im Block **Informationen zur Lizenz**.

Bei einer Kontaktaufnahme mit dem technischen Support-Service von Kaspersky Lab benötigen Sie alle genannten Informationen (s. Pkt. 11.6 auf S. 140).

11.5. Lizenzverwaltung

Die Möglichkeit zur Nutzung von Kaspersky Anti-Virus wird durch das Vorhandensein eines *Lizenzschlüssels* bestimmt. Den Schlüssel erhalten Sie durch den Kauf des Produkts und er berechtigt Sie ab dem Tag der Installation des Schlüssels zur Nutzung des Programms.

Ist kein Lizenzschlüssel vorhanden und die Anwendung wurde nicht als Testversion aktiviert, dann funktioniert Kaspersky Anti-Virus im Modus, in dem nur ein einziges Update möglich ist. Danach können keine weiteren Aktualisierungen vorgenommen werden.

Wenn eine Testversion der Anwendung aktiviert wurde, stellt Kaspersky Anti-Virus nach Ablauf der Testdauer seine Funktion ein.

Mit Ablauf der Gültigkeitsdauer einer kommerziellen Lizenz bleibt die Funktionalität des Programms unter Ausnahme der Updatemöglichkeit für die Bedrohungssignaturen erhalten. Sie können Ihren Computer mit Hilfe der Untersuchungsaufgaben weiterhin auf das Vorhandensein von Viren untersuchen und die Schutzkomponenten verwenden, allerdings nur mit den Bedrohungssignaturen, die bei Ablauf der Lizenzgültigkeit aktuell waren. Demzufolge können wir Ihnen keinen hundertprozentigen Schutz vor neuen Viren garantieren, die nach dem Ende der Lizenzgültigkeit für das Programm auftreten.

Um eine Infektion Ihres Computers durch neue Viren zu verhindern, empfehlen wir Ihnen, die Lizenz für die Benutzung von Kaspersky Anti-Virus zu verlängern. Zwei Wochen vor Ablauf der Lizenzgültigkeit werden Sie vom Programm darüber benachrichtigt. Innerhalb dieser zwei Wochen wird bei jedem Programmstart eine entsprechende Meldung auf dem Bildschirm angezeigt.

Um die Lizenz zu verlängern, ist es erforderlich, einen neuen Lizenzschlüssel für die Anwendung zu kaufen und zu installieren oder einen Aktivierungscode anzugeben. Gehen Sie dazu folgendermaßen vor:

Setzen Sie sich mit der Firma in Verbindung, bei der Sie das Produkt gekauft haben, und erwerben Sie einen Lizenzschlüssel für die Nutzung des Programms oder einen Aktivierungscode.

oder:

Erwerben Sie direkt bei Kaspersky Lab den Lizenzschlüssel oder einen Aktivierungscode. Verwenden Sie dazu im Fenster zur Lizenzverwaltung den Hyperlink [Lizenz kaufen](#) (s. Abb. 46). Füllen Sie das entsprechende Formular auf der automatisch geöffneten Webseite aus. Nach Eingang der Bezahlung wird Ihnen per E-Mail an die im Bestellformular angegebene Adresse ein Link zugeschickt. Über diesen Link können Sie einen Lizenzschlüssel herunterladen oder einen Aktivierungscode für das Programm erhalten.

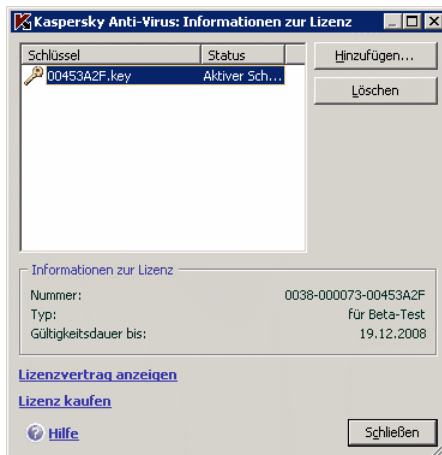


Abbildung 46. Informationen zur Lizenz

Informationen zum verwendeten Lizenzschlüssel befinden sich im Block **Informationen zur Lizenz** des Abschnitts **Service** im Hauptfenster der Anwendung. Um in das Fenster zur Lizenzverwaltung zu wechseln, klicken Sie mit der linken Maustaste an eine beliebige Stelle des Blocks. Im folgenden Fenster (s. Abb. 46) können Sie Informationen über den aktiven Schlüssel lesen, einen Schlüssel hinzufügen oder löschen.

Durch die Auswahl eines Schlüssels in der Liste des Blocks **Informationen zur Lizenz** werden Daten über Nummer, Typ und Gültigkeitsdatum der Lizenz angezeigt. Um einen neuen Lizenzschlüssel hinzuzufügen, verwenden Sie die Schaltfläche **Hinzufügen** und aktivieren Sie die Anwendung mit Hilfe des **Aktivierungsassistenten** (s. Pkt. 11.5 auf S. 138). Um einen Schlüssel aus der Liste zu löschen, klicken Sie auf die Schaltfläche **Löschen**.

Zur Anzeige der Bedingungen des Lizenzvertrags für die Benutzung des Produkts dient der Link [Lizenzvertrag anzeigen](#). Um mit Hilfe des Webformulars auf der Kaspersky-Lab-Seite eine Lizenz zu erwerben, klicken Sie auf den Link [Lizenz kaufen](#).

11.6. Technischer Support für Benutzer

Kaspersky Anti-Virus bietet Ihnen ein breites Spektrum von Möglichkeiten zur Lösung von Fragen und Problemen, die mit der Arbeit des Programms

verbunden sind. Alle entsprechenden Optionen finden Sie unter **Support** (s. Abb. 47) im Abschnitt **Service**.

Abhängig vom Problem, das Sie lösen möchten, bieten wir Ihnen an, folgende Leistungen des technischen Supports zu verwenden:

Benutzerforum. Diese Ressource ist ein spezieller Bereich der Kaspersky-Lab-Webseite und enthält Fragen, Kommentare und Vorschläge der Programmbenutzer. Sie können die wichtigsten Themen des Forums kennen lernen, eigene Beiträge über die Anwendung beisteuern oder Antworten auf Ihre Frage finden.

Um zu dieser Ressource zu gelangen, verwenden Sie den Link [Benutzerforum](#).

Wissensdatenbank. Auch diese Ressource ist eine separate Webseite von Kaspersky Lab und enthält Tipps des Technischen Support-Services über die Arbeit mit Kaspersky-Lab-Produkten und Antworten auf häufige Fragen. Versuchen Sie, über diese Ressource eine Antwort auf Ihre Frage oder die Lösung Ihres Problems zu finden.

Um technische Online-Unterstützung zu erhalten, verwenden Sie den Link [Wissensdatenbank](#).

Feedback über die Arbeit des Programms. Dieser Dienst dient dazu, um eine ausführliche Beurteilung der Programmarbeit abzugeben oder ein Problem bei der Programmarbeit zu beschreiben. Füllen Sie das spezielle Formular auf der Webseite des Herstellers aus und beschreiben Sie die Situation genau. Um ein Problem genau zu untersuchen, benötigen die Kaspersky-Lab-Spezialisten bestimmte Informationen über Ihr System. Sie können die Systemkonfiguration selbständig beschreiben oder eine Funktion zum automatischen Sammeln von Informationen über Ihren Computer verwenden.

Um zum Formular für die Programmbeurteilung bzw. zur Problembeschreibung zu gelangen, verwenden Sie den Link [Senden Sie uns einen Fehlerbericht oder Ihre Meinung](#).

Hilfe des technischen Supports. Wenn Sie bei der Arbeit mit Kaspersky Anti-Virus Hilfe benötigen, verwenden Sie den Link, der sich im Block **Lokaler Technischer Support-Service** befindet. Dadurch wird die Kaspersky-Lab-Webseite geöffnet, auf der Sie genaue Informationen darüber finden, wie Sie Hilfe von unseren Spezialisten erhalten können.

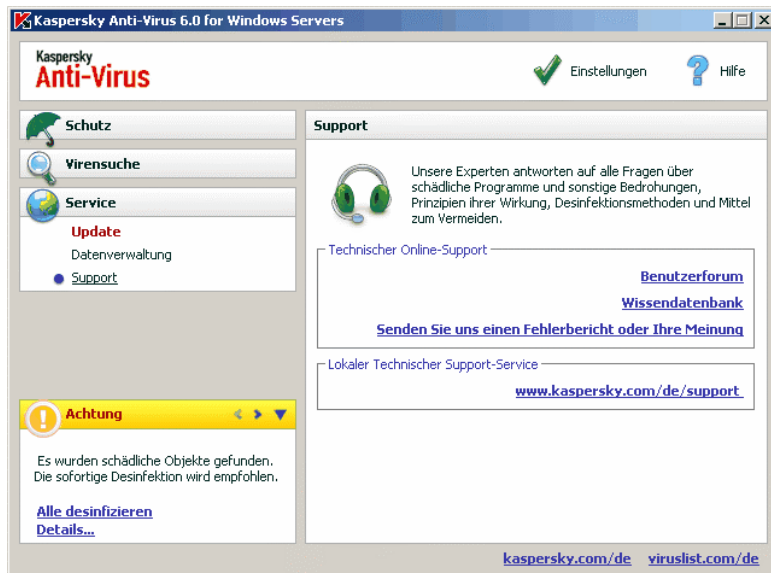


Abbildung 47. Informationen zum technischen Kundendienst

11.7. Konfiguration der Oberfläche von Kaspersky Anti-Virus

Kaspersky Anti-Virus bietet die Möglichkeit, das Aussehen des Programms zu verändern. Dazu können unterschiedliche grafische Elemente und Farbpaletten erstellt und verwendet werden. Zusätzlich besteht die Möglichkeit, aktive Elemente der Benutzeroberfläche anzupassen. Dazu zählen das Programmsymbol im Infobereich der Taskleiste und Popupmeldungen.

Gehen Sie folgendermaßen vor, um die Programmoberfläche anzupassen:

1. Öffnen Sie das Konfigurationsfenster von Kaspersky Anti-Virus über den Link Einstellungen des Hauptfensters.
2. Wählen Sie **Ansicht** im Abschnitt **Service** der Konfigurationsstruktur des Programms (s. Abb. 48).

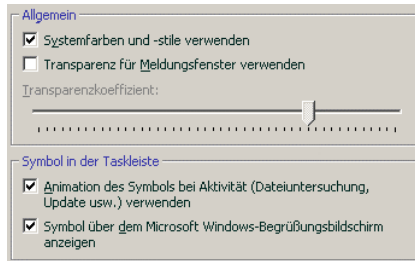


Abbildung 48. Einstellungen für die Programmoberfläche

Auf der rechten Seite des Konfigurationsfensters können Sie festlegen:

- ob der Schutzindikator von Kaspersky Anti-Virus beim Start des Betriebssystems angezeigt werden soll oder nicht.

Standardmäßig erscheint dieser Indikator in der rechten oberen Bildschirmcke, wenn das Programm gestartet wird. Er informiert darüber, dass der Schutz Ihres Computers vor jeder Art von Bedrohung aktiviert ist. Wenn Sie den Schutzindikator nicht verwenden möchten, deaktivieren Sie das Kontrollkästchen **Symbol über dem Microsoft Windows-Begrüßungsbildschirm anzeigen**.

- ob das Programmsymbol im Infobereich der Taskleiste animiert werden soll oder nicht.

In Abhängigkeit von der ausgeführten Programmaktion ändert sich das Symbol im Infobereich. Die Animation des Programmsymbols wird standardmäßig verwendet. Wenn Sie keine Animation wünschen, deaktivieren Sie das Kontrollkästchen **Animation des Symbols bei Aktivität verwenden**. In diesem Fall gibt das Symbol nur den Schutzstatus Ihres Computers wieder: Wenn der Schutz aktiviert ist, ist das Symbol farbig. Wenn der Schutz angehalten oder abgeschaltet wurde, nimmt das Symbol graue Farbe an.

- Transparenzstufe der Popupmeldungen.

Alle Operationen von Kaspersky Anti-Virus, die Ihre sofortige Aufmerksamkeit oder Entscheidung erfordern, besitzen das Aussehen einer Popupmeldung über dem Programmsymbol im Infobereich. Die Meldungsfenster sind halbtransparent, damit sie nicht bei der Arbeit stören. Wenn der Mauscursor auf das Meldungsfenster geführt wird, wird die Transparenz aufgehoben. Sie können die Transparenzstufe solcher Meldungen ändern. Verschieben Sie dazu den Zeiger auf der Skala **Transparenzkoeffizient** an die gewünschte Position. Deaktivieren Sie das Kontrollkästchen **Transparenz für Meldungsfenster verwenden**, wenn die Meldungen ohne Transparenz angezeigt werden sollen.

- Verwendung eigener grafischer Elemente und Farbpaletten auf der Programmoberfläche.

Alle auf der Oberfläche von Kaspersky Anti-Virus verwendeten Farben, Schriften, Piktogramme und Texte können verändert werden. Sie können eine individuelle grafische Oberfläche für das Programm erstellen und es in einer anderen Sprache lokalisieren. Um eine grafische Oberfläche zu verbinden, geben Sie das Verzeichnis mit ihren Parametern im Feld **Ordner mit Beschreibung der grafischen Oberfläche** an. Verwenden Sie zur Auswahl des Verzeichnisses die Schaltfläche **Durchsuchen**.

Standardmäßig werden für die grafische Programmoberfläche die Systemfarben und -stile verwendet. Sie können diese verwerfen. Deaktivieren Sie dazu das Kontrollkästchen **Systemfarben und -stile verwenden**. In diesem Fall werden die Schemen verwendet, die Sie bei der Konfiguration des Bildschirmdesigns angegeben haben.

Beachten Sie, dass Änderungen der Interfaceparameter von Kaspersky Anti-Virus beim Wiederherstellen der Standardeinstellungen oder bei der Deinstallation der Anwendung nicht gespeichert werden.

11.8. Verwendung zusätzlicher Dienste

Kaspersky Anti-Virus bietet Ihnen an, folgende zusätzlichen Dienste zu verwenden:

- Benachrichtigung des Benutzers per E-Mail über das Eintreten bestimmter Ereignisse bei der Arbeit des Programms.
- Selbstschutz von Kaspersky Anti-Virus vor dem Beenden, Löschen und Verändern von Modulen, sowie Kennwortschutz für den Zugriff auf das Programm.
- Lösen von Kompatibilitätsproblemen mit Kaspersky Anti-Virus 6.0 bei der Arbeit mit anderen Anwendungen.

Um zur Konfiguration der genannten Dienste zu gelangen,

1. Öffnen Sie das Konfigurationsfenster des Programms über den Link [Einstellungen](#) des Hauptfensters.
2. Wählen Sie den Punkt **Service** in der Konfigurationsstruktur.

Auf der rechten Seite können Sie festlegen, ob die Zusatzdienste bei der Programmarbeit verwendet werden sollen oder nicht.

11.8.1. Benachrichtigungen über die Ereignisse von Kaspersky Anti-Virus

Bei der Arbeit von Kaspersky Anti-Virus treten unterschiedliche Ereignisse ein. Sie können informativen Charakter besitzen oder wichtige Informationen enthalten. Ein Ereignis kann beispielsweise über die erfolgreiche Aktualisierung des Programms informieren oder einen Fehler bei der Arbeit einer bestimmten Komponente festhalten, der dringend behoben werden muss.

Um sich über die Ereignisse bei der Arbeit von Kaspersky Anti-Virus informieren zu lassen, können Sie den Dienst für Benachrichtigungen verwenden.

Die Benachrichtigungen können durch eine der folgenden Methoden erfolgen:

- Popupmeldungen über dem Programmsymbol im Infobereich der Taskleiste
- Tonsignale
- E-Mail-Nachrichten
- Protokollieren von Informationen im Ereignisbericht

Um diesen Dienst zu verwenden,

1. Aktivieren Sie das Kontrollkästchen **Ereignisbenachrichtigung aktivieren** im Block **Interaktion mit dem Benutzer** (s. Abb. 49).



Abbildung 49. Aktivieren des Benachrichtigungsmodus

2. Legen Sie die Typen der Ereignisse von Kaspersky Anti-Virus fest, über deren Eintreten Sie benachrichtigt werden möchten, und wählen Sie eine Methode zum Senden der Benachrichtigungen (s. Pkt. 11.8.1.1 auf S. 146).
3. Passen Sie die Einstellungen für das Senden von Benachrichtigungen per E-Mail an, wenn Sie diese Benachrichtigungsmethode wünschen (s. Pkt. 11.8.1.2 auf S. 147).

11.8.1.1. Ereignistypen und Methoden zum Senden von Benachrichtigungen

Bei der Arbeit von Kaspersky Anti-Virus treten Ereignisse der folgenden Typen auf:

Kritische Ereignisse – Ereignisse mit kritischer Priorität. Es wird ausdrücklich empfohlen, sich über solche Ereignisse benachrichtigen zu lassen, weil sie auf Probleme bei der Arbeit des Programms oder auf Schwachstellen im Schutz Ihres Computers hinweisen. Beispiele: *Die Bedrohungssignaturen sind beschädigt* oder *Die Lizenzgültigkeit ist abgelaufen*.

Funktionsstörung – Ereignisse, die zur Funktionsunfähigkeit der Anwendung führen. Beispielsweise das Fehlen einer Lizenz und der Bedrohungssignaturen.

Wichtige Ereignisse – Ereignisse, die unbedingt beachtet werden müssen, weil Sie wichtige Situationen bei der Programmarbeit wiedergeben. Beispiele: *Alle Schutzkomponenten sind deaktiviert* oder *Der Computer wurde lange nicht untersucht*.

Informative Ereignisse – Ereignisse mit informativem Charakter, die in der Regel keine wichtigen Informationen enthalten. Beispiele: *Alle gefährlichen Objekte wurden neutralisiert*.

Um festzulegen, über welche Ereignisse und auf welche Weise Sie benachrichtigt werden möchten:

1. Klicken Sie auf den Link Einstellungen im Programmhauptfenster.
2. Wählen Sie im Konfigurationsfenster des Programms den Abschnitt **Service**, aktivieren Sie das Kontrollkästchen **Ereignisbenachrichtigung aktivieren** und wechseln Sie mit der Schaltfläche **Erweitert** zu den ausführlichen Einstellungen.

Im folgenden Fenster **Benachrichtigungseinstellungen** (s. Abb. Abbildung 50) können Sie folgende Benachrichtigungsmethoden für die oben genannten Ereignisse anpassen:

- *Popupmeldung* über dem Programmsymbol im Infobereich. Die Meldung enthält Informationen über das eingetretene Ereignis.

Um diesen Typ der Benachrichtigung zu verwenden, aktivieren Sie das Kontrollkästchen in der Spalte **Anzeige** gegenüber dem Ereignis, über das Sie benachrichtigt werden möchten.

- *Tonsignale*.

Wenn Sie möchten, dass die Benachrichtigung von einem Audiosignal begleitet wird, aktivieren Sie das Kontrollkästchen in der Spalte **Ton** neben dem Ereignis.

- *Benachrichtigung per E-Mail.*

Um diesen Typ der Benachrichtigung zu verwenden, aktivieren Sie das Kontrollkästchen in der Spalte **E-Mail** gegenüber dem Ereignis, über das Sie benachrichtigt werden möchten, und passen Sie die Parameter für das Senden von Benachrichtigungen an (s. Pkt. 11.8.1.2 auf S. 147).

- *Protokollieren von Informationen im Ereignisbericht.*

Damit Informationen über das Eintreten eines bestimmten Ereignisses im Bericht protokolliert werden, aktivieren Sie das Kontrollkästchen in der Spalte **Bericht** gegenüber dem Ereignis und passen Sie die Parameter für den Ereignisbericht (s. Pkt. 11.8.1.3 auf S. 149) an.

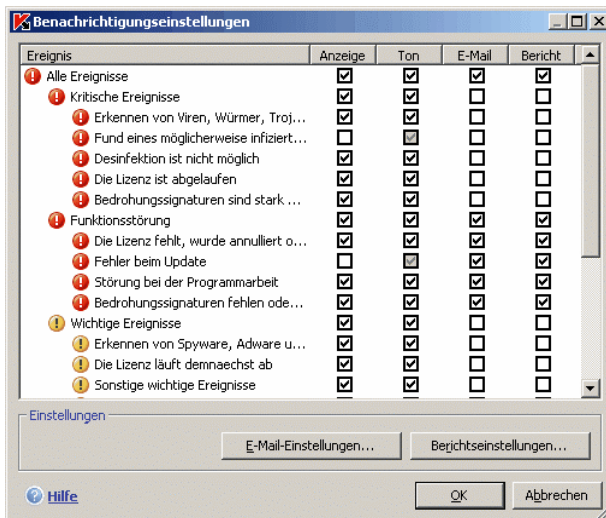


Abbildung 50. Ereignisse bei der Programmarbeit und entsprechende Benachrichtigungsmethoden

11.8.1.2. Konfiguration des Sendens von Benachrichtigungen per E-Mail

Nachdem Sie die Ereignisse gewählt haben (s. Pkt. 11.8.1.1 auf S. 146), über deren Eintreten Sie per E-Mail benachrichtigt werden möchten, müssen Sie die folgenden Einstellungen für das Senden der Benachrichtigungen vornehmen:

1. Öffnen Sie das Konfigurationsfenster des Programms über den Link **Einstellungen** des Hauptfensters.
2. Wählen Sie den Punkt **Service** in der Konfigurationsstruktur.
3. Klicken Sie im Block **Interaktion mit dem Benutzer** auf der rechten Seite des Fensters auf die Schaltfläche **Erweitert**.
4. Aktivieren Sie auf der Registerkarte **Berichtseinstellungen** in der Spalte **E-Mail** die Kontrollkästchen für die Ereignisse, bei deren Eintreten eine E-Mail-Benachrichtigung gesendet werden soll.
5. Legen Sie im Fenster, das mit der Schaltfläche **E-Mail-Einstellungen** geöffnet wird, folgende Parameter für das Senden von E-Mail-Benachrichtigungen fest:
 - Geben Sie im Block **Benachrichtigungsabsender** die Parameter des Absenders der Benachrichtigungen an.

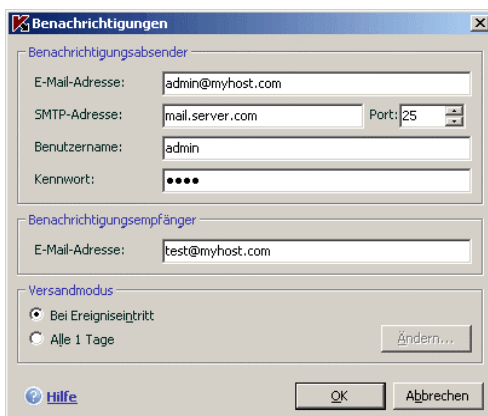


Abbildung 51. Einstellungen für E-Mail-Benachrichtigung

- Geben Sie im Block **Benachrichtigungsempfänger** die E-Mail-Adresse an, an welche die Benachrichtigungen geschickt werden sollen.
- Geben Sie im Block **Versandmodus** den Modus zum Senden der Benachrichtigungen per E-Mail an. Damit das Programm die Nachricht beim tatsächlichen Eintreten eines Ereignisses abschickt, wählen Sie **Bei Ereigniseintritt**. Erstellen Sie zur Benachrichtigung über Ereignisse nach einem bestimmten Zeitraum einen Zeitplan für das Senden von Nachrichten. Klicken Sie dazu auf die Schaltfläche **Ändern**. Standardmäßig erfolgt die Benachrichtigung täglich.

11.8.1.3. Parameter des Ereignisberichts

Um die Parameter des Ereignisberichts anzupassen:

1. Öffnen Sie im Hauptfenster mit dem Link Einstellungen das Konfigurationsfenster des Programms.
2. Wählen Sie in der Konfigurationsstruktur den Punkt **Service**.
3. Klicken Sie auf der rechten Seite des Fensters im Block **Interaktion mit dem Benutzer** auf die Schaltfläche **Erweitert**.

Wählen Sie im Fenster **Benachrichtigungseinstellungen** für das gewünschte Ereignis die Option zur Protokollierung im Bericht und klicken Sie auf die Schaltfläche **Berichtseinstellungen**.

Kaspersky Anti-Virus bietet die Möglichkeit, Informationen über Ereignisse, die bei der Arbeit der Anwendung eintreten, im allgemeinen Ereignisbericht von Microsoft Windows (**Anwendung**) oder in einem separaten Ereignisbericht von Kaspersky Anti-Virus (**Kaspersky Event Log**) aufzuzeichnen.

Zur Anzeige der Berichte dient das Microsoft Windows-Standardfenster **Ereignisanzeige**, das mit Hilfe des folgenden Befehls geöffnet wird: **Start** → **Einstellungen** → **Systemsteuerung** → **Verwaltung** → **Ereignisanzeige**.

11.8.2. Selbstschutz und Zugriffsbeschränkung für das Programm

Kaspersky Anti-Virus ist ein Programm, das den Computer vor schädlichen Programmen schützt, und wird dadurch selbst zu einem Ziel für schädliche Programme, die versuchen, die Arbeit des Programms zu blockieren oder es sogar vom Computer zu löschen.

Außerdem kann ein PC von verschiedenen Benutzern verwendet werden, deren Fertigkeiten im Umgang mit Computern möglicherweise nicht ausreichend sind. Der ungehinderte Zugriff auf das Programm und dessen Einstellungen kann das Sicherheitsniveau des Computers stark einschränken.

Um die Stabilität des Sicherheitssystems Ihres Computers zu gewährleisten, verfügt das Programm über Mechanismen zum Selbstschutz, zum Schutz vor externem Zugriff und zum Kennwortschutz für den Programmmzugriff.

Um die Selbstschutzmechanismen für das Programm zu aktivieren:

1. Öffnen Sie das Konfigurationsfenster des Programms mit dem Link Einstellungen des Hauptfensters.
2. Wählen Sie in der Konfigurationsstruktur den Punkt **Service**.

Nehmen Sie im Block **Selbstschutz** (s. Abb. 52) die entsprechenden Einstellungen vor:

- Selbstschutz aktivieren.** Wenn dieses Kontrollkästchen aktiviert ist, wird der Mechanismus zum Schutz der Anwendung vor dem Verändern oder Löschen von eigenen Dateien auf der Festplatte, Prozessen im Arbeitsspeicher und Einträgen in der Systemregistrierung wirksam.
- Externe Dienststeuerung verbieten.** Wenn dieses Kontrollkästchen aktiviert ist, wird jeder Versuch zur Fernsteuerung von Diensten der Anwendung blockiert.

Wird versucht, eine der oben genannten Aktionen auszuführen, dann erscheint eine Meldung über dem Programmsymbol im Infobereich der Taskleiste (falls der Benachrichtigungsdienst vom Benutzer nicht deaktiviert wurde).

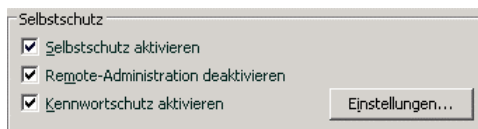


Abbildung 52. Einstellungen für den Programmschutz

Um den Zugriff auf das Programm mit Hilfe eines Kennworts zu schützen, aktivieren Sie das Kontrollkästchen **Kennwortschutz aktivieren** und geben Sie im Fenster, das mit der Schaltfläche **Einstellungen** geöffnet wird, das Kennwort und den Bereich an, für den die Zugriffsbeschränkung gelten soll (s. Abb. 53).

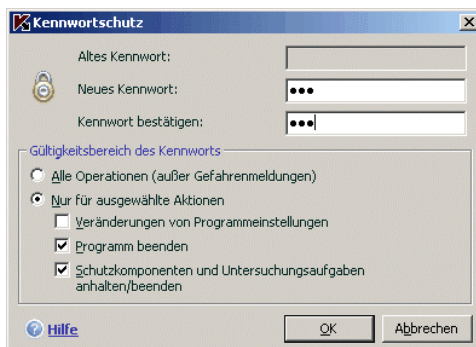


Abbildung 53. Einstellungen für den Kennwortschutz des Programms

Sie können entweder alle Operationen mit dem Programm blockieren (unter Ausnahme der Arbeit mit Meldungen über den Fund gefährlicher Objekte) oder das Ausführen folgender Aktionen untersagen:

- Die Einstellungen für die Arbeit des Programms ändern.
- Die Arbeit von Kaspersky Anti-Virus beenden.
- Den Schutz Ihres Computers deaktivieren oder vorübergehend anhalten.

Jede der oben genannten Aktionen führt zu einer Verringerung des Schutzniveaus Ihres Computers. Deshalb sollten Sie festlegen, welche Personen zur Arbeit mit dem Server berechtigt sein sollen.

Wenn ein Benutzer versucht, die von Ihnen festgelegten Aktionen auf dem Server auszuführen, wird die Anwendung nun immer das Kennwort abfragen.

11.8.3. Lösen von Kompatibilitätsproblemen von Kaspersky Anti-Virus mit anderen Anwendungen

In einigen Fällen können bei der Verwendung von Kaspersky Anti-Virus Konflikte bei der Arbeit mit Anwendungen, die auf dem Computer installiert sind, auftreten. Das steht mit dem in diese Programme integrierten Selbstschutzmechanismus in Verbindung, der reagiert, wenn Kaspersky Anti-Virus versucht, auf die Programme zuzugreifen. Zu diesen Programmen gehören beispielsweise das Plug-in Authentica des Programms Adobe Reader, das der Zugriffskontrolle für Dokumente im pdf-Format dient, das Programm zur Steuerung von Mobiltelefonen Oxygen Phone Manager II, sowie einige Arten von Spielen, die über einen Crackschutz verfügen.

Um dieses Problem zu lösen, aktivieren Sie das Kontrollkästchen **Kompatibilität mit dem Selbstschutz von Anwendungen** im Abschnitt **Service** des Konfigurationsfensters der Anwendung. Damit die Änderungen dieses Parameters wirksam werden, ist der Neustart des Betriebssystems erforderlich.

11.9. Export/Import der Einstellungen von Kaspersky Anti-Virus

Kaspersky Anti-Virus bietet Ihnen die Möglichkeit zum Exportieren und Importieren seiner Programmeinstellungen.

Um die aktuellen Programmeinstellungen zu exportieren,

1. Öffnen Sie das Hauptfenster von Kaspersky Anti-Virus.
2. Wählen Sie den Abschnitt **Service** und klicken Sie auf den Link Einstellungen.
3. Klicken Sie im Block **Konfigurationsverwaltung** auf die Schaltfläche **Speichern**.
4. Geben Sie Name und Pfad der Konfigurationsdatei an.

Um die Programmeinstellungen aus einer Konfigurationsdatei zu importieren,

1. Öffnen Sie das Hauptfenster von Kaspersky Anti-Virus.
2. Wählen Sie den Abschnitt **Service** und klicken Sie auf den Link Einstellungen.
3. Klicken Sie auf die Schaltfläche **Laden** und wählen Sie die Datei, aus der Sie die Parameter für Kaspersky Anti-Virus importieren möchten.

11.10. Wiederherstellen der Standardeinstellungen

Sie können jederzeit zu den empfohlenen Programmeinstellungen zurückkehren. Diese gelten als optimal und werden von den Kaspersky-Lab-Spezialisten empfohlen. Die Wiederherstellung der Einstellungen erfolgt mit Hilfe des Konfigurationsassistenten.

Um die Schutzeinstellungen wiederherzustellen,

1. Wählen Sie den Abschnitt **Service** und wechseln sie mit dem Link Einstellungen in das Konfigurationsfenster des Programms.
2. Klicken Sie im Abschnitt **Konfigurationsverwaltung** auf die Schaltfläche **Wiederherstellen**.

Im folgenden Fenster können Sie angeben, welche Parameter bei der Wiederherstellung der empfohlenen Sicherheitsstufe beibehalten werden und für welche Komponenten diese gelten sollen.

In der Grundeinstellung werden alle in der Liste enthaltenen Parameter gespeichert (die entsprechenden Kontrollkästchen sind deaktiviert). Wenn bestimmte Parameter nicht beibehalten werden sollen, aktivieren Sie die entsprechenden Kontrollkästchen.

Klicken Sie zum Abschluss der Konfiguration auf die Schaltfläche **Weiter**. Der Konfigurationsassistent wird gestartet (s. Pkt. 3.2 auf S. 26). Folgen Sie den Anweisungen.

Nach dem Abschluss des Assistenten wird für Datei-Anti-Virus die Sicherheitsstufe **Empfohlen** eingestellt, wobei die von Ihnen zum Speichern gewählten Parameter berücksichtigt werden. Zusätzlich werden die Einstellungen übernommen, die Sie während der Arbeit des Assistenten vorgenommen haben.

KAPITEL 12. VERWALTUNG DER ANWENDUNG ÜBER KASPERSKY ADMINISTRATION KIT

Kaspersky Administration Kit ist ein System zur zentralisierten Lösung der wichtigsten Verwaltungsaufgaben, die der Verwaltung des Sicherheitssystems eines Firmencomputernetzwerks dienen, das auf Anwendungen basiert, die zu den Produkten Kaspersky Anti-Virus Business Optimal und Kaspersky Corporate Suite gehören.

Kaspersky Anti-Virus 6.0 for Windows Servers ist eines der Produkte von Kaspersky Lab, die über die eigene Anwendungsoberfläche, über die Befehlszeile (diese Methoden werden weiter oben in diesem Handbuch beschrieben) oder mit Hilfe der Anwendung Kaspersky Administration Kit (wenn der Computer in ein System zur zentralisierten Remoteverwaltung integriert ist) verwaltet werden können.

Gehen Sie folgendermaßen vor, um Kaspersky Anti-Virus 6.0 for Windows Servers über Kaspersky Administration Kit zu steuern:

- Richten Sie im Netzwerk einen *Administrationsserver* ein. Installieren Sie die *Administrationskonsole* am Arbeitsplatz des Administrators (Details siehe Administratorenhandbuch zur Einrichtung von "Kaspersky Administration Kit").
- Richten Sie Kaspersky Anti-Virus 6.0 for Windows Servers und den *Administrationsagenten* (der zum Lieferumfang von Kaspersky Administration Kit gehört) auf den Dateiservern des Netzwerks ein. Details über die Remote-Installation des Pakets Kaspersky Anti-Virus 6.0 auf Netzwerkcomputern finden Sie im Administratorenhandbuch zur Einrichtung von "Kaspersky Administration Kit".

Beenden Sie die Arbeit der Administrationskonsole, bevor Sie das Upgrade des Steuerungs-Plug-ins für Kaspersky Anti-Virus über Kaspersky Administration Kit vornehmen.

Die Verwaltung der Anwendung über Kaspersky Administration Kit erfolgt mit der Administrationskonsole (s. Abb. 54). Sie stellt ein standardmäßiges **Interface** dar, **das in MMC integriert ist**, und erlaubt dem Administrator folgende Funktionen auszuführen:

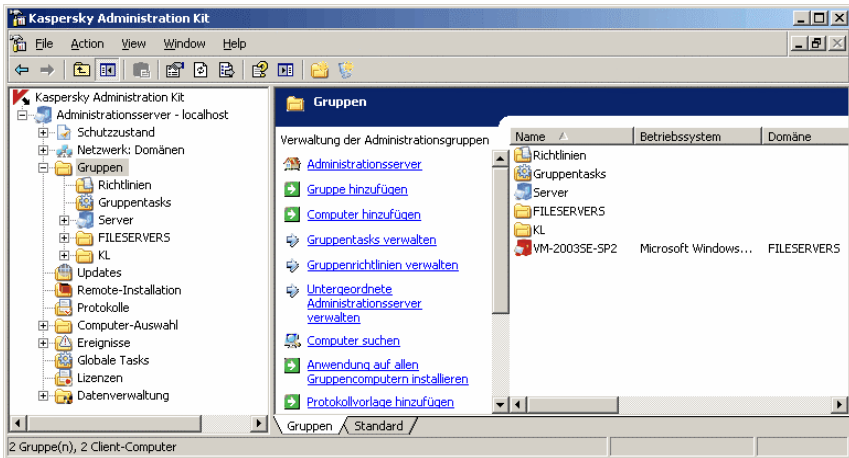


Abbildung 54. Administrationskonsole von Kaspersky Administration Kit

- entfernte Installation von Kaspersky Anti-Virus 6.0 for Windows Servers und des *Administrationsagenten* auf den Netzwerkcomputern.
- entfernte Konfiguration von Kaspersky Anti-Virus 6.0 auf den Netzwerkcomputern.
- Aktualisierung der Bedrohungssignaturen und der Module von Kaspersky Anti-Virus.
- Verwaltung der Lizenzen für Kaspersky Anti-Virus auf den Netzwerkcomputern.
- Anzeige von Informationen über die Arbeit der Anwendung auf den Client-Computern.

Bei der Arbeit über Kaspersky Administration Kit verwaltet der Administrator die Anwendung, indem er Richtlinienparameter, Aufgabenparameter und Anwendungsparameter festlegt.

Anwendungsparameter sind eine Auswahl von Funktionsparametern der Anwendung, zu denen generelle Schutzparameter, Parameter für den Backup-Speicher und die Quarantäne, Parameter für die Berichtsführung u.a. gehören.

Eine **Aufgabe** ist eine benannte Aktion, die von der Anwendung ausgeführt werden kann. Entsprechend der Funktionen werden die Aufgaben für die Anwendung Kaspersky Anti-Virus for Windows Servers in Typen unterteilt (Aufgabe zur Virensuche, Aufgabe zum Update der Anwendung, Aufgabe zum Rollback von Updates, Aufgabe zur Installation eines Lizenzschlüssels). Jeder konkreten Aufgabe entspricht bei ihrer Ausführung eine Auswahl von Parametern für die Arbeit von Kaspersky Anti-Virus – die *Aufgabenparameter*.

Eine Besonderheit der zentralisierten Verwaltung besteht darin, dass die Netzwerkcomputer in Gruppen organisiert sind, die durch das Erstellen und Festlegen von Gruppenrichtlinien verwaltet werden.

Eine **Richtlinie** ist eine Auswahl von Parametern, die für die Arbeit der Anwendung auf den Computern einer Gruppe des logischen Netzwerks gelten, sowie eine Auswahl von Beschränkungen für das Ändern dieser Parameter, die sich auf die Konfiguration der Anwendung oder einer Aufgabe auf einem einzelnen Client-Computer beziehen.

Eine Richtlinie umfasst die Parameter zur vollständigen Konfiguration der gesamten Anwendungsfunktionalität. Zu einer Richtlinie gehören die Anwendungsparameter und die Parameter aller Aufgabentypen, unter Ausnahme spezifischer Parameter für einen konkreten Aufgabentyp.

12.1. Anwendung verwalten

Kaspersky Administration Kit bietet die Möglichkeit, den Start und das Beenden von Kaspersky Anti-Virus 6.0 auf einem einzelnen Client-Computer entfernt zu verwalten. Außerdem kann die Konfiguration allgemeiner Funktionsparameter der Anwendung entfernt verwaltet werden. Dazu zählen beispielsweise das Aktivieren/Deaktivieren des Computerschutzes und die Konfiguration der Parameter für Backup- und Quarantänespeicher und der Parameter für die Berichtsführung.

Zur Verwaltung der Anwendungsparameter:

1. Wählen Sie im Ordner **Gruppen** (s. Abb. 54) den Ordner mit dem Namen der Gruppe aus, zu welcher der Client-Computer gehört.
2. Wählen Sie im Detailfenster den Computer aus, für den die Anwendungsparameter geändert werden sollen, und verwenden Sie den Befehl **Anwendungen** im Kontextmenü oder den entsprechenden Punkt im Menü **Aktion**.
3. Im Eigenschaften-Fenster des Client-Computers auf der Registerkarte **Anwendungen** (s. Abb. 55) wird eine vollständige Liste aller Kaspersky-Lab-Anwendungen angezeigt, die auf dem Client-Computer installiert sind.

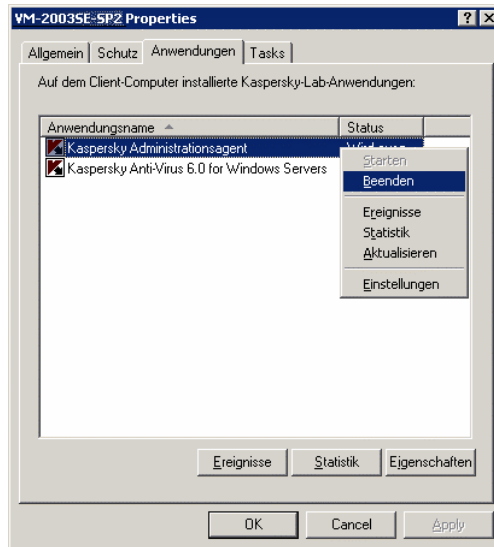


Abbildung 55. Liste der Kaspersky-Lab-Anwendungen

Unter der Liste der Anwendungen befinden sich folgende Schaltflächen, mit deren Hilfe sie folgende Aktionen vornehmen können:

- eine Liste der Ereignisse anzeigen, die bei der Arbeit der Anwendung auf dem Client-Computer eingetreten sind und auf dem Administrationsserver registriert wurden.
- aktuelle statistische Informationen über die Arbeit der Anwendung anzeigen.
- die Parameter der Anwendung anpassen (s. Pkt. 12.1.2 auf S.158).

12.1.1. Anwendung starten / beenden

Der Start und das Beenden von Kaspersky Anti-Virus auf einem entfernten Client-Computer wird mit Hilfe der entsprechenden Befehle im Eigenschaften-Fenster des Computers verwaltet (s. Abb. 55).

Die entsprechenden Aktionen können auch mit Hilfe der Schaltflächen **Starten / Beenden** aus dem Konfigurationsfenster für die Anwendungsparameter auf der Registerkarte **Allgemein** ausgeführt werden (s. Abb. 56).

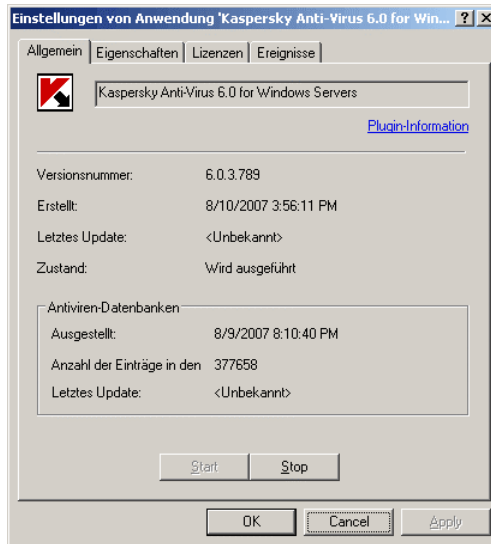


Abbildung 56. Parameter von Kaspersky Anti-Virus anpassen.
Registerkarte **Allgemein**

Der obere Bereich des Fensters enthält folgende Angaben: Name der installierten Anwendung, Informationen über Version, Installationsdatum und Status der Anwendung (ob die Anwendung auf dem lokalen Computer gestartet oder beendet wurde), Informationen über den Zustand der Datenbanken mit den Bedrohungssignaturen.

12.1.2. Anwendungsparameter anpassen

Um die Funktionsparameter der Anwendung anzuzeigen oder zu ändern:

1. Öffnen Sie das Eigenschaften-Fenster des Client-Computers auf der Registerkarte **Anwendungen** (s. Abb. 55).
2. Wählen Sie die Anwendung **Kaspersky Anti-Virus 6.0 for Windows Servers** aus und verwenden Sie die Schaltfläche **Eigenschaften**. Dadurch wird das Konfigurationsfenster für die Anwendungsparameter geöffnet.

Alle Registerkarten (außer der Registerkarte **Einstellungen**) sind für die Anwendung Kaspersky Administration Kit 6.0 standardmäßig und werden im entsprechenden Administratorenhandbuch ausführlich beschrieben.

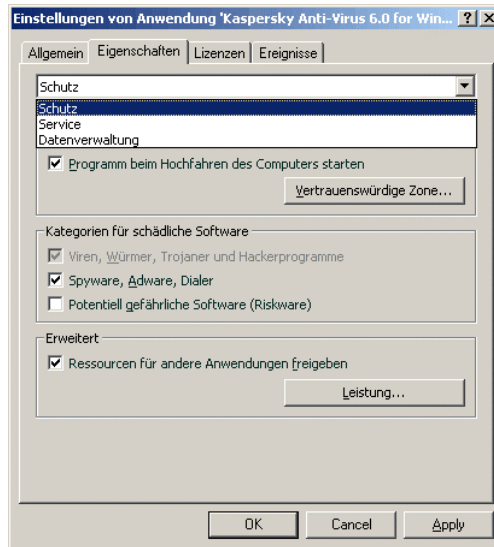


Abbildung 57. Parameter von Kaspersky Anti-Virus anpassen.
Registerkarte **Einstellungen**

Wenn für eine Anwendung eine Richtlinie erstellt wurde (s. Pkt. 12.3.1 auf S. 168), in der das Verändern bestimmter Parameter verboten ist, dann stehen diese bei der Konfiguration der Anwendungsparameter nicht für Änderungen zur Verfügung.

Auf der Registerkarte **Einstellungen** können generelle und dienstbezogene Schutzparameter von Kaspersky Anti-Virus, Parameter für den Backup-Speicher, die Quarantäne und den Dienst zur Berichtsführung angepasst werden. Wählen Sie dazu aus der Dropdown-Liste im oberen Bereich des Fensters den gewünschten Wert und nehmen Sie die Einstellungen vor.

Schutz

In diesem Fenster können Sie:

- den Echtzeitschutz des Computers aktivieren / deaktivieren (s. Pkt. 6.1 auf S. 54).
- den automatischen Start der Anwendung beim Hochfahren des Computers festlegen (s. Pkt. 6.1.5 auf S. 58).
- die vertrauenswürdige Zone und eine Liste der Ausnahmen erstellen (s. Pkt. 6.3 auf S. 60).
- die Kategorien der schädlichen Programme auswählen, die von der

Anwendung kontrolliert werden sollen (s. Pkt. 6.2 auf S. 59).

- die Leistungsparameter der Anwendung und die Parameter für die Multiprozessoren-Konfiguration einstellen (s. Pkt. 6.7 auf S. 6.7).

Service

Im Fenster zur Konfiguration der Dienstparameter können Sie:

- den Dienst zum Empfang von Benachrichtigungen über eingetretene Ereignisse anpassen (s. Pkt. 11.8.1 auf S. 145).
- den Dienst für den Selbstschutz der Anwendung anpassen und den Zugriff auf die Anwendungseinstellungen mit Hilfe eines Kennworts beschränken (s. Pkt. 11.8.2 auf S. 149).
- das Aussehen der Anwendung anpassen (s. Pkt. 12.3.1 auf S. 168).
- Parameter für die Kompatibilität von Kaspersky Anti-Virus mit anderen Anwendungen anpassen (s. Pkt. 11.8.3 auf S. 151).

Datenverwaltung

In diesem Fenster können Sie die Parameter für das Erstellen der Berichtsstatistik über die Arbeit der Anwendung anpassen (s. Pkt. 11.3.1 auf S. 132) und die Speicherdauer für Dateien im Backup-Speicher (s. Pkt. 11.2.2 auf S. 129) und in der Quarantäne (s. Pkt. 11.1.2 auf S. 126) festlegen.

12.1.3. Spezifische Parameter anpassen

Bei der Verwaltung von Kaspersky Anti-Virus über Kaspersky Administration Kit können Sie den Modus für die Interaktion der Anwendung mit dem Benutzer aktivieren / deaktivieren und die Informationen über die technische Unterstützung ändern. Dazu:

1. Öffnen Sie das Eigenschaften-Fenster des Client-Computers auf der Registerkarte **Anwendungen** (s. Abb. 55).
2. Wählen Sie die Anwendung **Kaspersky Anti-Virus 6.0 for Windows Servers** aus und verwenden Sie die Schaltfläche **Eigenschaften**. Dadurch wird das Konfigurationsfenster für die Anwendungsparameter geöffnet (s. Abb. 57). Wählen Sie aus der Dropdown-Liste im oberen Teil des Fensters den Wert **Service** aus.

Auf der Registerkarte **Service** im Block **Ansicht** können Sie den interaktiven Funktionsmodus von Kaspersky Anti-Virus auf dem entfernten Computer aktivieren / deaktivieren. Dazu zählen die Anzeige des Symbols von Kaspersky Anti-Virus in der Taskleiste sowie die Anzeige von Meldungen über das Eintreten

von Ereignissen bei der Arbeit der Anwendung (beispielsweise über den Fund eines gefährlichen Objekts).

Wenn das Kontrollkästchen **Interaktion mit Interface erlauben** aktiviert ist, sind für den Benutzer, der auf dem entfernten Computer arbeitet, das Symbol von Kaspersky Anti-Virus und die Popupmeldungen sichtbar. Außerdem besitzt er die Möglichkeit, in den Meldungsfenstern, die über das Eintreten eines bestimmten Ereignisses informieren, über die weiteren Aktionen zu entscheiden. Um den interaktiven Funktionsmodus der Anwendung auszuschalten, deaktivieren Sie das Kontrollkästchen.

Im Fenster, das mit der Schaltfläche **Einstellungen** geöffnet wird, können Sie auf der Registerkarte **Individuelle Support-Informationen** die Informationen über die technische Unterstützung für Benutzer ändern. Diese Informationen werden im Abschnitt **Service** unter dem Punkt **Support** von Kaspersky Anti-Virus angezeigt (s. Abb. 47).

Um die Informationen zu ändern, geben Sie im oberen Feld den gewünschten Text über den angebotenen Support ein. Im unteren Feld können Sie die Hyperlinks anpassen, die im Block **Technischer Online-Support** angezeigt werden, die bei Auswahl des Abschnitts **Service** im Punkt **Support** angezeigt werden.

Die Liste wird mit Hilfe der Schaltflächen **Hinzufügen**, **Ändern** und **Löschen** bearbeitet. Kaspersky Anti-Virus fügt einen neuen Link am Anfang der Liste hinzu. Die Reihenfolge der Links kann mit Hilfe der Schaltflächen **Aufwärts/Abwärts** geändert werden.

Wenn das Fenster keine Daten enthält, können die standardmäßig angegebenen Informationen über den technischen Support nicht geändert werden.

12.2. Aufgaben verwalten

Dieser Abschnitt enthält Informationen über die Verwaltung von Aufgaben für Kaspersky Anti-Virus 6.0 for Windows Servers. Detaillierte Angaben zur Konzeption der Aufgabenverwaltung über Kaspersky Administration Kit finden Sie im Administratorenhandbuch des Produkts.

Bei der Installation der Anwendung wird für jeden Computer eine Auswahl von Systemaufgaben erstellt. Zu dieser Liste (s. Abb. 58) zählen Echtzeitschutzaufgaben (Datei-Anti-Virus), Aufgaben zur Virensuche (Arbeitsplatz untersuchen, Autostart-Objekte untersuchen, Kritische Bereiche untersuchen) und Update-Aufgaben (Bedrohungssignaturen und Programm-Module aktualisieren, Update rückgängig machen, Updates verteilen).

Der Start von Systemaufgaben kann verwaltet und ihre Parameter können

angepasst werden. Das Löschen dieser Aufgaben ist nicht möglich.

Außerdem können Sie eigene Aufgaben erstellen, beispielsweise Aufgaben zur Virensuche, zum Update der Anwendung, zum Rollback des Updates oder zur Installation eines Lizenzschlüssels.

Um eine Liste der Aufgaben anzuzeigen, die für einen Client-Computer erstellt wurden:

1. Wählen Sie im Ordner **Gruppen** (s. Abb. 54) den Ordner mit dem Namen der Gruppe aus, zu welcher der Client-Computer gehört.
2. Wählen Sie im Detailfenster den Computer aus, für den Sie eine lokale Aufgabe erstellen möchten, und verwenden Sie den Befehl **Tasks** im Kontextmenü oder den entsprechenden Punkt im Menü **Aktion**. Dadurch wird im Anwendungshauptfenster das Eigenschaften-Fenster des Client-Computers geöffnet.
3. Auf der Registerkarte **Tasks** (s. Abb. 58) befindet sich eine vollständige Liste der Aufgaben, die für diesen Client-Computer erstellt worden sind.

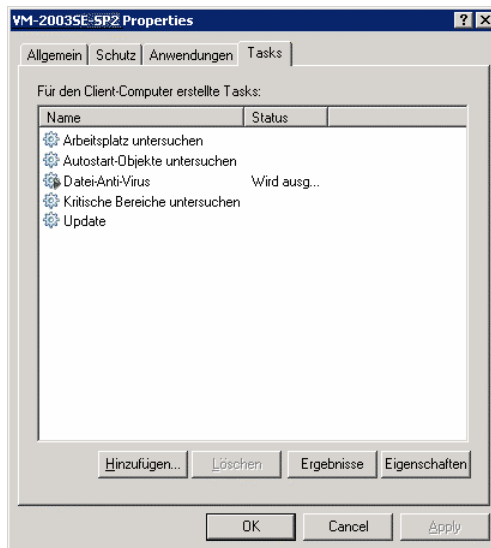


Abbildung 58. Liste der Aufgaben der Anwendung

12.2.1. Aufgaben starten und beenden

Der Start von Aufgaben erfolgt auf einem Client-Computer nur dann, wenn die entsprechende Anwendung läuft (s. Pkt. 12.1.1 auf S. 157). Wird eine Anwendung beendet, dann wird die Ausführung aller laufenden Aufgaben abgebrochen.

Start und Beenden von Aufgaben erfolgen automatisch (dem Zeitplan entsprechend). Außerdem können Aufgaben manuell (mit Hilfe des Befehls im Kontextmenü) oder aus dem Konfigurationsfenster der Aufgabe gestartet und beendet werden. Die Ausführung einer laufenden Aufgabe kann auch angehalten und später fortgesetzt werden.

Um eine Aktion manuell zu starten / zu beenden / anzuhalten / fortzusetzen:

wählen Sie die betreffende Aufgabe aus, öffnen Sie das Kontextmenü und wählen Sie den Befehl **Starten / Beenden / Anhalten / Fortsetzen** oder verwenden Sie die entsprechenden Punkte im Menü **Aktion**.

Sie können die entsprechenden Operationen auch aus dem Konfigurationsfenster der Aufgabe initiieren. Verwenden Sie dazu die gleichnamigen Schaltflächen auf der Registerkarte **Allgemein** (s. Abb. Abbildung 59).

12.2.2. Aufgaben erstellen

Wenn Sie über Kaspersky Administration Kit mit einer Aufgabe arbeiten, können Sie folgende Aufgabentypen erstellen:

- lokale Aufgaben – gelten für einen einzelnen Computer
- Gruppenaufgaben – gelten für Computer, die zu einer logischen Gruppe gehören
- globale Aufgaben – gelten für eine beliebige Auswahl von Computern aus beliebigen Gruppen eines logischen Netzwerks.

Sie können die Einstellungen von Aufgaben anpassen, die Aufgabenausführung überwachen, Aufgaben von einer Gruppe in eine andere kopieren und verschieben, oder löschen. Dazu dienen die standardmäßigen Kontextmenübefehle **Kopieren/Einfügen**, **Ausschneiden/Einfügen** und **Löschen** bzw. die entsprechenden Punkte im Menü **Aktion**.

12.2.2.1. Lokale Aufgabe erstellen

Um lokale Aufgabe zu erstellen, gehen Sie folgendermaßen vor:

1. Öffnen Sie das Eigenschaften-Fenster des Client-Computers auf der Registerkarte **Tasks** (s.Abb. Abbildung 58).
2. Verwenden Sie die Schaltfläche **Hinzufügen**, um eine neue Aufgabe hinzuzufügen. Das Fenster zum Erstellen einer neuen Aufgabe wird geöffnet. Seine Oberfläche entspricht einem Programmassistenten von Microsoft Windows und besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Weiter** und **Zurück**. Die Arbeit des Assistenten wird mit der Schaltfläche **Fertig stellen** abgeschlossen oder kann auf einer beliebigen Etappe mit der Schaltfläche **Abbrechen** abgebrochen werden.

Schritt 1. Allgemeine Angaben über die Aufgabe eingeben

Das erste Fenster des Assistenten dient der Eingabe des Aufgabennamens (Feld **Name**).

Schritt 2. Anwendung und Aufgabentyp auswählen

Auf dieser Etappe ist es erforderlich, die Anwendung anzugeben, für die die Aufgabe erstellt wird: Kaspersky Anti-Virus 6.0 for Windows Servers. Außerdem wird hier der Aufgabentyp gewählt. Für Kaspersky Anti-Virus 6.0 können folgende Aufgaben erstellt werden:

- *Virensuche* – Aufgabe zur Virensuche in den vom Benutzer angegebenen Bereichen.
- *Update* – Aufgabe zum Download und Verteilen eines Pakets mit Updates für die Anwendung.
- *Rollback des Updates* – Aufgabe zum Rollback des zuletzt ausgeführten Updates der Anwendung.
- *Installation eines Lizenzschlüssels* – Aufgabe zum Hinzufügen eines neuen Lizenzschlüssels für die Arbeit mit der Anwendung.

Schritt 3. Parameter der gewählten Aufgabentyps anpassen

Abhängig vom Aufgabentyp, der beim vorigen Schritt ausgewählt wurde, variiert der Inhalt der folgenden Fenster:

VIRENSUCHE

In Konfigurationsfenster für die Aufgabe zur Virensuche wird eine Liste der Untersuchungsobjekte erstellt (s. Pkt. 8.2 auf S. 89) und die Aktion angegeben,

die von Kaspersky Anti-Virus ausgeführt werden soll, wenn ein gefährliches Objekt gefunden wird (s. Pkt. 8.4.4 auf S. 98).

UPDATE

Für die Aufgabe zum Update der Bedrohungssignaturen und der Programm-Module ist es erforderlich, die Updatequelle festzulegen, aus der die Updates heruntergeladen werden sollen (s. Pkt. 10.4.1 auf S. 111). In der Grundeinstellung erfolgt das Update vom Updateserver der Anwendung Kaspersky Administration Kit.

UPDATE RÜCKGÄNGIG MACHEN

Die Aufgabe zum Update-Rollback besitzt keine spezifischen Einstellungen.

LIZENZSCHLÜSSEL INSTALLIEREN

Geben Sie für die Aufgabe zum Hinzufügen eines Lizenzschlüssels mit Hilfe der Schaltfläche **Durchsuchen** den Pfad der Schlüsseldatei an. Wenn der neue Schlüssel als Reserveschlüssel verwendet werden soll, aktivieren Sie das Kontrollkästchen **Als Reserveschlüssel hinzufügen**. Der Reserve-lizenzschlüssel wird aktiviert, wenn die Gültigkeitsdauer des aktiven Lizenzschlüssels abläuft.

Das Feld im unteren Bereich enthält Informationen über den neuen Schlüssel (Nummer, Typ und Gültigkeitsdauer der Lizenz).

Schritt 4. Aufgabenstart im Namen eines anderen Benutzerkontos anpassen

Bei diesem Schritt können Sie den Start der Aufgabe im Namen eines anderen Benutzerkontos anpassen, das nicht über ausreichende Rechte für den Zugriff auf das Untersuchungsobjekt oder die Updatequelle verfügt (s. Pkt. 6.4 auf S. 67).

Schritt 5. Zeitplan anpassen

Beim letzten Schritt der Aufgabenkonfiguration können Sie einen Zeitplan für den automatischen Start der Aufgabe festlegen.

Wählen Sie dazu in der Dropdown-Liste die gewünschte Frequenz für den Aufgabenstart und passen Sie im unteren Fensterbereich die Zeitplan-Einstellungen an.

Schritt 6. Erstellen der Aufgabe abschließen

Im letzten Fenster des Assistenten werden Sie über den erfolgreichen Abschluss des Vorgangs zum Erstellen der Aufgabe informiert.

12.2.2.2. Gruppenaufgabe erstellen

Um eine Gruppenaufgabe zu erstellen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur die Gruppe aus, für die Sie eine Aufgabe erstellen möchten.
2. Wählen Sie den zu dieser Gruppe gehörenden Ordner **Gruppentasks** aus, öffnen Sie das Kontextmenü und wählen Sie den Befehl **Neu → Task** oder verwenden Sie den entsprechenden Punkt im Menü **Aktion**. Dadurch wird der Assistent zum Erstellen einer neuen Aufgabe gestartet, der dem Assistenten zum Erstellen einer lokalen Aufgabe entspricht (Details s. Pkt. 12.2.1 auf S. 163). Folgen Sie den Anweisungen des Assistenten.

Nachdem die Arbeit des Assistenten abgeschlossen wurde, wird die Aufgabe dem Ordner **Gruppentasks** der entsprechenden Gruppe und aller zu ihr gehörenden untergeordneten Gruppen hinzugefügt und im Detailfenster angezeigt.

12.2.2.3. Globale Aufgabe erstellen

Um eine lokale Aufgabe zu erstellen, gehen Sie folgendermaßen vor:

1. Wählen Sie in der Konsolenstruktur das Element **Globale Tasks** aus, öffnen Sie das Kontextmenü und wählen Sie den Befehl **Neu → Task** oder den entsprechenden Punkt im Menü **Aktion**.
2. Dadurch wird der Assistent zum Erstellen einer neuen Aufgabe gestartet, der dem Assistenten zum Erstellen einer lokalen Aufgabe entspricht (Details s. Pkt. 12.2.1 auf S. 163). Ein Unterschied besteht darin, dass eine Etappe vorhanden ist, auf der eine Liste der Client-Computer des logischen Netzwerks angelegt wird, für welche die globale Aufgabe erstellt wird.
3. Wählen Sie die Computer des logischen Netzwerks aus, auf denen die Aufgabe gestartet werden soll. Es können Computer aus unterschiedlichen Ordnern oder ein ganzer Ordner ausgewählt werden (Einzelheiten siehe Administratorenhandbuch zu "Kaspersky Administration Kit").

Globale Aufgaben werden nur für die festgelegte Auswahl von Computern ausgeführt. Wenn zu einer Gruppe, für deren Computer eine Remote-Installationsaufgabe erstellt wurde, neue Client-Computer hinzugefügt werden, dann wird diese Aufgabe für die neuen Computer nicht ausgeführt. In diesem Fall muss eine neue Aufgabe erstellt oder die Einstellungen der vorhandenen Aufgabe müssen entsprechend angepasst werden.

Nachdem die Arbeit des Assistenten abgeschlossen wurde, wird die globale Aufgabe dem Element **Globale Tasks** der Konsolenstruktur hinzugefügt und im Detailfenster anzeigt.

12.2.3. Aufgabenparameter anpassen

Um die Parameter der Aufgaben eines Client-Computers anzuzeigen oder zu ändern:

1. Öffnen Sie das Eigenschaften-Fenster des Client-Computers auf der Registerkarte **Tasks** (s. Abb. 58).
2. Wählen Sie die Aufgabe in der Liste aus und klicken Sie auf die Schaltfläche **Eigenschaften**. Dadurch wird das Konfigurationsfenster für die Aufgabenparameter geöffnet (s. Abb. Abbildung 60).

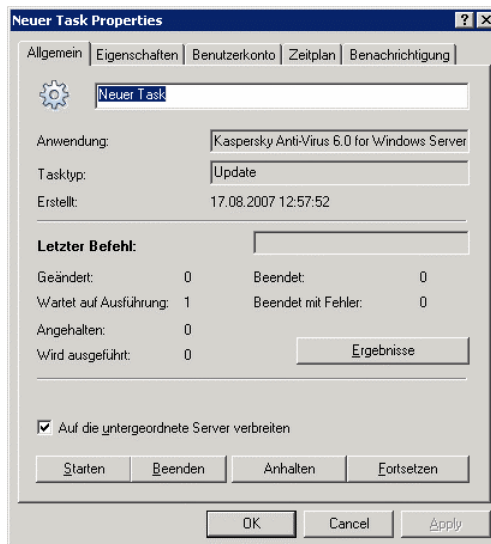


Abbildung 59. Aufgabenparameter anpassen

Alle Registerkarten (außer der Registerkarte **Eigenschaften**) sind für die Anwendung Kaspersky Administration Kit 6.0 standardmäßig und werden im entsprechenden Administratorenhandbuch ausführlich beschrieben. Die Registerkarte **Eigenschaften** bietet spezifische Parameter für Kaspersky Anti-Virus, wobei der Inhalt dieser Registerkarte in Abhängigkeit des gewählten Aufgabentyps variiert.

Die Konfiguration der Parameter für Aufgaben einer Anwendung über das Interface von Kaspersky Administration Kit entspricht der Konfiguration über das lokale Interface von Kaspersky Anti-Virus. Eine Ausnahme bilden die für die jeweilige Aufgabe spezifischen Parameter. Eine detaillierte Beschreibung der Konfiguration von Aufgabenparametern finden Sie in Kapitel 7 – Kapitel 10 auf S. 73 – 107 der vorliegenden Dokumentation.

Wenn für die Anwendung eine Richtlinie erstellt wird (s. Pkt. 12.3 auf S. 168), in der das Ändern bestimmter Parameter verboten ist, stehen diese bei der Konfiguration von Aufgaben nicht zur Verfügung.

12.3. Richtlinien verwalten

Die Verwendung von Richtlinien erlaubt es, einheitliche Einstellungen für die Anwendung und Aufgaben auf die Client-Computer zu verteilen, die zu einer Gruppe des logischen Netzwerks gehören.

Dieser Abschnitt enthält Informationen über das Erstellen und die Konfiguration einer Richtlinie für Kaspersky Anti-Virus 6.0 for Windows Servers. Detaillierte Angaben zur Konzeption der Richtlinienverwaltung über Kaspersky Administration Kit 6.0 finden Sie im Administratorenhandbuch des Produkts.


12.3.1. Richtlinie erstellen

Um eine Richtlinie für Kaspersky Anti-Virus zu erstellen, gehen Sie folgendermaßen vor:

1. Wählen Sie im Ordner **Gruppen** (s. Abb. 54) die Computergruppe aus, für die eine Richtlinie erstellt werden soll.
2. Wählen Sie den zur gewählten Gruppe gehörenden Ordner **Richtlinien** aus, öffnen Sie das Kontextmenü und verwenden Sie den Befehl **Neu** → **Richtlinie**. Auf dem Bildschirm erscheint das Fenster zum Erstellen einer neuen Richtlinie.

Das Interface des Programms zum Erstellen einer neuen Richtlinie besitzt die Form eines Programmassistenten für Microsoft Windows und besteht aus einer Reihe von Fenstern (Schritten). Zur Navigation zwischen den Fenstern dienen die Schaltflächen **Weiter** und **Zurück**. Die Arbeit des Assistenten wird mit der Schaltfläche **Fertig stellen** abgeschlossen oder kann auf einer beliebigen Etappe mit der Schaltfläche **Abbrechen** abgebrochen werden.

Während eine Richtlinie erstellt wird, können die angegebenen Parameter bei

jedem Schritt mit Hilfe der Schaltfläche  fixiert werden. Wenn das Schloss auf der Schaltfläche geschlossen ist, dann werden künftig bei der Verwendung der Richtlinie auf Client-Computern die von der Richtlinie festgelegten Werte benutzt.

Schritt 1. Allgemeine Angaben über die Richtlinie eingeben

Die ersten Schritte des Assistenten bestehen aus Eingabefenstern. Hier ist es erforderlich, den Namen der Richtlinie anzugeben (Feld **Name**) und die Anwendung **Kaspersky Anti-Virus 6.0 for Windows Servers** aus der Dropdown-Liste **Anwendungsname** auszuwählen. Damit die Einstellungen der Richtlinie sofort nach dem Erstellen wirksam werden, muss das Kontrollkästchen **Als aktive Richtlinie verwenden** aktiviert werden.

Schritt 2. Status der Richtlinie auswählen

In diesem Fenster können Sie den Status der Richtlinie festlegen. Wählen Sie dazu in der Auswahlliste den gewünschten Status aus: aktive Richtlinie oder inaktive Richtlinie.

In einer Gruppe können mehrere Richtlinien für eine Anwendung erstellt werden, wobei aber nur eine davon als aktive Richtlinie gelten kann.

Schritt 3. Schutzkomponenten auswählen und anpassen

Auf dieser Etappe können Sie den Computerschutz und die Komponente Datei-Anti-Virus aktivieren / deaktivieren. Standardmäßig sind der Schutz und der Datei-Anti-Virus aktiviert.

Um zur detaillierten Konfiguration der Schutzparameter oder zur Konfiguration von Datei-Anti-Virus zu gelangen, wählen Sie das entsprechende Element in der Liste aus und klicken Sie auf die Schaltfläche **Einstellungen**.

Schritt 4. Parameter der Virensuche anpassen

Bei diesem Schritt können Sie die Parameter anpassen, die von den Untersuchungsaufgaben verwendet werden sollen.

Wählen Sie im Block **Sicherheitsstufe** eine von drei vordefinierten Sicherheitsstufen aus (s. Pkt. 7.1 auf S. 74). Verwenden Sie die Schaltfläche **Einstellungen**, um eine gewählte Stufe genau anzupassen. Um die Parameter der Sicherheitsstufe **Empfohlen** wiederherzustellen, klicken Sie auf die Schaltfläche **Grundeinstellung**.

Geben Sie im Block **Aktion** die Aktion an, die Kaspersky Anti-Virus ausführen soll, wenn ein gefährliches Objekt gefunden wird (s. Pkt. 8.4.4 auf S. 98).

Schritt 5. Update-Einstellungen anpassen

In diesem Fenster können Sie die Parameter für das Update von Kaspersky Anti-Virus anpassen.

Geben Sie im Block **Update-Eigenschaften** an, ob das Update der Programm-Module ausgeführt werden soll (s. Pkt. 10.4.2 auf S. 114). Geben Sie im Fenster, das mit der Schaltfläche **Einstellungen** geöffnet wird, die Parameter des lokalen Netzwerks an (s. Pkt. 10.4.3 auf S. 116) und legen Sie die Updatequelle fest (s. Pkt. 10.4.1 auf S. 111).

Aktivieren / deaktivieren Sie im Block **Aktionen nach dem Update** die Untersuchung des Quarantänespeichers nach jedem Download eines neuen Updatepakets (s. Pkt. 10.4.4 auf S. 118).


Schritt 6. Richtlinie übernehmen

Auf dieser Etappe können Sie die Methode zum Verteilen der Richtlinie auf die Client-Computer der Gruppe wählen (zu Einzelheiten siehe Administratorenhandbuch zu "Kaspersky Administration Kit 6.0").

Schritt 7. Erstellen der Richtlinie abschließen

Das letzte Fenster des Assistenten informiert Sie darüber, dass der Vorgang zum Erstellen der Aufgabe erfolgreich abgeschlossen wurde.

Nachdem die Arbeit des Assistenten abgeschlossen wurde, wird die Richtlinie für Kaspersky Anti-Virus dem Ordner **Richtlinien** der entsprechenden Gruppe hinzugefügt und im Detailfenster angezeigt.

Sie können die Einstellungen der neuen Richtlinie ändern und mit Hilfe der Schaltfläche  für jede Gruppe von Einstellungen eine Beschränkung für das Ändern der Richtlinienparameter festlegen. Einstellungen, die auf diese Weise fixiert wurden, können vom Benutzer auf dem Client-Computer nicht geändert werden. Die Verteilung der Richtlinie an die Client-Computer erfolgt bei der ersten Synchronisierung der Clients mit dem Server.

Sie können Richtlinien von einer Gruppe in eine andere kopieren und verschieben oder sie löschen. Dazu dienen die standardmäßigen Kontextmenübefehle **Kopieren/Einfügen**, **Ausschneiden/Einfügen** und **Löschen** bzw. die entsprechenden Punkte im Menü **Aktion**.

12.3.2. Richtlinienparameter anzeigen und ändern

Auf dieser Etappe können Sie Änderungen in der Richtlinie vornehmen und ein Verbot für das Ändern von Parametern in den Richtlinien untergeordneter Gruppen, in den Anwendungsparametern und Aufgabenparametern erlassen.

Um die Parameter einer Richtlinie anzuzeigen oder zu ändern:

1. Wählen Sie in der Konsolenstruktur im Ordner **Gruppen** die Computergruppe aus, deren Einstellungen Sie ändern möchten.
2. Wählen Sie den zu dieser Gruppe gehörenden Ordner **Richtlinien** aus. Dadurch werden im Detailfenster alle Richtlinien angezeigt, die für diese Gruppe erstellt worden sind.
3. Wählen Sie in der Richtlinienliste die erforderliche Richtlinie für **Kaspersky Anti-Virus 6.0 for Windows Servers** aus (der Anwendungsname wird im Feld **Anwendung** angegeben).
4. Öffnen Sie das Kontextmenü der gewählten Richtlinie und verwenden Sie den Befehl **Eigenschaften**. Das Konfigurationsfenster der Richtlinie für Kaspersky Anti-Virus wird geöffnet (s. Abb. Abbildung 60).

Alle Registerkarten (außer **Eigenschaften**) sind für die Anwendung Kaspersky Administration Kit 6.0 standardmäßig. Eine ausführliche Beschreibung der Registerkarten ist im entsprechenden Administratorenhandbuch enthalten.

Die Registerkarte **Eigenschaften** bietet spezifische Richtlinienparameter für Kaspersky Anti-Virus 6.0. Die Richtlinienparameter umfassen Anwendungsparameter (s. Pkt. 12.1.2 auf S. 158) und Aufgabenparameter (s. Pkt. 12.2 auf S. 161).

Wählen Sie zur Konfiguration der Parameter den erforderlichen Wert aus der Dropdown-Liste im oberen Fensterbereich aus und nehmen Sie die gewünschten Einstellungen vor.

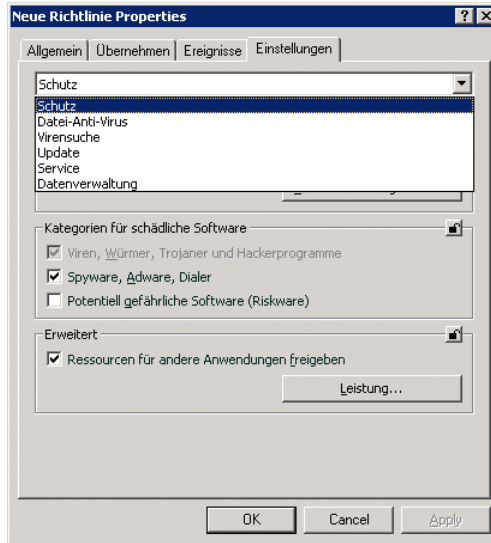


Abbildung 60. Richtlinienparameter anpassen

KAPITEL 13. ARBEIT MIT DEM PROGRAMM AUS DER BEFEHLSZEILE

Sie können mit Kaspersky Anti-Virus mit Hilfe der Befehlszeile arbeiten. Dabei ist die Möglichkeit zum Ausführen der folgenden Operationen vorgesehen:

- Starten, Beenden, Anhalten und Fortsetzen der Arbeit von Datei-Anti-Virus.
- Starten, Beenden, Anhalten und Fortsetzen der Arbeit von Aufgaben zur Virensuche.
- Erhalt von Informationen über den aktuellen Status von Datei-Anti-Virus und Aufgaben sowie ihrer Statistik.
- Untersuchung von ausgewählten Objekten.
- Update der Bedrohungssignaturen und Programm-Module.
- Aufruf der Hilfe über die Syntax der Befehlszeile.
- Aufruf der Hilfe über die Syntax eines Befehls.

Syntax der Befehlszeile:

```
avp.com <Befehl> [Parameter]
```

Der Zugriff auf die Anwendung über die Befehlszeile muss aus dem Installationsordner des Produkts oder unter Angabe des vollständigen Pfads von avp.com erfolgen.

Als **<Befehl>** werden verwendet:

ADDKEY	Aktivierung der Anwendung mit Hilfe einer Schlüsseldatei (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
ACTIVATE	Aktivierung der Anwendung über das Internet mit Hilfe eines Aktivierungscodes
START	Starten von Datei-Anti-Virus oder einer Aufgabe

PAUSE	Anhalten der Arbeit von Datei-Anti-Virus oder einer Aufgabe (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
RESUME	Fortsetzen der Arbeit von Datei-Anti-Virus oder einer Aufgabe
STOP	Beenden der Arbeit von Datei-Anti-Virus oder einer Aufgabe (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
STATUS	Bildschirmanzeige des aktuellen Status von Datei-Anti-Virus oder einer Aufgabe
STATISTICS	Bildschirmanzeige der Statistik über die Arbeit von Datei-Anti-Virus oder einer Aufgabe
HELP	Hilfe über die Befehlssyntax, Anzeige einer Befehlsliste
SCAN	Untersuchung von Objekten auf das Vorhandensein von Viren
UPDATE	Starten des Programm-Updates
ROLLBACK	Rückgängigmachen des zuletzt durchgeführten Updates der Anwendung (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
EXIT	Beenden der Arbeit mit dem Programm (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)
IMPORT	Importieren von Einstellungen für Kaspersky Anti-Virus (dieser Befehl kann nur ausgeführt werden, wenn das über die Programmoberfläche festgelegte Kennwort angegeben wird)

EXPORT	Exportieren von Einstellungen für Kaspersky Anti-Virus
---------------	--

Jedem Befehl entspricht eine eigene Auswahl von Parametern, die für eine konkrete Komponente von Kaspersky Anti-Virus spezifisch sind.

13.1. Aktivierung der Anwendung

Die Aktivierung des Programms kann auf zwei Arten erfolgen:

- über das Internet mit Hilfe eines Aktivierungscode (Befehl ACTIVATE)
- mit Hilfe einer Schlüsseldatei (Befehl ADDKEY)

Syntax der Befehlszeile:

```
ACTIVATE <Aktivierungscode>
```

```
ADDKEY <Dateiname> /password=<Kennwort>
```

Beschreibung der Parameter:

<Dateiname>	Name der Schlüsseldatei für die Anwendung (Endung *.key).
<Aktivierungscode>	Aktivierungscode für die Anwendung, den Sie beim Kauf des Produkts erhalten haben.
<Kennwort>	Kennwort für Kaspersky Anti-Virus, das über die Programmoberfläche festgelegt wurde.

Beachten Sie, dass dieser Befehl nur ausgeführt wird, wenn das Kennwort angegeben wird.

Beispiel:

```
avp.com ACTIVATE 11AA1-11AAA-1AA11-1A111
```

```
avp.com ADDKEY 1AA111A1.key /password=<Kennwort>
```

13.2. Steuerung von Datei-Anti-Virus und Aufgaben

Syntax der Befehlszeile:

```
avp.com <Befehl> <Profil|Aufgabenname>
[/R[A]:<Berichtsdatei>]
avp.com STOP|PAUSE <Profil|Aufgabenname>
/password=<Kennwort> [/R[A]:<Berichtsdatei>]
```

Beschreibung der Parameter:

<p><Befehl></p>	<p>Die Steuerung der Komponenten und Aufgaben von Kaspersky Anti-Virus wird mit Hilfe der folgenden Befehle ausgeführt:</p> <p>START – Start einer Echtzeitschutz-Komponente oder einer Aufgabe.</p> <p>STOP – Beenden einer Echtzeitschutz-Komponente oder einer Aufgabe.</p> <p>PAUSE – Anhalten der Arbeit einer Echtzeitschutz-Komponente oder einer Aufgabe.</p> <p>RESUME – Fortsetzen der Arbeit einer Echtzeitschutz-Komponente oder einer Aufgabe.</p> <p>STATUS – Den aktuellen Status einer Echtzeitschutz-Komponente oder einer Aufgabe auf dem Bildschirm anzeigen.</p> <p>STATISTICS – Die Statistik über die Arbeit einer Echtzeitschutz-Komponente oder einer Aufgabe auf dem Bildschirm anzeigen.</p> <p>Beachten Sie, dass die Befehle PAUSE und STOP nur ausgeführt werden, wenn das Kennwort eingegeben wird.</p>
<p><Profil Aufgabenname></p>	<p>Als Wert des Parameters <Profil> können eine beliebige Echtzeitschutz-Komponente der Anwendung, ein Modul, das zu den Komponenten gehört, eine erstellte Untersuchungs- oder Update-Aufgabe angegeben werden (Die von der Anwendung standardmäßig verwendeten Werte werden in der folgenden Tabelle genannt).</p> <p>Als Wert für den Parameter <Aufgabenname> kann der Name einer beliebigen vom Benutzer erstellten Untersuchungs- oder Update-Aufgabe angegeben werden.</p>
<p><Kennwort></p>	<p>Kennwort für Kaspersky Anti-Virus, das über die Programmoberfläche angegeben wurde.</p>

	Programmoberfläche angegeben wurde.
/R[A]:<Berichtsdatei>	<p>R:<Berichtsdatei> – nur wichtige Ereignisse im Bericht protokollieren.</p> <p>/RA:<Berichtsdatei> – alle Ereignisse im Bericht protokollieren.</p> <p>Die Angabe des absoluten oder relativen Dateipfads ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt. Dabei werden alle Ereignisse angezeigt.</p>

Für den Parameter <Profil> wird einer der folgenden Werte angegeben:

RTP	<p>alle Schutzkomponenten</p> <p>Der Befehl avp.com START RTP startet die Komponente Datei-Anti-Virus, wenn diese mit der Schaltfläche II der grafischen Benutzeroberfläche oder mit dem Befehl PAUSE aus der Befehlszeile vorübergehend angehalten wurde.</p> <p>Wenn die Komponente mit der Schaltfläche ■ der grafischen Benutzeroberfläche oder mit dem Befehl STOP aus der Befehlszeile beendet wurde, ist zum Starten der Komponente der Befehl avp.com START FM erforderlich.</p>
FM	Datei-Anti-Virus
UPDATER	Update
RetranslationCfg	Verteilung der Updates für die Anwendung in die lokale Updatequelle
Rollback	Rollback des letzten Updates der Anwendung
SCAN_OBJECTS	die Aufgabe "Virensuche"
SCAN_MY_COMPUTER	die Aufgabe "Arbeitsplatz"
SCAN_CRITICAL_AREAS	die Aufgabe "Kritische Bereiche"

SCAN_STARTUP	die Aufgabe "Autostart-Objekte"
SCAN_QUARANTINE	Aufgabe zur Untersuchung der Quarantäneobjekte
Die aus der Befehlszeile gestarteten Komponenten und Aufgaben werden mit den Parametern ausgeführt, die im Interface des Programms festgelegt wurden.	

Beispiele:

Um Datei-Anti-Virus zu aktivieren, geben Sie in der Befehlszeile ein:

```
avp.com START FM
```

Um die Aufgabe Arbeitsplatz zu beenden, geben Sie in der Befehlszeile ein:

```
avp.com STOP SCAN_MY_COMPUTER /password=<Kennwort>
```

13.3. Virenuntersuchung von Objekten

Die Befehlszeile zum Starten der Virenuntersuchung eines bestimmten Bereichs und zur Bearbeitung von schädlichen Objekten besitzt folgendes allgemeines Aussehen:

```
avp.com SCAN [<Untersuchungsobjekt>] [<Aktion>]  
[<Dateitypen>] [<Ausnahmen>] [<Konfigurationsdatei>]  
[<Berichtsparameter>] [<zusätzliche Parameter>]
```

Für die Untersuchung von Objekten können Sie auch die in Kaspersky Anti-Virus erstellten Aufgaben verwenden, indem Sie die erforderliche Befehlszeile benutzen (s. Pkt. 13.2 auf S. 175). Dabei wird die Aufgabe mit den Parametern ausgeführt, die im Interface des Produkts festgelegt wurden.

Beschreibung der Parameter.

<Untersuchungsobjekt> - Der Parameter gibt eine Liste der Objekte an, die auf das Vorhandensein von schädlichem Code untersucht werden sollen.

Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.

<files>	<p>Liste mit den Pfaden der Dateien und/oder Ordner für die Untersuchung.</p> <p>Die Angabe des absoluten oder relativen Pfads ist zulässig. Als Trennzeichen für die Elemente der Liste dient das Leerzeichen.</p> <p>Kommentare:</p> <ul style="list-style-type: none"> • Wenn der Objektname ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt. • Wenn ein konkreter Ordner angegeben wird, werden alle darin enthaltenen Dateien untersucht.
/MEMORY	Objekte des Arbeitsspeichers.
/STARTUP	Autostart-Objekte.
/MAIL	Mail-Datenbanken.
/REMDRIVES	alle Wechseldatenträger.
/FIXDRIVES	alle lokalen Laufwerke.
/NETDRIVES	alle Netzwerklaufwerke.
/QUARANTINE	Objekte in Quarantäne.
/ALL	vollständige Untersuchung des Computers.
/@:<filelist.lst>	<p>Pfad der Datei mit einer Liste der Objekte und Ordner, die untersucht werden sollen. Die Datei muss das Textformat besitzen. Jedes Untersuchungsobjekt muss in einer separaten Zeile stehen.</p> <p>Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Pfad ein Leerzeichen enthält, wird er in Anführungszeichen gesetzt.</p>

<p><Aktion> - Der Parameter bestimmt die Aktionen mit einem schädlichen Objekt, das während der Untersuchung gefunden wird. Wenn der Parameter nicht angegeben wird, wird standardmäßig die Aktion ausgeführt, die dem Wert /i8 entspricht.</p>	
/i0	Keine Aktion ausführen, nur Informationen im Bericht protokollieren.
/i1	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – überspringen.
/i2	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; infizierte Objekte aus Containern (zusammengesetzten Objekten) nicht löschen; Container mit ausführbarer Kopfzeile (sfx-Archive) löschen (diese Aktion wird standardmäßig verwendet).
/i3	infizierte Objekte desinfizieren; wenn die Desinfektion nicht möglich ist – löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i4	infizierte Objekte löschen; Container-Objekte vollständig löschen, wenn die darin enthaltenen infizierten Dateien nicht gelöscht werden können.
/i8	Beim Fund eines infizierten Objekts den Benutzer nach der Aktion fragen.
/i9	Den Benutzer nach der Aktion fragen, wenn die Untersuchung abgeschlossen wird.
<p><Dateitypen> - Der Parameter bestimmt die Typen der Dateien, die der Virenuntersuchung unterzogen werden. Wenn der Parameter nicht angegeben wird, werden standardmäßig nur infizierbare Dateien nach ihrem Inhalt untersucht.</p>	
/fe	nur infizierbare Dateien nach Erweiterung untersuchen.
/fi	nur infizierbare Dateien nach Inhalt untersuchen.

/fa	Alle Dateien untersuchen.
<p><Ausnahmen> - Der Parameter bestimmt die Objekte, die von der Untersuchung ausgeschlossen werden sollen.</p> <p>Der Parameter kann mehrere Werte aus der folgenden Liste enthalten. Die Werte werden durch Leerzeichen getrennt.</p>	
-e:a	Archive nicht untersuchen.
-e:b	Mail-Datenbanken nicht untersuchen.
-e:m	E-Mail-Nachrichten im Format plain text nicht untersuchen.
-e:<filemask>	Objekte nach Maske nicht untersuchen.
-e:<seconds>	Objekte überspringen, deren Untersuchung länger dauert, als der durch den Parameter <seconds> angegebene Zeitraum.
-es:<size>	Objekte überspringen, deren Größe (in MB) über dem Wert liegt, der durch den Parameter <size> angegeben wird.
<p><Konfigurationsdatei> - bestimmt den Pfad der Konfigurationsfenster, in der die Parameter für die Arbeit des Programms bei der Untersuchung enthalten sind.</p> <p>Die Konfigurationsdatei ist eine Datei im Textformat, die eine Auswahl von Befehlszeilenparametern für die Antiviren-Untersuchung enthält.</p> <p>Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die im Interface von Kaspersky Anti-Virus festgelegt wurden.</p>	
/C:<Dateiname>	Die Werte der Parameter, die in der Konfigurationsdatei <Dateiname> angegeben sind, verwenden.

<Berichtsparameter> - Der Parameter bestimmt das Format des Berichts über die Untersuchungsergebnisse.	
Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt. Alle Ereignisse werden angezeigt.	
/R:<Berichtsdatei>	nur wichtige Ereignisse in der angegebenen Berichtsdatei protokollieren.
/RA:<Berichtsdatei>	alle wichtigen Ereignisse in der angegebenen Berichtsdatei protokollieren.
<zusätzliche Parameter> - Parameter, der die Verwendung von Technologien zur Virenuntersuchung festlegt.	
/iChecker=<on off>	Verwendung der Technologie iChecker aktivieren / deaktivieren.
/iSwift=<on off>	Verwendung der Technologie iSwift aktivieren / deaktivieren.

Beispiele:

*Untersuchung des Arbeitsspeichers, der Autostart-Objekte, der Mail-Datenbanken sowie der Ordner **My Documents**, **Program Files** und der Datei **test.exe**:*

```
avp.com SCAN /MEMORY /STARTUP /MAIL "C:\Documents and
Settings\All Users\My Documents" "C:\Program Files"
"C:\Downloads\test.exe"
```

Anhalten der Untersuchung von ausgewählten Objekten, Starten der vollständigen Untersuchung des Computers, bei Abschluss der Untersuchung soll die Virensuche in den ausgewählten Objekten fortgesetzt werden:

```
avp.com PAUSE SCAN_OBJECTS /password=<Kennwort>
avp.com START SCAN_MY_COMPUTER
avp.com RESUME SCAN_OBJECTS
```

*Untersuchung der Objekte, deren Liste in der Datei **object2scan.txt** angegeben ist. Für die Arbeit soll die Konfigurationsdatei **scan_setting.txt** verwendet werden. Über die Untersuchungsergebnisse soll ein Bericht erstellt werden, in dem alle Ereignisse aufgezeichnet werden:*

```
avp.com SCAN /MEMORY /@:objects2scan.txt
/C:scan_settings.txt /RA:scan.log
```

Beispiel für die Konfigurationsdatei:

```
/MEMORY /@:objects2scan.txt /C:scan_settings.txt
/RA:scan.log
```

13.4. Programm-Update

Der Befehl für das Update der Programm-Module und Bedrohungssignaturen von Kaspersky Anti-Virus besitzt folgende Syntax:

```
avp.com UPDATE [<Updatequelle>]
[/R[A]:<Berichtsdatei>] [/C:<Dateiname>]
[/APP=<on|off>]
```

Beschreibung der Parameter:

<Updatequelle>	HTTP-, FTP-Server oder Netzwerkordner für den Download der Updates. Als Wert für diesen Parameter kann der vollständige Pfad oder die URL-Adresse der Updatequelle angegeben werden. Wenn der Pfad nicht angegeben wird, wird die Updatequelle aus den Parametern des Diensts für das Programm-Update übernommen.
/R[A]:<Berichtsdatei>	<p>/R:<Berichtsdatei> - nur wichtige Ereignisse im Bericht protokollieren.</p> <p>/R[A]:<Berichtsdatei> - alle Ereignisse im Bericht protokollieren.</p> <p>Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt. Alle Ereignisse werden angezeigt.</p>

<code>/C:<Dateiname></code>	<p>Pfad der Konfigurationsdatei, die die Parameter für die Arbeit des Programms beim Update enthält.</p> <p>Die Konfigurationsdatei ist eine Datei im Textformat, die eine Auswahl von Befehlszeilenparametern für das Update der Anwendung enthält.</p> <p>Die Angabe des absoluten oder relativen Pfads ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Werte verwendet, die im Interface von Kaspersky Anti-Virus festgelegt wurden.</p>
<code>/APP=<on off></code>	Update der Programm-Module aktivieren/deaktivieren.

Beispiele:

Update der Bedrohungssignaturen, alle Ereignisse protokollieren:

```
avp.com UPDATE /RA:avbases_upd.txt
```

*Update der Programm-Module von Kaspersky Anti-Virus, die Parameter der Konfigurationsdatei **updateapp.ini** verwenden:*

```
avp.com UPDATE /APP=on /C:updateapp.ini
```

Beispiel für die Konfigurationsdatei:

```
"ftp://my_server/kav updates" /RA:avbases_upd.txt  
/app=on
```

13.5. Rollback des letzten Programm-Updates

Syntax der Befehlszeile:

```
ROLLBACK [/R[A]:<Berichtsdatei>] [/password=<Kennwort>]
```

/R[A]:<Berichtsdatei>	<p>/R:<Berichtsdatei> - nur wichtige Ereignisse im Bericht aufzeichnen.</p> <p>/R[A]:<Berichtsdatei> - alle Ereignisse im Bericht aufzeichnen.</p> <p>Die Angabe des absoluten oder relativen Pfads der Datei ist zulässig. Wenn der Parameter nicht angegeben wird, werden die Untersuchungsergebnisse auf dem Bildschirm angezeigt, alle Ereignisse werden angezeigt.</p>
<Kennwort>	Kennwort für Kaspersky Anti-Virus, das über die Programmoberfläche festgelegt wurde.
<p>Beachten Sie, dass dieser Befehl nur ausgeführt wird, wenn das Kennwort angegeben wird.</p>	

Beispiel:

```
avp.com ROLLBACK /RA:rollback.txt /password=<Kennwort>
```

13.6. Export von Parametern

Syntax der Befehlszeile:

```
avp.com EXPORT <Profil> <Dateiname>
```

Beschreibung der Parameter:

<Profil>	Datei-Anti-Virus oder Aufgabe, für die der Export von Parametern ausgeführt wird. Als Wert des Parameters <Profil> kann einer der in Pkt. 13.2 auf S. 175 genannten Werte verwendet werden.
<Dateiname>	Pfad der Datei, in welche die Parameter von Kaspersky Anti-Virus exportiert werden. Ein absoluter oder relativer Pfad kann angegeben werden. Die Konfigurationsdatei wird im Binärformat (<i>dat</i>) gespeichert, falls kein anderes Format angegeben oder kein Format festgelegt wird, und kann später zum Übertragen von Anwendungseinstellungen auf andere Computer verwendet werden. Die Konfigurationsdatei kann auch im Textformat gespeichert werden. Dazu erhält der Dateiname die Endung <i>txt</i> . Beachten Sie, dass der Import von Schutzparametern aus einer Textdatei nicht unterstützt wird. Diese Datei kann nur zur Ansicht der grundlegenden Funktionsparameter der Anwendung verwendet werden.

Beispiele:

```
avp.com EXPORT c:\settings.dat
```

13.7. Import von Parametern

Syntax der Befehlszeile:

```
avp.com IMPORT <Dateiname> [/password=<Kennwort>]
```

<Dateiname>	<p>Pfad der Datei, aus welcher die Parameter von Kaspersky Anti-Virus importiert werden. Ein absoluter oder relativer Pfad kann angegeben werden.</p> <p>Der Import von Schutzparametern ist nur aus einer Datei im Binärformat möglich.</p> <p>Wenn die Anwendung im Silent-Modus über die Befehlszeile oder über den Gruppenrichtlinienobjekt-Editor installiert wird, muss die Konfigurationsdatei den Namen <i>install.cfg</i> tragen, andernfalls wird sie von der Anwendung nicht erkannt.</p>
<Kennwort>	Kennwort für Kaspersky Anti-Virus, das über die Programmoberfläche festgelegt wurde.
<p>Beachten Sie, dass dieser Befehl nur ausgeführt wird, wenn das Kennwort angegeben wird.</p>	

Beispiel:

```
avp.com IMPORT c:\settings.dat /password=<Kennwort>
```

13.8. Anwendung starten

Syntax der Befehlszeile:

```
avp.com
```

13.9. Anwendung beenden

Syntax der Befehlszeile:

```
EXIT /password=<Kennwort>
```

<Kennwort>	Kennwort für Kaspersky Anti-Virus, das über die Programmoberfläche festgelegt wurde.
<p>Beachten Sie, dass dieser Befehl nur ausgeführt wird, wenn das Kennwort angegeben wird.</p>	

13.10. Anlegen einer Tracing-Datei

Das Anlegen einer Tracing-Datei kann erforderlich sein, wenn bei der Arbeit mit der Anwendung Probleme auftreten, deren genaue Analyse durch die Experten des Technischen Support-Services notwendig ist.

Befehlssyntax:

```
avp.com TRACE [file] [on|off] [<Tracing-Niveau>]
```

[on off]	Anlegen der Tracing-Datei aktivieren/deaktivieren.
[file]	Tracing in Form einer Datei erstellen.
<Tracing-Niveau>	Für diesen Parameter kann ein Zahlenwert im Bereich von 0 (minimale Stufe, nur kritische Meldungen) bis 700 (maximale Stufe, alle Meldungen) festgelegt werden. Wenn Sie sich an den Technischen Support-Service wenden, nennt Ihnen der zuständige Spezialist das erforderliche Tracing-Niveau. Andernfalls gilt das Niveau 500 als empfehlenswert.
<p>Achtung! Es wird empfohlen, das Anlegen von Tracing-Dateien nur zur Diagnose eines konkreten Problems zu aktivieren. Sollte das Tracing ständig aktiv sein, so kann die Leistungsfähigkeit des Computers sinken und es kann zu einer Überfüllung der Festplatte kommen.</p>	

Beispiele:

Erstellen von Tracing-Dateien deaktivieren:

```
avp.com TRACE file off
```

Erstellen einer Tracing-Datei zum Senden an den Technischen Support-Service, mit einem maximalen Tracing-Niveau von 500:

```
avp.com TRACE file on 500
```

13.11. Anzeige der Hilfe

Zur Anzeige der Hilfe über die Syntax der Befehlszeile dient folgender Befehl:

```
avp.com [ /? | HELP ]
```

Um Hilfe über die Syntax eines konkreten Befehls zu erhalten, können Sie einen der folgenden Befehle verwenden:

```
avp.com <Befehl> /?  
avp.com HELP <Befehl>
```

13.12. Rückgabecodes der Befehlszeile

In diesem Abschnitt werden die Rückgabecodes der Befehlszeile beschrieben. Die allgemeinen Codes können von einem beliebigen Befehl der Befehlszeile zurückgegeben werden. Als Rückgabecodes für Aufgaben sind die allgemeinen Codes sowie spezifische Codes für einen konkreten Aufgabentyp möglich.

Allgemeine Rückgabecodes	
0	Operation wurde erfolgreich ausgeführt
1	Ungültiger Parameterwert
2	Unbekannter Fehler
3	Fehler bei Ausgabenausführung
4	Aufgabenausführung wurde abgebrochen
Rückgabecodes für Aufgaben zur Antiviren-Untersuchung	
101	Alle gefährlichen Objekte wurden bearbeitet
102	Es wurden gefährliche Objekte gefunden

KAPITEL 14. PROGRAMM ÄNDERN, REPARIEREN ODER LÖSCHEN

Zur Deinstallation des Programms stehen folgende Varianten zur Verfügung:

- mit Hilfe des Installationsassistenten (s. Pkt. 14.1 auf S. 190)
- aus der Befehlszeile (s. Pkt. 14.2 auf S. 193)
- über Kaspersky Administration Kit (siehe "Handbuch für Kaspersky Administration Kit").
- über Domänen-Gruppenrichtlinien für Microsoft Windows Server 2000/2003 (s. Pkt. 3.4.3 auf S. 35).

14.1. Ändern, Reparieren oder Löschen des Programms mit Hilfe des Installationsassistenten

Die Reparatur des Programms kann dann von Nutzen sein, wenn Sie Fehler in seiner Arbeit feststellen, die auf inkorrekte Einstellungen oder beschädigte Programmdateien zurückgehen.

Um den ursprünglichen Programmzustand wiederherzustellen, um Komponenten von Kaspersky Anti-Virus, die bei der Erstinstallation nicht installiert wurden, zu installieren, oder um das Programm zu löschen,

1. Legen Sie die CD mit der Programmdistribution in das CD-ROM-Laufwerk ein, wenn die Installation von dort aus erfolgte. Wenn die Installation von Kaspersky Anti-Virus aus einer anderen Quelle erfolgte (gemeinsamer Ordner, Ordner auf der Festplatte usw.), vergewissern Sie sich, dass die Programmdistribution in dieser Quelle vorhanden ist und Sie zugriffsberechtigt sind.
2. Wählen Sie **Start → Programme → Kaspersky Anti-Virus 6.0 for Windows Servers → Ändern, Reparieren oder Löschen.**

Dadurch wird das Installationsprogramm in Form eines Assistenten gestartet. Im Folgenden werden die Schritte zur Reparatur, zum Ändern des Bestands der Programmkomponenten und zum Löschen des Programms ausführlich beschrieben.

Schritt 1. Startfenster des Installationsprogramms

Wenn Sie alle oben beschriebenen Aktionen ausgeführt haben, die für die Reparatur oder das Ändern des Komponentenbestands erforderlich sind, wird auf dem Bildschirm das Begrüßungsfenster des Installationsprogramms für Kaspersky Anti-Virus geöffnet. Klicken Sie auf die Schaltfläche **Weiter**.

Schritt 2. Auswahl einer Operation

Nun müssen Sie festlegen, welche Operation Sie mit dem Programm vornehmen möchten: Zur Auswahl stehen das Ändern der Programmkomponenten, das Wiederherstellen des ursprünglichen Zustands der installierten Komponenten oder das Löschen bestimmter Komponenten oder des ganzen Programms. Klicken Sie zum Ausführen der von Ihnen gewünschten Operation auf die entsprechende Schaltfläche. Die weitere Aktion des Installationsprogramms ist von der gewählten Operation abhängig.

Das Ändern des Komponentenbestands entspricht der benutzerdefinierten Installation des Programms (s. Schritt 7 auf S. 24), bei der Sie festlegen können, welche Komponenten installiert und welche gelöscht werden sollen.

Die Reparatur des Programms erfolgt auf Basis der installierten Komponenten. Alle Dateien der Komponenten, die installiert sind, werden aktualisiert und für jede dieser Komponenten wird die **empfohlene** Sicherheitsstufe eingestellt.

Achtung!

Wenn Kaspersky Anti-Virus 6.0 im entfernten Modus deinstalliert wird, wird der Server nicht automatisch neu gestartet. Zur vollständigen Deinstallation der Anwendungskomponenten und zur künftigen korrekten Arbeit des Computers ist es allerdings empfehlenswert, den Neustart manuell durchzuführen.

Beim Löschen des Programms können Sie wählen, welche der bei der Arbeit des Programms erstellten und verwendeten Daten, auf Ihrem Computer gespeichert werden sollen. Um alle Daten von Kaspersky Anti-Virus zu löschen, wählen Sie die Variante **Die Anwendung vollständig löschen**. Um bestimmte Daten zu speichern, wählen Sie die Variante **Objekte der Anwendung speichern** und geben Sie an, welche Objekte beibehalten werden sollen:

- *Aktivierungsdaten* – Informationen über die Tatsache der Aktivierung der Anwendung

- *Bedrohungssignaturen* – vollständige Signaturen der gefährlichen Programme, Viren und anderen Bedrohungen, die beim letzten Update aktuell waren.
- *Backup-Objekte* – Sicherungskopien von gelöschten oder desinfierten Objekten. Es wird empfohlen, diese Objekte zu speichern, um sie bei Bedarf später wiederherzustellen.
- *Quarantäneobjekte* – Objekte, die möglicherweise von Viren oder Virusmodifikationen infiziert sind. Solche Objekte enthalten Code, der Ähnlichkeit mit dem Code eines bekannten Virus besitzt. Allerdings lässt sich nicht sicher sagen, ob sie schädlich sind. Es wird empfohlen, diese Objekte zu speichern, weil sie sich als virenfrei erweisen oder später unter Verwendung von aktualisierten Bedrohungssignaturen desinfiziert werden können.
- *Schutzeinstellungen* – Parameterwerte für die Arbeit von Datei-Anti-Virus.
- *iSwift-Daten* – Datenbank, die Informationen über untersuchte Objekte des NTFS-Dateisystems enthält. Sie erlaubt die Beschleunigung der Untersuchung von Objekten. Durch die Verwendung dieser Datenbank untersucht Kaspersky Anti-Virus nur jene Objekte, die seit der letzten Untersuchung verändert wurden.

Achtung.

Wenn zwischen der Deinstallation einer Version von Kaspersky Anti-Virus und der Installation einer anderen Version ein größerer Zeitraum liegt, wird davon abgeraten, die aus der vorherigen Programminstallation stammende *iSwift*-Datenbank zu verwenden. In der Zwischenzeit kann ein gefährliches Programm auf den Computer gelangt sein, dessen schädliche Aktionen bei Verwendung dieser Datenbank nicht erkannt werden, was zu einer Infektion des Computers führen kann.

Klicken Sie auf die Schaltfläche **Weiter**, um die gewählte Operation zu starten. Der Prozess zum Kopieren der notwendigen Dateien auf Ihren Computer oder zum Löschen der ausgewählten Komponenten und Daten wird gestartet.

Schritt 3. Abschluss der Operation zum Reparieren, Ändern oder Löschen des Programms

Der Prozess zum Reparieren, Ändern oder Löschen wird auf dem Bildschirm dargestellt. Danach werden Sie über den Abschluss des Vorgangs informiert.

Die Deinstallation macht in der Regel den Neustart des Computers erforderlich, weil Änderungen im System berücksichtigt werden müssen. Auf dem Bildschirm erscheint eine Bestätigungsabfrage für den Neustart des Computers. Klicken Sie auf die Schaltfläche **Ja**, um den Neustart sofort vorzunehmen, oder auf die Schaltfläche **Nein**, um den Computer später manuell neu zu starten.

14.2. Deinstallation des Programms aus der Befehlszeile

Um Kaspersky Anti-Virus 6.0 for Windows Servers aus der Befehlszeile zu deinstallieren, geben Sie ein:

```
msiexec /x <Paketname>
```

Es wird ein Installationsassistent gestartet (s. Kapitel 14 auf S. 190), mit dessen Hilfe Sie die Deinstallation der Anwendung vornehmen können.

Um die Anwendung im Silent-Modus ohne Neustart des Computers zu deinstallieren (der Neustart muss nach der Deinstallation manuell erfolgen), geben Sie folgende Befehlszeile ein:

```
msiexec /x <Paketname> /qn
```

Um die Anwendung im Silent-Modus mit anschließendem Neustart des Computers zu deinstallieren, geben Sie folgende Befehlszeile ein:

```
msiexec /x <Paketname> ALLOWREBOOT=1 /qn
```

Wenn bei der Installation der Anwendung ein Kennwort zum Verbot der Deinstallation der Anwendung festgelegt wurde, muss beim Entfernen des Produkts dieses Kennwort verwendet werden. Andernfalls wird der Deinstallationsvorgang nicht ausgeführt.

Um die Anwendung mit Kennwortangabe für die Deinstallation der Anwendung zu installieren, geben Sie ein:


```
msiexec /x <Paketname> KLUNINSTPASSWD=***** – zur  
Installation im interaktiven Modus.
```

```
msiexec /x <Paketname> KLUNINSTPASSWD=***** /qn – zur  
Installation im Silent-Modus ohne Neustart des Computers.
```

ANHANG A. ZUSÄTZLICHE INFORMATIONEN

Dieser Anhang enthält Informationen über die Formate von zu untersuchenden Dateien und über zulässige Masken, die bei der Konfiguration von Kaspersky Anti-Virus verwendet werden können.

A.1. Liste der Objekte, die nach Erweiterung untersucht werden

Wenn Sie als Untersuchungsobjekte für Datei-Anti-Virus oder für eine Untersuchungsaufgabe die Variante  **Programme und Dokumente (nach Erweiterung) untersuchen** gewählt haben, dann werden Dateien mit den unten aufgezählten Erweiterungen ausführlich auf Viren analysiert.

com – ausführbare Programmdatei.

exe – ausführbare Datei, selbstextrahierendes Archiv.

sys – Systemtreiber.

prg – Text der Programme dBase, Clipper oder Microsoft Visual FoxPro, Programm des Pakets WAVmaker.

bin – Binärdatei.

bat – Datei einer Paketaufgabe.

cmd – Befehlsdatei für Microsoft Windows NT (entspricht einer bat-Datei für DOS), OS/2.

dpl – komprimierte Bibliothek für Borland Delphi.

dll – Dynamic Link Library (Dynamische Verbindungsbibliothek).

scr – Bildschirmschonerdatei für Microsoft Windows.

cpl – Systemsteuerungsmodul (control panel) in Microsoft Windows.

ocx – Microsoft OLE-Objekt(Object Linking and Embedding).

tsp – Programm, das im Timesharing-Modus arbeitet.

drv – Treiber für ein bestimmtes Gerät.

vxd – Treiber für ein virtuelles Microsoft-Windows-Gerät.

pif – Datei mit Informationen zum Programm.

lnk – Linkdatei in Microsoft Windows.

reg – Registrierungsdatei für Schlüssel der Microsoft-Windows-Systemregistrierung.

ini – Initialisierungsdatei.
cla – Java-Klasse.
vbs – Visual-Basic-Skript.
vbe – BIOS-Video-Erweiterung.
js, jse – JavaScript-Quelltext.
htm – Hypertext-Dokument.
htt – Hypertext-Entwicklung von Microsoft Windows.
hta – Hypertext-Programm für Microsoft Internet Explorer.
asp – Active-Server-Pages-Skript.
chm – kompilierte HTML-Datei.
pht – HTML-Datei mit eingebettetem PHP-Skript.
php – Skript, das in eine HTML-Datei eingebettet wird.
wsh – Microsoft Windows Script Host-Datei.
wsf – Microsoft-Windows-Skript.
the – Bildschirmschonerdatei für den Arbeitsplatz von Microsoft Windows 95
hlp – Hilfedatei des Formats Win Help.
eml – E-Mail-Nachricht für Microsoft Outlook Express.
nws – neue E-Mail-Nachricht für Microsoft Outlook Express.
msg – E-Mail-Nachricht für Microsoft Mail.
plg – E-Mail-Nachricht
mbx – Erweiterung für eine gespeicherte Nachricht in Microsoft Office Outlook.
*doc** – Dokument für Microsoft Office Word, z.B.: *doc* – Dokument für Microsoft Office Word, *docx* – Dokument für Microsoft Office Word 2007 mit XML-Unterstützung, *docm* – Dokument für Microsoft Office Word 2007 mit Makro-Unterstützung.
*dot** – Dokumentvorlage für Microsoft Office Word, z.B.: *dot* – Dokumentvorlage für Microsoft Office Word, *dotx* – Dokumentvorlage für Microsoft Office Word 2007, *dotm* – Dokumentvorlage für Microsoft Office Word 2007 mit Makro-Unterstützung.
fpm – Datenbankprogramm, Startdatei für Microsoft Visual FoxPro.
rtf – Dokument im Rich-Text-Format.
shs – Fragment für Shell Scrap Object Handler.
dwg – Datenbank für AutoCAD-Skizzen.
msi – Microsoft Windows Installer-Paket.
otm – VBA-Projekt für Microsoft Office Outlook.
pdf – Adobe Acrobat-Dokument.
swf – Shockwave Flash-Paketobjekt.

jpg, jpeg – Grafikdatei zum Speichern von komprimierten Bildern.

emf – Datei des Formats Enhanced Metafile. Folgegeneration einer Metadatei des Betriebssystems Microsoft Windows. EMF-Dateien werden von 16-Bit-Microsoft Windows nicht unterstützt.

ico – Symboldatei für ein Objekt.

ov? – ausführbare Datei für MS DOS.

*xl** – Dokumente und Dateien für Microsoft Office Excel, z.B.: *xla* – Erweiterung für Microsoft Office Excel, *xlc* – Diagramm, *xlt* – Dokumentvorlage, *xlsx* – Arbeitsmappe für Microsoft Office Excel 2007, *xltm* – Arbeitsmappe für Microsoft Office Excel 2007 mit Makro-Unterstützung, *xlsb* – Arbeitsmappe für Microsoft Office Excel 2007 im Binärformat (nicht XML), *xltx* – Vorlage für Microsoft Office Excel 2007, *xlsm* – Vorlage für Microsoft Office Excel 2007 mit Makro-Unterstützung, *xlam* – Snap-In für Microsoft Office Excel 2007 mit Makro-Unterstützung.

*pp** – Dokumente und Dateien für Microsoft Office PowerPoint, z.B.: *pps* – Dia für Microsoft Office PowerPoint, *ppt* – Präsentation, *pptx* – Präsentation für Microsoft Office PowerPoint 2007, *pptm* – Präsentation für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, *potx* – Präsentationsvorlage für Microsoft Office PowerPoint 2007, *potm* – Präsentationsvorlage für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, *ppsx* – Diashow für Microsoft Office PowerPoint 2007, *ppsm* – Diashow für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung, *ppam* – Snap-In für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung.

*mda** – Dokumente und Dateien für Microsoft Office Access, z.B.: *mda* – Arbeitsgruppe für Microsoft Office Access, *mdb* – Datenbank usw.

sldx – Dia für Microsoft Office PowerPoint 2007.

sldm – Dia für Microsoft Office PowerPoint 2007 mit Makro-Unterstützung.

thmx – Thema für Microsoft Office 2007.

Beachten Sie, dass das tatsächliche Format einer Datei von dem Format abweichen kann, das in der Dateierweiterung angegeben ist.

A.2. Zulässige Ausschlussmasken für Dateien

Hier werden Beispiele für zulässige Masken genannt, die Sie beim Erstellen der Liste auszuschließender Dateien verwenden können:

- Masken ohne Dateipfad:

- ***.exe** – alle Dateien mit der Endung *exe*
- ***.ex?** – alle Dateien mit der Endung *ex?*, wobei anstelle von ? ein beliebiges Zeichen stehen kann.
- **test** – alle Dateien mit dem Namen *test*
- Masken mit absolutem Dateipfad:
 - **C:\dir*.*** oder **C:\dir*** oder **C:\dir** – alle Dateien im Ordner *C:\dir*
 - **C:\dir*.exe** – alle Dateien mit der Endung *exe* im Ordner *C:\dir*
 - **C:\dir*.ex?** – alle Dateien mit der Endung *ex?* im Ordner *C:\dir*, wobei anstelle von ? ein beliebiges Zeichen stehen kann.
 - **C:\dir\test** – nur die Datei *C:\dir\test*

Um zu verhindern, dass die Dateien in allen untergeordneten Ordnern des gewählten Ordners untersucht werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen **Untergeordnete einschließen**.

- Masken mit relativem Dateipfad:
 - **dir*.*** oder **dir*** oder **dir** – alle Dateien in allen Ordnern von *dir*
 - **dir\test** – alle Dateien *test* in den Ordnern von *dir*
 - **dir*.exe** – alle Dateien mit der Endung *exe* in allen Ordnern von *dir*
 - **dir*.ex?** – alle Dateien mit der Endung *ex?* in allen Ordnern von *dir*, wobei anstelle von ? ein beliebiges Zeichen stehen kann.

Um zu verhindern, dass die Dateien in allen untergeordneten Ordnern des gewählten Ordners untersucht werden, aktivieren Sie beim Erstellen der Maske das Kontrollkästchen **Untergeordnete einschließen**.

Hinweis:

Die Verwendung der Ausnahmemaske *.* oder * ist nur unter Angabe der Klassifikation der auszuschließenden Bedrohung entsprechend der Viren-Enzyklopädie zulässig. In diesem Fall wird die betreffende Bedrohung in allen Objekten von der Untersuchung ausgeschlossen. Werden diese Masken ohne Angabe einer Klassifikation verwendet, so entspricht dies dem Deaktivieren des Echtzeitschutzes.

Außerdem wird davor gewarnt, als Ausnahme ein virtuelles Laufwerk zu wählen, das auf der Basis eines Ordners des Dateisystems mit dem Befehl *subst* erstellt wurde. Dies wäre sinnlos, da das Programm das virtuelle Laufwerk bei der Untersuchung als Ordner betrachten und folglich untersuchen würde.

A.3. Zulässige Ausschlussmasken nach der Klassifikation der Viren-Enzyklopädie

Wenn eine Bedrohung, die einen bestimmten Status nach der Klassifikation der Viren-Enzyklopädie besitzt, als Ausnahme hinzugefügt wird, können Sie angeben:

- den vollständigen Namen der Bedrohung, wie er in der Viren-Enzyklopädie auf der Seite www.viruslist.de genannt wird (beispielsweise **not-a-virus:RiskWare.RemoteAdmin.RA.311** oder **Flooder.Win32.Fuxx**).
- den Namen der Bedrohung als Maske, beispielsweise:
 - **not-a-virus*** – legale, aber potentiell gefährliche Programme sowie Scherzprogramme von der Untersuchung ausschließen.
 - ***Riskware.*** – alle potentiell gefährlichen Programme des Typs Riskware von der Untersuchung ausschließen.
 - ***RemoteAdmin.*** – alle Programmversionen zur entfernten Verwaltung von der Untersuchung ausschließen.

A.4. Beschreibung von Parametern der Datei *setup.ini*

Die Datei *setup.ini*, die sich im Distributionsordner von Kaspersky Anti-Virus befindet, wird verwendet, wenn die Anwendung im Silent-Modus über die Befehlszeile (s. Pkt. 3.3 auf S. 33) oder über den Gruppenrichtlinienobjekt-Editor (s. Pkt. 3.4 auf S. 34) installiert wird. Die Datei enthält folgende Parameter:

[Setup] – generelle Parameter für die Installation der Anwendung.

InstallDir=<Pfad des Ordners für die Installation der Anwendung>.

Reboot=yes|no – gibt an, ob zum Abschluss der Anwe3.ndungsinstallation der Neustart des Computers erfolgen soll (Standardmäßig wird kein Neustart ausgeführt).

SelfProtection=yes|no – gibt an, ob der Selbstschutz von Kaspersky Anti-Virus bei der Installation aktiviert werden soll (Der Selbstschutz ist standardmäßig aktiviert).

MSExclusions=yes|no – gibt an, ob die von der Firma Microsoft für Server empfohlenen Ausnahmen zur Liste der Ausnahmen hinzugefügt werden sollen.

AddPath=yes|no – gibt an, ob der Pfad von avp.com zu der Systemumgebungsvariablen %Path% hinzugefügt werden soll.

[Components] – Auswahl der zu installierenden Anwendungskomponenten. Wenn diese Gruppe keine Elemente enthält, wird die Anwendung vollständig installiert.

FileMonitor=yes|no – Installation der Komponente Datei-Anti-Virus.

[Tasks] – Aktivieren der Aufgaben von Kaspersky Anti-Virus. Wenn keine Aufgaben angegeben werden, werden nach der Installation alle Aufgaben gestartet. Ist mindestens eine Aufgabe angegeben, dann werden alle nicht gewählten Aufgaben deaktiviert.

ScanMyComputer=yes|no – Aufgabe zur vollständigen Untersuchung des Computers.

ScanStartup=yes|no – Aufgabe zur Untersuchung von Autostart-Objekten.

ScanCritical=yes|no – Aufgabe zur Untersuchung von kritischen Bereichen.

Updater=yes|no – Aufgabe zum Update der Bedrohungssignaturen und Programm-Module.

Anstatt des Werts **yes** können auch die Werte **1, on, enable, enabled** benutzt werden, anstelle von **no** sind auch die Werte – **0, off, disable, disabled** zulässig.

ANHANG B. KASPERSKY LAB

Das Unternehmen

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

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

Einzigartige Erfahrung

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

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

Kaspersky Anti-Virus

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

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

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

Komplexe Technologien für Ihre Sicherheit

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

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

Service

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

B.1. Andere Produkte von Kaspersky Lab

Kaspersky Lab News Agent

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

News Agent verfügt außerdem über folgende Funktionen:

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

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

Kaspersky® OnLine Scanner

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

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

Kaspersky® OnLine Scanner Pro

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

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

Kaspersky Anti-Virus® 7.0

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

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

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

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

Der Proaktive Schutz umfasst:

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

Kaspersky® Internet Security 7.0

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

Die Funktion des Antiviren-Schutzes umfasst:

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

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

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

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

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

Kaspersky Anti-Virus Mobile

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

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

Kaspersky Anti-Virus für File-Server

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

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

Vorzüge und Funktionen:

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

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

Kaspersky Open Space Security

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

Das Softwareprodukt umfasst vier Produkte:

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

Im Folgenden wird jedes Produkt genau beschrieben.

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

Vorzüge und Funktionen:

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

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

Daten und ermöglicht den Benutzern den schnellen Zugriff auf Netzwerkressourcen.

Vorzüge und Funktionen:

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

Kaspersky Enterprise Space Security

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

Vorzüge und Funktionen:

- *Schutz für Workstations und Server vor Viren, Trojanern und Würmern*

- *Schutz der Mailserver Sendmail, Qmail, Postfix und Exim*
- *Untersuchung aller E-Mails auf einem Microsoft Exchange Server, einschließlich der gemeinsamen Ordner*
- *Bearbeitung von E-Mails, Datenbanken und anderen Objekten auf Lotus Notes/Domino-Servern*
- *Schutz vor Phishing-Angriffen und Spam*
- *Verhinderung von massenhaften E-Mails und Viren-Epidemien*
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Remote-Administration des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung*
- *Unterstützung von Cisco[®] NAC (Network Admission Control);*
- *Proaktiver Schutz für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.*
- *Personal Firewall mit IDS/IPS-System*
- *Schutz bei der Arbeit in Wi-Fi-Netzwerken*
- *Untersuchung des Internet-Traffics in Echtzeit*
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Dynamisches Ressourcen-Management bei der vollständigen Untersuchung des Systems*
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Berichtssystem über den Status des Schutzsystems*
- *Automatisches Update der Datenbanken*

Kaspersky Total Space Security

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

Vorzüge und Funktionen:

- *Komplexer Schutz vor Viren, Spyware, Hackerangriffen und Spam auf allen Ebenen eines Unternehmensnetzwerks von der Workstation bis zur Internet-Gateway.*

- *Proaktiver Schutz* für Workstations vor neuen Schadprogrammen, die noch nicht in die Datenbanken aufgenommen wurden.
- *Schutz für Mailserver und Groupware-Server*
- *Echtzeit-Untersuchung des Internet-Datenverkehrs (HTTP/FTP)*, der in ein lokales Netzwerk eintrifft.
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Sperren des Zugriffs auf infizierte Workstations*
- *Verhinderung von Viren-Epidemien*
- *Zentrale Berichte über den Schutzstatus*
- *Remote-Administration* des Produkts, einschließlich zentraler Installation, Konfiguration und Steuerung
- *Unterstützung von Cisco® NAC (Network Admission Control)*;
- *Unterstützung von Hardware-Proxyservern*
- *Filterung des Internet-Datenverkehrs* nach einer Liste vertrauenswürdiger Server, nach Objekttypen und nach Benutzergruppen
- *Verwendung der iSwift-Technologie zur Vermeidung wiederholter Untersuchungen* innerhalb eines Netzwerks
- *Dynamisches Ressourcen-Management* bei der vollständigen Untersuchung des Systems
- *Personal Firewall* mit IDS/IPS-System
- *Sichere Arbeit in Netzwerken aller Typen*, einschließlich Wi-Fi
- *Schutz vor Phishing-Angriffen und Spam*
- *Möglichkeit zur Remote-Reparatur (Intel® Active Management - Intel® vPro™)*
- *Rollback-Funktion für schädliche Veränderungen im System*
- *Technologie zum Selbstschutz des Antiviren-Programms vor Schadprogrammen*
- *Vollständige Unterstützung von 64-Bit-Betriebssystemen*
- *Automatisches Update der Datenbanken*

Kaspersky Security für Mail-Server

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

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

Funktionen:

- *Zuverlässiger Schutz vor schädlichen und potenziell gefährlichen Programmen*
- *Spam-Filterung*
- *Scan von ein- und ausgehenden E-Mails und E-Mail-Anhängen*
- *Antiviren-Untersuchung aller E-Mails auf einem Microsoft Exchange Server, einschließlich der gemeinsamen Ordner*
- *Untersuchung von E-Mails, Datenbanken und anderen Objekten auf Lotus Notes/Domino-Servern*
- *Filterung von E-Mails nach Typen der Anhänge*
- *Isolierung verdächtiger Objekte in einem speziellen Speicher*
- *Komfortable Bedienung*
- *Verhinderung von Viren-Epidemien*
- *Monitoring für den Status des Schutzsystems mit Hilfe von Benachrichtigungen*
- *Berichtssystem über die Arbeit der Anwendung*
- *Skalierbarkeit im Rahmen der verfügbaren Systemressourcen*
- *Automatisches Update der Datenbanken*

Kaspersky Security für Internet-Gateway

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

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

Funktionen:

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

Kaspersky® Anti-Spam

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

Kaspersky® Anti-Spam ist ein Filterprogramm, das, am "Eingang" des firmeninternen Netzwerks installiert, sämtliche eingehenden E-Mails auf Spam überprüft. Das Programm ist kompatibel mit jedem beliebigen Mailing-System und kann sowohl auf bereits funktionierenden als auch auf separaten Mailservern installiert werden.

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

Kaspersky Anti-Virus® for MIMESweeper

Kaspersky Anti-Virus® for MIMESweeper bietet die Hochgeschwindigkeits-Antiviren-Untersuchung des Datenverkehrs auf Servern, die Clearswift

MIMESweeper for SMTP / Clearswift MIMESweeper for Exchange / Clearswift MIMESweeper for Web verwenden.

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

B.2. Kontaktinformationen

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

Weitere Information erhalten Sie bei:

Kaspersky Labs GmbH
Steinheilstraße 13
85053 Ingolstadt

Technischer Support	E-Mail: support@kaspersky.de
Allgemeine Informationen	WWW: http://www.kaspersky.de/ http://www.viruslist.de/
Feedback zu unseren Benutzerhandbüchern	docfeedback@kaspersky.com (Diese Adresse ist für Rückmeldungen über das Handbuch und elektronische Hilfesystem gedacht.)

ANHANG C. ENDBENUTZER- LIZENZVERTRAG

Endbenutzer-Lizenzvertrag für die erworbene KASPERSKY LAB SOFTWARE

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

Indem Sie das Sicherheitsetikett auf der CD-Box aufreißen oder wenn Sie die SOFTWARE installieren, erklären Sie sich mit den Bestimmungen des EULAs einverstanden. Falls Sie mit den Bestimmungen des EULAs NICHT einverstanden sind, geben Sie die erworbene Software bitte innerhalb von 14 Tagen an die Einkaufsstelle zurück. Nach Eingabe des Aktivierungscode sind eine Rückgabe der Software ausgeschlossen.

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

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

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

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

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

2. EINSCHRÄNKUNGEN

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

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

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

5. GEWÄHRLEISTUNG. KASPERSKY LAB gewährleistet, dass:

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

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

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

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

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